CNS. 31-01-2018.

MOD-1

Cyber Attacks.

1] Motives

A Hacker is a successful name for Cyber attack. Hackers are youngsters/teenagers who use attack kits designed by other which are freely downloaded from internet.

Attackers include company insiders like unsatisfied employees.

Cyber terrorists who expose extreme religious & political cause.

Main motives for launching Cyber attacks are:

1] Theft of Sensitive Information.
2] Distruption of Services.
3] Illegal access to or use of Resources.

1] Theft of sensitive info.

Many organisation store & communicate sensitive info on new products to be designed.

Revenue service can be usually advantageous to a company competitors.

Military & Defence plan details of any nation.

pvt Bodies like Corps, Banks, etc & individual's personal info. like credit, cards, passwords, etc.

Taking this is called "Identity Theft".

2] Distruption of services.

Interruption of service against an organisation server which causes unavailable or inaccessible services.

Eg: attacks being launched by business rivals of e-commerce web-sites.

3] Illegal access to or use of resources.
The Goal is to use to obtain free access of services to paid resources.
Eg: Online digital products such as magazines, journal articles, free talk time, etc.

Common attacks.

Attempting to retrieve personal info. from individuals is one common attack which has 2 categories
1] Pharming attack. 2] Phishing attack.

1] It is a cyber attack intended to readirect a web-site's traffic to another fake site.
2] ~~St~~ It is an attempt to obtain sensitive info. such as user name, password & credit card details by discussing it with a trust-worthy entity in an electronic communication.

One type of intruding into a system is through password guessing attack, side channel attack, skimming attack.
All these forms are identity theft.

Password Guessing attack is done by guessing the keystrokes used by the user.

DOS ~~ED~~ [Denial of Services]
These attackers exhaust the computing power, memory capacity or communication bandwidth of their targets so they are unavailable.

Another important classes of attacks is caused by various types of malware.

-> Viruses -> Trojan.

-> Worm -> Spyware.

Virus typically infects a file. So, it spreads from one file to another.

Worms are usually stand-alone program that infects a computer so a worm spreads from one computer to another.

Trojan is a kind of malware which modifies the files, data theft, etc.

Spy-ware installed on a machine can be used to monitor user activities as a key logger to recover valuable info. such as passwords / user keystrokes.

Vulnerability.

Vulnerability in procedures, protocols, h/w or s/w within an organisation that will cause damage.

There are atleast 4 important vulnerability classes in the domain of security, they are

-> Human vulnerabilities. -> Software vulnerabilities.

-> Protocol vulnerabilities. -> Configuration vulnerabilities.

Human vulnerabilities includes human behaviour / action.

Eg: user clicking on the link in a e-mail received from the unknown resources. This type is kalled phishing.

Protocol vulnerabilities includes no. of ~~wor~~ networking protocols including ARP, ACMP, UDP, DNS and various protocols have been used in a anticipated way for attacks.

Eg: Pharming attack is an example. It also leads for man in the middle attack.

Software vulnerabilities is caused by weekly written system code or application s/w which normally happens at the time of ~~user~~ i/p's.

Configuration vulnerabilities relates to configuration settings on newly installed files, etc. By Read/Write executable permissions on files, etc providing privileges on the application, etc.

Different Strategies

Defence Strategies.

1] Access Control → Authentication.
└→ Authorisation.

Authentication

Access control is to permit or deny the entry into the system which is called as authentication process. which can be implemented by some of the trusted third party appⁿs/s/w's & also it may be a part of OS to protect the s/m.

Authorisation.

Involves granting a specific entity the permission to access some restricted data or perform some restricted operations

2] Data Protection.

Data confidentiality. & Data Integrity.

Data confidentiality ~~&~~ is the protection of data from disclosure to an unauthorised party or process.

Data Integrity, it is a assurance that data hasn't been modified, tampered with or made inconsistent in any way

To perform this data protection some of the cryptographic techniques are used. This is done by encryption & decryption of data for confidentiality & cryptography checksum is used for data integrity.

5] Prevention and detection.

Access Control and message encryptions are all of preventing strategies.

Cryptographic checksum on the other hand detects tampering of messages.

The intrusion detection system also looks for certain patterns of behaviour.

Response, recovering, forensic.

Once an attack or infection has been detected response measure should be quickly taken like shutting down all the system or part of the system during a malware infection in which necessary actions should be taken like quarantined and necessary patches are applied.

Cyber forensic is an emerging discipline with a set of tools that helps trace back the criminals of cyber crime.

Guiding Principles.

1> Security is as much a human problem than a technological problem & must be addressed at different levels.

2> Security should be factored at inception not as an after thought.

3> Security ~~by~~ being unknown is often bogus.

4> Always consider the defult denial policy for adoption in access control.

5> An entity should be given the least amount of permissions or privileges to accomplish a given task.

6> Use defence in depth to ~~ana~~ enhance the security of an architectural design,

7→ Identify vulnerabilities and respond appropriately.

8→ Carefully study the trade of involving security before making any.

Co-prime, Congruency, Relative prime.

Modulo Arithmetic.

Let 'd' be an integer & let 'n' be a +ve integer. Let q and r be quotient & remainders obtained ~~fo~~ by dividing d by n.

Therefore, the relationship b/w d, n, q, r is

$d = (n*q)+r$.

$n=10$ $\quad r=3$.

$q = \{0, 1, 2, 3..\}$.

the set of d values

$\{\ldots -27, -17, -7, 3, 13, 23, 33, \ldots\}$.

Congruency modulo.

represented by $r \equiv d \pmod{n}$

If 2 integers are congruent modulo n then they differ by an integral multiple of n.

$a \bmod n = r \qquad b \bmod n = r$.

then, $a = n*q_1+r$.

$b = n*q_2+r$.

$a-b = n*q_1+r-(n*q_2+r)$.

$a-b = n(q_1-q_2)$.

Since q_1 & q_2 are integers a & b differ by an integral multiple of n.

1] $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n.$

2] $(a-b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n.$

3] $(a*b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n.$

Properties of modulo arithmetic.

→ Verify property-1 for $n = 8$, $a = 27$, $b = 34$.

$(27+34) \bmod 8 = 61 \bmod 8 = \underline{\underline{5}}.$

~~a~~ $\underbrace{(27 \bmod 8) + (34 \bmod 8)}_{3\ +\ 2} = 5 \bmod 8 = \underline{\underline{5}}.$

∴ LHS = RHS.

GCD

If ~~a~~ two integers a & b, if a divides b and a divides c & their exists number a' > a such that a'/b and a'/c, then a is referred to the greatest common divisor of b and c denoted as

$a = \gcd(b, c).$

If gcd of b, c i.e $\gcd(b, c) = 1$.
(b, c) can be a prime or co-prime or relatively prime.

$\gcd(b, c) = 1.$

d	n
161	120

Euclid's formula.

$d\,b = (n*q) + r.$

$161 = 120(1) + (41).$

$120 = 41(2) + (38).$

$41 = 38(1) + (3).$

$38 = 3(12) + (2).$

$3 = 2(1) + \boxed{1}.$

$2 = 1(2) + (0).$

$\gcd = \underline{1}.$

Eg: (56,15)

$56 = 15(3) + (11).$

$15 = 11(1) + (4).$

$11 = 4(2) + (3).$

$4 = 3(1) + \boxed{1}.$

$3 = 1(3) + (0).$

Eg: gcd (161, 112)

$161 = 112(1) + 49$

$112 = 49(2) + 14$

$49 = 14(3) + \boxed{7}$ gcd.

$14 = 7(2) + 0.$

Extended Euclid's Algorithm

GCD theorem.

Given integers b and c there exists two integers x & y such that $\boxed{bx + cy = \gcd(b,c)}$

$bx + cy = 1$, if b and c are relatively prime or co prime numbers.

$7 = 49 - 14 * 3.$

$7 = (1)49 - (112 - 49 * 2) * 3,$

$7 = 49 * 7 + 112 * (-3).$ $\quad 49 \; (-112 - 1 * 2) * 3$

$= (161 - 112 * 1) * 7 + 112 * (-3).$ $\quad 1 * 49 * \overset{3*2+1}{3 * 2} - (112 * 3)$

$= (161 * 7) + 112 * (-10).$ $\quad 49 * 7 + 112 * (-3).$

$x = 7.$

$y = -10.$

gcd (79, 12)

$12 \bmod 79 = 12.$

$79 \bmod 12 = 7.$

$79 = 12(6) + (7)$

$12 = 7(1) + (5)$

$7 = 5(1) + (2)$

$5 = 2(2) + \boxed{(1)}$ gcd.

$2 = 1(2) + 0.$

$2 = 5 - 2*(2).$

$2 = 5 - 2*2.$

$= (1)5 - (7 - 5*1)*2.$

$= 5*(3) + 7*(-2)$

$= (12 - 7*1)*3 + 7*(-2).$

$= 12*3 + 7*(-5).$

$= 12*3 + (79 - 12*6)*(-5).$

$= 12*33 + 79*(-5)*$

$= x = -5$

$y = 33.$

In cryptography, we often need to compute multiplicative inverse modulo prime no's i.e

$b*x + c*y = 1$, Since $c*y$ differs from 1 by an integral multiple of b.

$c*y \equiv 1 \bmod b.$

It follows that y is actually the inverse of c mod b.

To obtain inverse of c mod b we use extended Euclidean algorithm.

The inverse c%b cx mod b. 12 mod 79.

12 mod 79.

12^{-1} mod 79.

$12*y \equiv 1 \bmod 79.$

$12*y = 1*5*79 \bmod 79.$

$12 * y \equiv 1 \bmod 79$.

or.

$* 33 = 1 + 5 * 79 \equiv 1 \pmod{79}$

$33 = 1 \bmod 79$.

$35^{-1} \bmod 6$.

$35y = 1 \bmod 6$.

$5y \equiv 1 \bmod 6$.

$25y \equiv 5 \bmod 6$.

$1y = 5 \bmod 6$.

$\underline{y=5}$.

$30^{-1} \bmod 7$.

$30y \equiv 1 \bmod 7$.

$2y \equiv 1 \bmod 7$

$8y \equiv 4 \bmod 7$.

$\boxed{y=4}$.

$42^{-1} \bmod 5$.

$4\overset{2y}{\cancel{y}} \equiv 1 \bmod 5$.

$8y \equiv 1 \bmod 5$.

Chinese Remainder Theorem. [CRT]

Used to solve a set of congruent with one variable but with different modulus which are relatively prime as shown below.

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$.

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

To solve set of equations, there are few steps

1] Find $M = m_1 \times m_2 \times m_3 \dots m_k$.

This is to find the common modulo.

2] Finding $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_k = \frac{M}{m_k}$.

3] Finding the multiplicative inverse of ~~$M_1, M_2, \ldots$~~ $M_1, M_2, M_3, \ldots\ldots M_k$. using the corresponding $(m_1, m_2, m_3, \ldots\ldots m_k) = m_1^{-1}, m_2^{-1}, \ldots\ldots m_k^{-1}$.

$$M_1^{-1} \bmod m_1 \quad M_2^{-1} \bmod m_2 \; \ldots \; M_k^{-1} \bmod m_k .$$

# 4] $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots\ldots + a_k * M_k \times M_k^{-1}) \bmod M$.

$x \equiv 2 \pmod 3$ —— (1)
$x \equiv 3 \pmod 5$ —— (2)
$x \equiv 2 \pmod 7$ —— (3)

$M = 3 \times 5 \times 7 = 105$.

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$.

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$.

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$.

Rough

$35y \equiv 1 \bmod 3$
$2y \equiv 1 \bmod 3$
$\underline{y = 2}$ $\underline{M_1^{-1} = 2}$.

$21y \equiv 1 \bmod 5$.
$\underline{y = 1}$ $\underline{M_2^{-1} = 1}$.

$15y \equiv 1 \bmod 7$.
$\underline{y = 1}$ $\underline{M_3^{-1} = 1}$.

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$.
$x = (140 + 63 + 30) \bmod 105$.
$x = 233 \bmod 105$.
$x = 23$. —— (1) —— (2) —— (3).

TE Let ~~N~~ $N = 210$ & $n_1 = 5$ $n_2 = 6$, $n_3 = 7$, Compute $f^{-1}(3, 5, 2)$ $x_1 = 3$ $x_2 = 5$ $x_3 = 2$.

$\frac{\overset{46}{253}}{105}$
84

$x_1 = 3$ $n_1 = 5$ $N = 210$ $f^{-1}(3,5,2)$.

$x_2 = 5$ $n_2 = 6$

$x_3 = 2$ $n_3 = 7$

$N_1 = \frac{210}{5} = 42$.

$N_2 = \frac{210}{6} = 35$.

$N_3 = \frac{210}{7} = 30$.

$42y \equiv 1 \bmod 5$.

$35y \equiv 1 \bmod 6$.

$30y \equiv 1 \bmod 7$.

$42y \equiv 1 \bmod 5$.

$2y \equiv 1 \bmod 5$.

$\underline{\underline{y=3}}$ $\underline{\underline{N_1^{-1} = 3}}$.

$x = (3 \times \underset{9}{42} \times 3 + \overset{175}{5 \times 35 \times 5} + \overset{120}{2 \times 30 \times 4})$

$\bmod 210$.

$x = (378 + 875 + 240) \bmod 210$.

$x = 1493 \bmod 210$.

$35y \equiv 1 \bmod 6$.

$5y \equiv 1 \bmod 6$.

$\underline{\underline{y=5}}$ $\underline{\underline{N_2^{-1} = 5}}$.

$9^{-1} \bmod 26$.

$9y \equiv 1 \bmod 26$.

$\underline{\underline{y=3}}$ $(27)-(26)$
$= \underline{1}$

$30y \equiv 1 \bmod 7$.

$2y \equiv 1 \bmod 7$.

$8y \equiv 4 \bmod 7$.

$\underline{\underline{y=4}}$ $\underline{\underline{N_3^{-1} = 4}}$.

Find an integer that have remainder of 3 when divided by 7 and 13 and divisible by 12. using CRT solve

$x \equiv 3 \bmod 7$

$x \equiv 3 \bmod 13$

$x \equiv 0 \bmod 12$

$M = 7 \times 13 \times 12 = 84 \times 13 = 1092$.

$M_1 = \frac{1092}{7} = 156$.

$M_2 = \frac{1092}{13} = 84$.

$M_3 = \frac{1092}{12} = 91$.

$156y \equiv 1 \bmod 7$.

$2y \equiv 1 \bmod 7$

$8y \equiv 4 \bmod 7$.

$\underline{y=4}$ $\underline{M_1^{-1} = 4}$

$84y \equiv 1 \bmod 13$ $\qquad$ $91y \equiv 1 \bmod 12$.

$6y \equiv 1 \bmod 13$. $\qquad$ $7y \equiv 1 \bmod 12$.

$\underline{y=11}$ $\qquad$ $\underline{y=5}$ $\underline{M_2^{-1}=5}$ $\underline{y=7}$ $\underline{M_3^{-1}=7}$.

$\underline{M_2^{-1}=11}$.

$x = (3 \times \overset{156}{\cancel{1092}} \times 4 + 3 \times \cancel{1092} \times 84 \times 11 + 0 \times 91 \times 7) \bmod 1092$.

$x = 4644 \bmod 1092$.

$x = 276$.

Basics of Cryptography.

Cryptography is the science of hiding messages so that only the intended recipient can decipher the received message.

The original msg to be transferred is called plain text. & its hidden version is cipher text.

The process of hiding the original plain text is called encryption.

The process of recovering the original plain text from the cipher text is called decryption.

Encryption involves the use of encryption functions or algorithms denoted by E.

Encryption key (e).

Decryption involves the use of decryption functions or algorithms denoted by D.

Decryption key (d).

$C = E_e(P)$. $\qquad$ C = cipher text.

$P = D_d(C)$. $\qquad$ P = Plain text.

Secret vs. Public key Cryptography.

The two types of cryptography techniques used are secret key & public key.

Secret key Cryptography.

Both sender & receiver share a common secret for encryption & decryption of message.

i.e (e=d)

This is also referred as symmetric key algorithm.

Public key Cryptography.

Two distinct keys are used i.e encryption key is called public key & decryption key is called private key.

The pub key of a receiver is used for encryption & at the receiving end the private key is used for decryption of message.

i.e pub key & prt key ~~has no any~~ doesn't have any relationship also known as asymmetric key algorithm.

$$C_1 = E_{e.Bpu}(P).$$

$$P = D_{d.Bpr}(C_1).$$

[Later] Types of attacks

The attacker is known as cryptanalysts.

Substitutional Ciphers.

→Monoalphabetic Cipher

The m cipher is used for substituting the alphabets with different alphabets which shifts the letters of one alphabets ~~with~~ against another alphabet to create the secret message which is called as "Caesar Cipher", which was found by an Roman Emperor Julius Caesar.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z for key = 5

↓

F

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

The shifting is done by key no. of positions i.e encryption process is cipher text = m + e mod 26.

$C = m + e \bmod 26$ m = message.

Decryption process is $m = C + d \bmod 26$.

if $e = 3$.

$d = -3 \bmod 26$.

$d = 23$.

Eg: Perform Caesar cipher for a key = 3 m = what is the population of Mars?.

key = 3.

C =

What is the population of MARS

ZKDW LV WKH SRSXODWLRQ RI PDUV

k = 5.

This is a secret message

YMNX NX FF XJHWJY RJXXFLJ.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

→<u>Polyalphabetic Cipher</u>.

In p cipher the cipher text corresponding to a particular character in the plain text is not fixed.

I] ~~Vigenere Cipher~~.

The plain text is broken into blocks of keyword size (m), the key length or the keyword uses a multidigit key i.e $k_1, k_2, k_3, \ldots k_m$ on each integers.

The first letter of each block is replaced by the letter k_1 position to its right.

The 2nd letter is replaced by the letter k_2 position to its right & so on.

Eg:

(1) Vigenere Cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Key (MATH)

key :(12, 0, 19, 7)

MAKE IT HAPPEN.

12,0,19,7 12,0 19,7,12,0,19,7.

× MATH MA TH MATH

YADL UAT AHBPAU

Key (04, 19, 3, 22, 7, 12, 5, 11)

~~4 19 3~~ 11 4 19

WISHING YOU MUCH SUCCESS.

4.

~~ABYD~~

ABYDPZL JSN

To decrypt a vegenere cipher we need to use the key in backward direction to the left.

W	I	S	H	I	N	G	Y	O	U	M	U	C	H	S	U	C	C	G	S	S
4	19	3	22	7	12	5	11	4	19	3	22	7	12	5	11	04	19	3	22	7

ABYDPZL JSN PQJT XFGVHOZ

(2) Hill Cipher.

It is a p cipher, as vegenere cipher the plain text ~~sa~~ is broken into blocks of size m.
where m is a linear eq^n.
the key in hill cipher is an $(m \times m)$ matrix of integers 0 to 25.

Each alphabet is assigned with a numeric value $A=0$, $B=1$, ... $Z=25$.

The relationship b/w block of plain text & its cipher text is expressed by $C_1 = P_1 K_{11} + P_2 K_{21} + \ldots + P_m . K_{m1}$ mod 26.

~~$C_2 = P_2 k_{21} +$~~

$$C_2 = P_1 K_{12} + P_2 K_{22} + \ldots P_m k_{m2} \text{ mod } 26.$$

$$C_m = P_1 K_{1m} + P_2 K_{2m} + \ldots P_m K_{mm} \text{ mod } 26.$$

i.e = $C = P.K.$ $K = (m \times m)$ matrix.

K represents a key comprising of $(m \times m)$ square matrix.

At the receiver end, the plain text can be recovered from cipher text using "$P = C.K^{-1}$".

Note : $K.K^{-1}$ = Identity Matrix.
Every time the inverse of matrix doesn't exist if the matrix is random value.

Calculation of Inverse of Matrix.

Consider a in cipher using a block of 2 $(m=2)$ where key = ~~(3, 7, 15, 12)~~ $\begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$.

Perform encryption of plain text HI.
The numerical equivalent of HI is 78.

$C = p.K.$

$C = \begin{bmatrix} 7 & 8 \end{bmatrix} \begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$

$C = \begin{bmatrix} \cancel{16}\,21+120 & 49+96 \end{bmatrix}$

$C = \begin{bmatrix} 141 & 145 \end{bmatrix}.$ mod 26.

$(11 \quad 15)$
$C = \begin{bmatrix} L & P \end{bmatrix}$

Decryption process.

~~$P = C.K^{-1}$~~ $\qquad K^{-1} = \begin{bmatrix} 10 & 5 \\ 7 & 9 \end{bmatrix}$
$P = C.K^{-1}.$

$P = \begin{bmatrix} 11 & 15 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 7 & 9 \end{bmatrix}$

$P = \begin{bmatrix} 110+105 & 55+135 \end{bmatrix}$

$P = \begin{bmatrix} 215 & 190 \end{bmatrix}$ mod 26.

$P = \begin{bmatrix} 7 & 8 \end{bmatrix}.$
$P = \begin{bmatrix} H & I \end{bmatrix}.$

[OTP] One Time Pad.

It is an encryption technique in which each character of the plain text is combined with a character from a random set of key.

In The (OTP) One Time Pad is that the encryption key has atleast the same length as the actual msg (plain text) & consists of truly random numbers and is not reused.

There are some rules mandatory for OTP'

1] The OTP shd consist of truly Random chars.

2] The $\overset{(key)}{OTP}$ shd have the same length of the plain text.

3] Only 2 copies of OTP should exist.

4] The OTP shd be used only once

5] Both copies of OTP are destroyed immediately after use.

~~6]~~

The key is prior sent to the receiver and the encryption is done.

To encrypt plain text data the sender uses keystream by mixing bit by bit [XOR operation]. Again It is XOR operation performed on decryption to get plain text.

Eg: A 0 1 1 0 0 1 0 1

key 1 1 0 1 0 1 0 1

XOR.

CT 1011 0000

key. 1101 0101 (XOR) Decryption.

PT 0110 0101

Hill cipher prob

Perform for a plain text HELP where the block of 2

HELP $m=2$. $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. H E L P.

7 4 11 15.

$C = P \cdot K$

$= \begin{bmatrix} 7 & 4 \\ 11 & 15 \end{bmatrix}_{2\times2} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}_{2\times2}$

$= \begin{bmatrix} 7 & 4 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 21+8 & 21+20 \end{bmatrix}$

$= \begin{bmatrix} 29 & 41 \end{bmatrix}$ mod 26.

$= \begin{bmatrix} 3 & 15 \end{bmatrix} = \begin{bmatrix} D & P \end{bmatrix}$

$$\begin{bmatrix} 11 & 15 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 33+30 & \cancel{45}\ 33+75 \end{bmatrix}$$

$$= \begin{bmatrix} 63 & 108 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 11 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} L & E \end{bmatrix}$$

$= D \quad P \quad L \quad E$

<u>Decryption</u>

$P = CK^{-1}$ $\qquad K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

$$= \begin{bmatrix} 3 & 15 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 45+300 & 51+135 \end{bmatrix}$$

$$= \begin{bmatrix} 345 & 186 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 7 & 4 \end{bmatrix}$$

$= H \quad E.$

$\therefore$ H E L P

$$= \begin{bmatrix} 11 & 4 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 165+80 & 187+36 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 245 & 223 \end{bmatrix} \text{ mod } 26.$$

$$= \begin{bmatrix} 11 & 15 \end{bmatrix}$$

$= L \quad P$

Difference b/w Substitution & Transposition Cipher.

In substitution cipher each letter retains its position but changes its identity.
In transposition cipher each letter retains its identity but changes its position.

Transposition Cipher.

TCipher shuffles, rearranges or permutes the bits in a block of plain text.

Row transposition Cipher

In Rt Cipher the plain text is arranged in the form of matrix for a particular fixed column value.
Eg: "Begin operation at NOON".

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \left[\begin{matrix} B & e & g & i \\ n & o & p & e \\ r & a & t & i \\ o & n & a & t \\ N & O & O & N \end{matrix}\right. & & & \left.\right] \end{array} \Rightarrow \begin{bmatrix} r & a & t & i \\ n & o & o & n \\ n & o & p & e \\ b & e & g & i \\ o & n & a & t \end{bmatrix}$$

Now, let's rearrange the rows as follows:
The 1st row is 3rd row.
The 2nd row is 5th row.
The 3rd row is 2nd row.
The 4th row is 1st row.
The 5th row is 4th row.

Now, rearranging the column as follows:
1st - 4th
2nd - 3rd.
3rd - 1st
4 - 2nd

$$\begin{bmatrix} i & t & r & a \\ n & o & n & o \\ e & p & n & o \\ i & g & B & e \\ t & a & o & n \end{bmatrix}$$

. it ra nono epno igBe taon.

Decipher 1

$$\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & t & r & a \\ n & o & n & o \\ e & p & n & o \\ i & g & B & e \\ t & a & o & n \end{bmatrix} \end{array} \Rightarrow \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & g & B & e \\ e & p & n & o \\ i & t & r & a \\ n & o & n & o \\ t & a & o & n \end{bmatrix} \end{array}$$

To decrypt the message the recipient would have to cast the cipher text in (5x4) matrix and reverse the column & row shuffle.

In the above technique, the message can be changed by identifying some interesting keywords

Decipher 2.

$$\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & g & B & e \\ e & p & n & o \\ i & t & r & a \\ n & o & n & o \\ t & a & o & n \end{bmatrix} \end{array} \Rightarrow \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} r & a & t & i \\ n & o & o & n \\ n & o & p & e \\ B & e & g & i \\ o & n & a & t \end{bmatrix} \end{array}$$

$$\begin{bmatrix} B & e & g & i \\ n & o & p & e \\ r & a & t & i \\ o & n & a & t \\ n & o & o & n \end{bmatrix}$$

Confusion.

Confusion seeks to make the relationship b/w the statistics of the CTxt and the value of encryption key as complex as possible.

Even if the attacker can get some handle on the statistics of CTxt, the way in which the key was used to produce that CTxt is so complex as to make it difficult to deduce the key.

This is achieved by complex substitution theorem.

Diffusion. [Rearrangement].

In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the CTxt.

This is achieved by having each CTxt digit be affected by many Ptxt digits

$$y_n = \left(\sum_{i=1}^{k} m_{n+i}\right) \bmod 26.$$

adding k sucassive letters to get CTxt letter y_n

In a binary block cipher, diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation.

Block Cipher.

It is one in which a block of PTxt is treated as a whole and used to produce a CTxt block of equal length, a block of 64b or 128b is used. A block cipher can be used to achieve the same effect as a stream cipher.

They seem applicable to a broader range of app^ns than stream ciphers.

The majority of n/w based symmetric cryptographic applications make use of block ciphers.

Stream Cipher

It is one that encrypts a digital data stream one bit or one byte at a time.

Eg: Vigenere Cipher.

If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream.

~~Substitution - Perm~~

Product Cipher ~~combines~~

It is a combination of substitution - permutation box.

Substitution Box is a device that takes i/p string of length m & returns string of length n. ~~and the~~

where m = n is occasional not always.

Data Encryption Stds.

In DES, $\boxed{m > n}$

An S-Box is a easily implemented using a table or array of 2^m rows, each row contains n-bit value.

S-Box has no restrictions.

Permutation Box performs permutation or rearrangement of bits in the i/p.

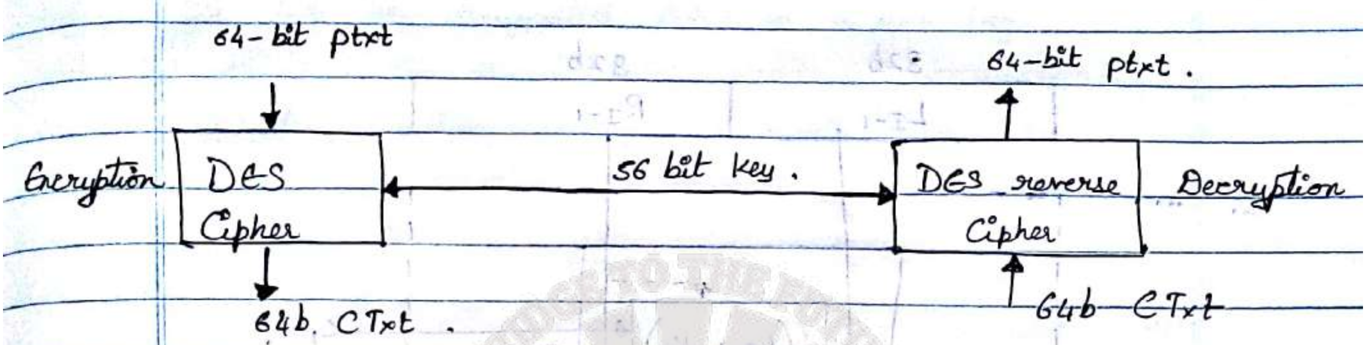
Permutation is more restricted than ~~diffusion~~ substitution.

Cascading P-Box & S-Box alternatively the strength of the cipher can be greatly increased.

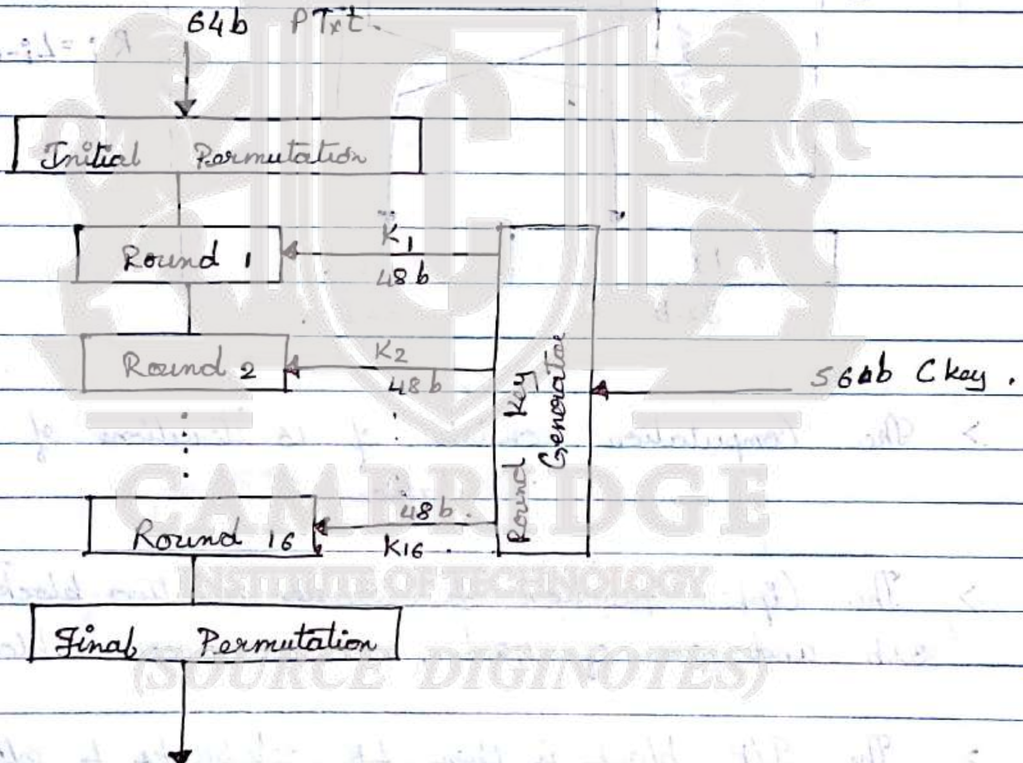
This concept is called product cipher.

DES.

Key : ~~64 bit~~ ~~q~~ 56 bit key.



General Structure of DES.

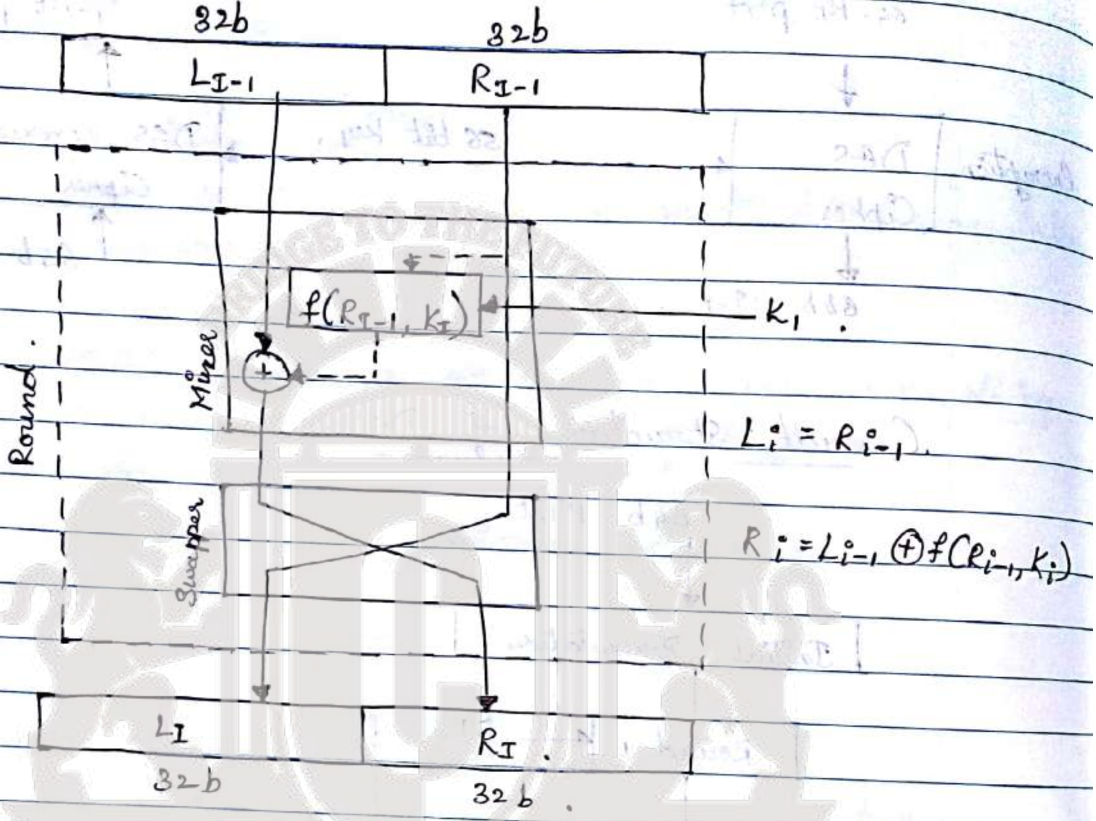


Feistel Cipher Structure.

Implements Shannon's S-P n/w concept where a single block of PTxt is transformed into CTxt after passing through the foll. stages.

- partitions i/p block into two halves.
- An initial permutation.

- 16 rounds of a given function.
- A 32b left-right swap and.
- A final permutation.



> The Computation consists of 16 iterations of a calculation

> The Cipher Function f operates on two blocks, one of 32b and one of 48 b, and produces a block of 32 b

> The I/P block is then LR, 32b blocks L followed by a 32 b block R

Let L_{i-1} & R_{i-1} be the left and right halves of the i/p to round i.

$L_i = R_{i-1}$.
$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$.

> The function f is applied at each round is referred as the "Round Function".

> At each iteration a diff block of key K bits is chosen from the 64b key designated KEY to a 48b key.

Round Function.

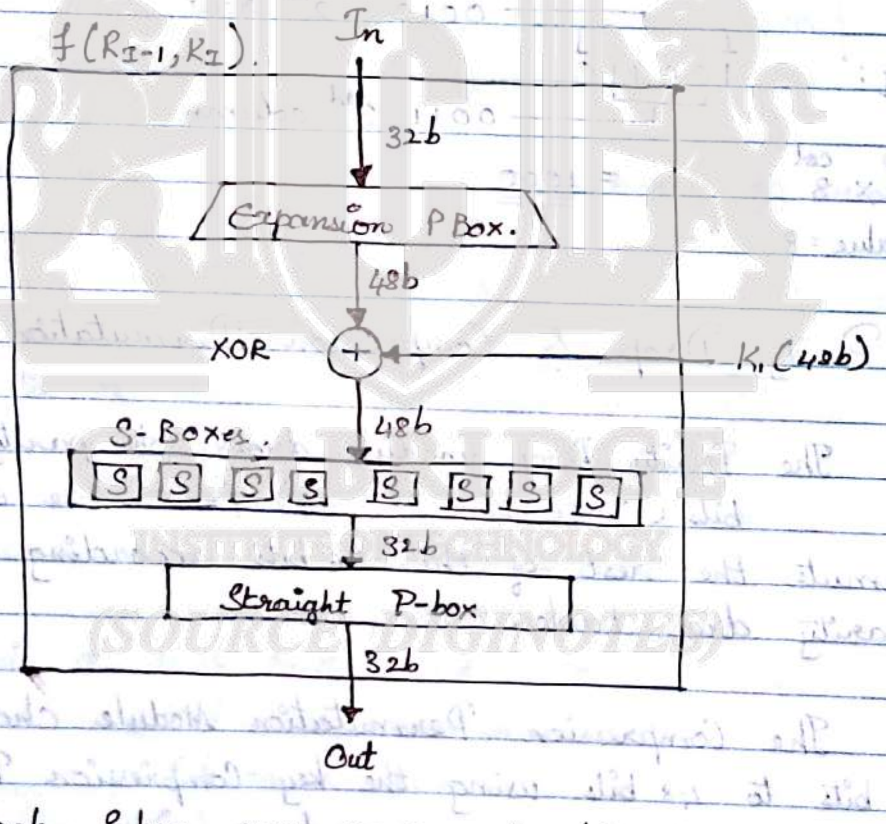
Four operations.

> Expansion.

> XOR with round key.

> Substitution.

> Permutation.



Each S box uses a corresponding 4 row x 16 column table i.e 8 tables. [n^{2n} array]. 2^4

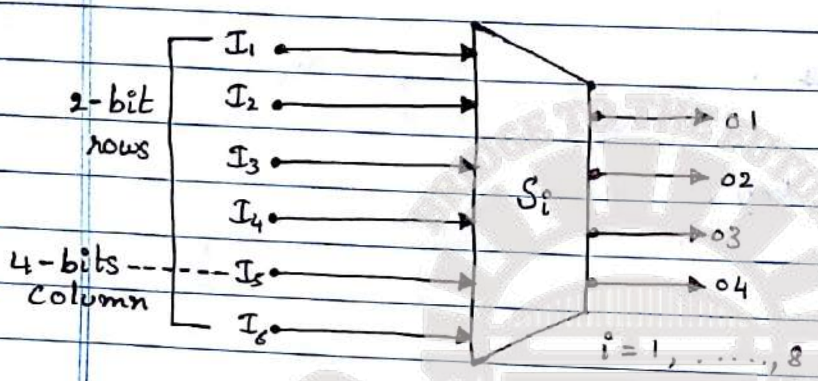
Given a 6 bit i/p, the 1st and 6th bits are used to address one of the rows and the remaining 4 bits are used to address one of the 16 columns.

Finally, the value found in the corresponding location of the table is the 4-bit o/p of the S box.

Substitution Box. [Substitution and Shrink]

48 bits ⇒ 32 bits. $[8*6 \Rightarrow 8*4]$.

2 bits used to select amongst 4 substitutions for the rest of the 4 bit quantity.



Eg : 100110

0010 2nd row.

0011 3rd column.

row col
2 x 3 = 1000

value = 8.

Parity Drop & Compression Permutation

The Parity Drop module drops the parity bits bits (8, 16, 24, ..., 64) from the 64-bit key & permutes the rest of the 56 bits according to the parity drop table.

The Compression Permutation Module changes the 56 bits to 48 bits using the key Compression Table, which are used as the key for a round.

Pabtis

MODULE - 2

Public Key Cryptosystem.

~~The f~~

RSA Operation.

> The first step in the RSA is used to generate a pub key & prt key pair.

This is usually a one-time operation unless an individual needs to obtain a fresh one for security reason.

Key Generation Process of RSA.

1] Choose two large prime numbers of same size p and q.
[Typically each p & q has b/w 512 to 2048 bits].

2] Compute $n = p*q$ and $\phi(n) = (p-1)*(q-1)$.

3] Select e such that $1 \le e \le \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

4] Compute d such that $1 \le d \le \phi(n)$ and
$e*d \equiv 1 \bmod \phi(n)$ or
$e*d \bmod \phi(n) = 1$.
knowing $\phi(n)$ makes d easy to compute.

Euler's $\phi(n)$ (totient). is used for a given +ve integer 'n' i.e $\phi(n)$ is the no. of +ve ints less than or equal to n that are co-prime to n.

Eg: $\phi(8) = 1, 3, 5, 7$. | $\phi(7) = 1, 2, 3, 4, 5, 6$.

$\phi(\text{prime}) = (\text{prime} - 1)$.

Public key = (e, n).
Private key = (d, n).

Encryption

Let m be a plaintext msg for each block m_i the corresponding Cipher text (C_i) is calculated as:

$$\boxed{C_i = m_i^e \bmod n}.$$

Decryption.

Given a block of txt C_i, the corresponding plain text m_i is:

$$\boxed{m_i = C_i^d \bmod n}.$$

Find out the Cipher text & decipher the message "HIDE" using RSA for $p = 3$ $q = 11$. and choose

$p = 3$ $n = 33$
$q = 11$ $\phi(n) = (3-1)(11-1)$
$= 20$.

H	I	D	E
7	8	3	4

$e = 7$

$d = 3$

$C_i = 7^7 \bmod 33$
$= 28$.

$m_i = 28^3 \bmod 33$
$= 21952 \bmod 33$
$= 7$.

H

$7y \equiv 1 \bmod 20$.
$\underline{y = 3}$ (d)

I

$C_i = 8^7 \bmod 33$
$= 2097152 \bmod 33$
$= 2$.

$m_i = 2^3 \bmod 33$
$= 48.\ (2^3)$.

~~$8y \equiv 1 \bmod 33$~~
~~$= 4$~~

$$\left.\begin{aligned} C_i &= 3^7 \bmod 33 \\ &= 2187 \bmod 33 \\ &= 9. \\ m_i &= 9^3 \bmod 33 \\ &= 729 \bmod 33 \\ &= 3. \end{aligned}\right\} D.$$

$$\left.\begin{aligned} C_i &= 4^7 \bmod 33. \\ &= 16384 \bmod 33. \\ &= 16. \\ m_i &= 16^3 \bmod 33. \\ &= 4096 \bmod 33 \\ &= 4. \end{aligned}\right\} E$$

$C_i = m_i^e \bmod n.$ $n = 33$

$= 30^7 \bmod 33.$

$= 30^1 \times 30^2 \times 30^4 \bmod 33$

$C_i = 24.$

H	I	D	E.
7B			

0 1 1 1 1 0 1 1

$30^{40}.$

$m_i = 24^3 \bmod 33$

$= 13824 \bmod 33$

$m_i = 30.$

$5^{500} \bmod \cancel{7}40.$

~~e=7~~

~~d=3.~~

$C_i = 5^{500} \bmod 40.$

500.

✓	✓	✓	✓	✓		✓		
1	1	1	1	1	0	1	0	0
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

$5^{82} \bmod 33 = 25.$

$5^4 \bmod 33 = 625 \bmod 33$

$= 31.$

$5^5 = 5^2 . 5^2 . 5^1$

$2^8 = 256.$

$2^7 = 128.$

$2^6 = 64.$

$2^5 = 32$

$2^4 = 8.$

$2^2 = 4.$

Performance of RSA.

Time Complexity

Encryption

$$C_i = m_i^e \bmod n.$$

$$= O(b^2).$$

Decryption

$$m_i = C_i^d \bmod n$$

$$= O(nb^2)$$

- Both Encryption & Decryption involves repetitive multiplication of b no. of bits.
- Unoptimized multiplication of two b-bit no's & reduction by modulo n (division) which takes $O(b^2)$ time.
- The encryption key is usually small integer e relative to n.
- The time complexity of encryption is $O(b^2)$.
- Decryption on other hand involves raising a b-bit no. to the power of 'd' which implementation of decryption involves d multiplications.
- Since d is same order as n the complexity of decryption operation $O(nb^2)$.

Speeding up RSA.

We can speed up the decryption of Cipher Text by computing,

$$m_i = C_i^d \bmod n.$$

$C, C^2, C^3, C^4, C^8, C^{16}, \ldots$ upto the max of db-bits term.

We multiply elements in this series whose positions corresponds to 1 in the binary representation of the decryption key d.

Ofcourse, each multiplication is mod n multiplication so, the intermediate products are never more than b-bits wide.

This approach with first computes square followed by product is referred as Square and Multiply Technique, which speeds up the decryption concept in RSA.

Eg: Write square & multiplication steps for decryption key = 57.

Dec = 57

$$m_i = C_i^{57} \bmod n.$$

Bin = 111001

1	1	1	0	0	1
2^5	2^4	2^3	2^2	2^1	2^0
$C^{32} \bmod n \times$	$C^{16} \bmod n \times$	$C^8 \bmod n$		$\times$	$C^1 \bmod n$

$$= \underline{C^{32} . C^{16} . C^8 . C^1 \bmod n}.$$

= ~~Applications of RSA~~

$5^{40} \bmod 7$.

40.

1	0	1	0	0	0
5	4	3	2	1	0
32	16	8	4	2	0

~~8^{32}~~

$5^8 \bmod 7 = 4$.

$390625 \bmod 7$ $\qquad$ $5^4 \bmod 7 = 2$.

~~8^{32}~~

$$5^{16} \bmod 7 = (5^8)^2 \bmod 7.$$
$$= 16 \bmod 7 = 2.$$

$$5^{32} \bmod 7 = (5^{16})^2 \bmod 7.$$
$$= 4 \bmod 7 = 4.$$

$5^{40} \bmod 7$.

$$= (5^{32} \times 5^8) \bmod 7$$
$$= 4 \times 4 \bmod 7.$$
$$= 16 \bmod 7,$$
$$= \underline{\underline{2}}.$$

Applications of RSA.

Providing msg confidentiality, msg integrity and authentication.

In summary, the principle drawback of pub key cryptography is speed,
while the principle ~~of~~ drawback of secret key cryptography is key management,
To combine (the speed of secret key cryptography & the convenience of public key cryptography, a session key is used.

Choose a fresh random no. 'S' as the secret key. This is referred to as session key.

The sender:

- Encrypts the msg with session key. $[E_S(m)]$.
- Encrypts the session key with the recipient's public key. $[E_{B.pu}(S)]$.
- Sends the encrypted msg & the encrypted session key in the same msg.

The receiver.

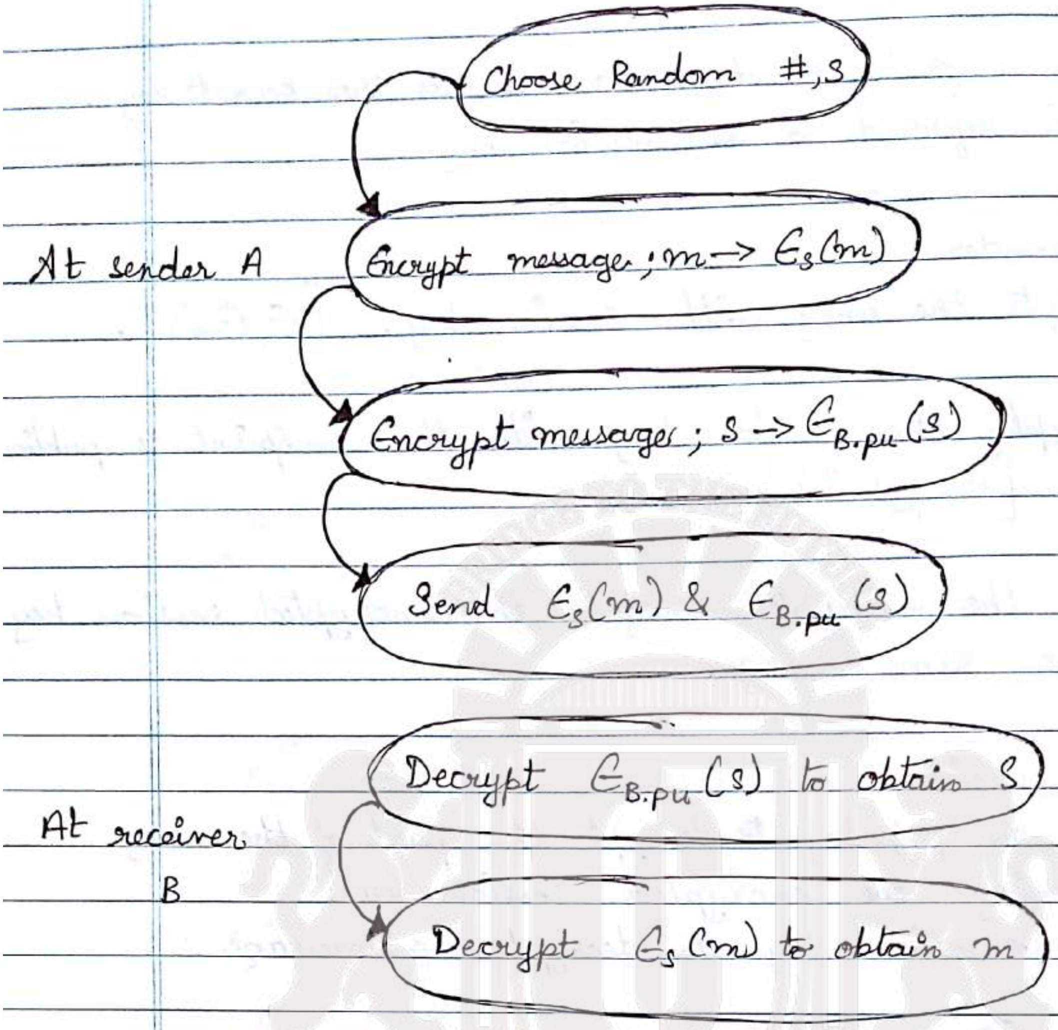
- Uses his pvt key to decrypt the part of the msg containing the encrypted session key.
- Uses the session key to decrypt the message.

$$S = [D_{B.pr}(S)]$$

$$m = [D_S(C)]$$

The session key is used to encrypt/decrypt the remaining msg in that session.
The session key is valid for the duration of the session & destroyed thereafter.

Encrypted message with encrypted session key.


Choose Random #, S
At sender A
Encrypt message; m -> E_S(m)
Encrypt messages; S -> E_B.pu(S)
Send E_S(m) & E_B.pu(S)
Decrypt E_B.pu(S) to obtain S
At receiver B
Decrypt E_S(m) to obtain m

~~35 = (1, 5, 7)~~

Practical issues.

i] Generating primes.

Other attacks.

i] Modular Factorisation.

Factoring a no. means representing it as the product of prime no's. A number is said to be factored when all of its prime factors are identified.

As the ~~sig~~size of the no. increases the difficulty of the factoring ~~a~~ increases rapidly.

Pollard rho algorithm is an algorithm used for factoring no's, other best known factorisation algorithms are

-> Quadratic Sieve -> Elliptic Curve -> General no. field sieve [GNFS].

Small Exponent attack.

Side - Channel Attack. -> time & power

Compute

23/02/18

Compute Inverse (b,c) // compute inverse of c mod D.

```
{
  old1 = 1        new1 = 0
  old2 = 0        new2 = 1
   b' = b          c' = c
   r = 2
  while (r>1)
  { q = b'/c'.
     r = b'%c'.
     t1 = old1 - new1 *q.
     old1 = new1
     new1 = t1
     t2 = old2 - new2 *q.
     old2 = new2
     new2 = temp2
     b' = c'
     c' = r
     // At this point new1 *b + new2*c = r
  }
  return new2
}
```

Find out the inverse for 12 mod 79.
or Compute gcd (12,79)

Inverse for 12.

12^{-1} mod 79. [Done before].

$12y \equiv 1 \bmod 79$.

Perform gcd on (622, 289).

~~622~~ , ~~289~~

x. Find gcd of (1070, 1066) using Euclidean algorithm.

1070 1066.

$^{2}2\overset{2}{6}6$
$\times 4$
1064

$1070 = 1066(1) + 4.$

$1066 = 4(266) + \boxed{2}$

$4 = 2(2) + 0.$

→ An integer n which lies b/w $0 \le n < 210$ satisfies the follg set of congruences.

~~4~~ $n \bmod 5 = 4.$

~~3~~ $n \bmod 6 = 3.$

~~2~~ $n \bmod 7 = 2.$

[CRT]

$n \equiv 4 \bmod 5.$ $M = (5 \times 6 \times 7) = 210.$

$n \equiv 3 \bmod 6.$ $M_1 = \frac{210}{5} = 42.$

$n \equiv 2 \bmod 7.$

$M_2 = \frac{210}{6} = 35$

1] $42y \equiv 1 \bmod 5.$

$2y \equiv 1 \bmod 5.$ $M_3 = \frac{210}{7} = 30.$

M_1^{-1} $\underline{y = 3}$

2] $35y \equiv 1 \bmod 6.$ 3] $30y \equiv 1 \bmod 7.$

M_2^{-1} $\underline{y = 5}.$ M_3^{-1} $2y \equiv 1 \bmod 7.$

$\underline{y = 4}.$

68 .3

$n = (4 \times \overset{42}{\cancel{210}} \times 3 + 3 \times 3\overset{5}{\cancel{6}} \times \overset{5}{\cancel{1}} + 2 \times 30 \times 4) \bmod 210.$

~~$n = (504 + 108 + 240) \bmod 210.$~~

~~$n = 852 \bmod 210.$~~ $35y \equiv 1 \bmod 6.$

$n = 1269 \bmod 210.$ $5y \equiv 1 \bmod 6.$

$\underline{n = 9}$ $\underline{y = 5}.$

Extended Euclidean.

$2 = 1066 - 4 * 266.$

$2 = 1066(1) - (1070 - 1066 * 1) * 266.$

$= 1066 * 267 - 1070 * 266.$

Perform transposition Cipher technique on the plain text "SECURE YOUR NETWORK NOW" by using row major form. (column = 5). & By performing row transposition, column transposition & row transposition.

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \hline \left[\begin{matrix} S & E & C & U & R \\ E & Y & O & U & R \\ N & E & T & W & O \\ R & K & N & O & W \end{matrix}\right] \end{array}$$

Row Transpose. $\begin{bmatrix} S & E & N & R \\ E & Y & E & K \\ C & O & T & N \\ U & U & W & O \\ R & R & O & W \end{bmatrix}$ Colm. Transpose. $\begin{bmatrix} S & E & C & U & R \\ E & Y & O & U & R \\ N & E & T & W & O \\ R & K & N & O & W \end{bmatrix}$

2nd row Transpose $\begin{bmatrix} S & E & N & R \\ E & Y & E & K \\ C & O & T & N \\ U & U & W & O \\ R & R & O & W \end{bmatrix}$

→ What is the relation b/w RSA encryption & decryption key?

$$d = e^{-1} \bmod \phi(n).$$

→ Find out the value of d if $n = 77$ and $e = 7$.

$n = 7 \times 11$ $p = 7$ $q = 11$.

$\phi(n) = (p-1)(q-1)$

$(7-1)(11-1)$

$p = 7$

$q = 11.$

$\phi(n) = 6 \times 10$
$= 60.$

$7y \equiv 1 \bmod 60.$

$60 \times 6 = 360$ $1y \equiv 43 \bmod 60.$

$350.$ $\underline{\underline{y = 43}}.$

26/02/18 **Cryptographic Hash.**

A cryptographic hash function $h(x)$ maps a binary string of arbitrary length to a fixed length binary string.

The properties of hash illustrates one way property. Given hash value 'y' it is computationally infeasible to find the input x such that $h(x) = y$.

Weak collision resistance:

Given an i/p value x_1, it is computationally infeasible to find another i/p value x_2 such that $h(x_1) = h(x_2)$. Time Complexity $O(2^{w})$.

Strong collision resistance.

It is computationally infeasible to find two input values x_1 & x_2 such that $h(x_1) = h(x_2)$.

Confusion + Diffusion.

If a single bit in the i/p stream is fixed then each bit of the hash value is flipped with probability roughly equal to 0.5.

Challenge

There is a fine difference b/w two collision resistance properties.

In the first, the hash designer chooses x_1 & challenges anyone to find x_2 where the hash values are same $h(x_1) = h(x_2)$.

The attacker tries to find x_1 & x_2 such that $h(x_1) = h(x_2)$.
In the 2nd challenge, the attacker has the ability to choose x_1

Side Channel attack in RSA

It is based on montioring of time & power consumption of a cryptographic algorithm on a device.

These attacks are quite successful in leaking sensitive info. such as secret / private keys. especially in the case of embedded device such as smart cards, credit cards, etc....

The attacker induces the card to perform cryptographic tasks involving the stored private key.

It is not possible for the attacker to inspect the contents of register & RAM during smart card operation.

So, there are inexpensive equipments available that enables ~~him~~ the attacker to connect smart card via probes to equipment that can accurately monitor variables such as timing & power consumption.

```
~~For~~ Given d, n, c
~~x=c~~ //want $c^d$ mod n
        $x=c$
        for ( $i=k-2$ ; $i \geq 0$ ; $i--$ )
          $x = x^2$ mod n
          if( $d_i == 1$ )
            $x = x \times c$ mod n
          return (x)
```

SHA-1 [Secured Hash Algorithm]

It is a cryptographic hash function which takes i/p & produces 160 bit o/p.

The hash value known as message digest typically represented in hexadecimal number total 40 digits long.

If a single bit in the msg is flipped, the SHA-1 recomputes 84 bits of 160 bits are flipped for a new hash value.

Attack Complexity.

Weak Collision Resistance.

How long will it take to find input x that hashes to a given value y? [Brute force].

```
do
  {  Generate random no. x'
        Compute  h(x')
   }
    while (h(x') != y)
      return (x').
```

Assume that ω is the length of the bits of the string It follows that the above loop would have to run on the average $2^{\omega-1}$ before finding x'.

Therefore, the brute force attack for one way function property & weak collision resistance takes $O(2^{\omega})$.

Strong Collision Resistance.

Given S is a set of i/p string and hash value pair. [Brute force].

```
notFound = true
while(notFound)
{ generate a random string x'
  search for a pair (x,y) in S where x=x'
  if(no such pair exists in S)
   { compute y'=h(x')
       search for a pair (x,y) in S where y=y'
       if(no such pair exists in x)
          insert (x',y') into S
       else
           notFound = false
  }
return (x and x')
```

Birthday Analogy.

What is the minimum no. of persons require so that the probability of two / more in the group having the same birthday is greater than 50%.

23 persons. $\frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \ldots$

It is known that in a class of 23 individuals there is greater than 50% chance the birthday of atleast two persons coincide. This is birthday paradox.

The random string generated for strong collision resistance is analogous to the random individuals in the birthday paradox.

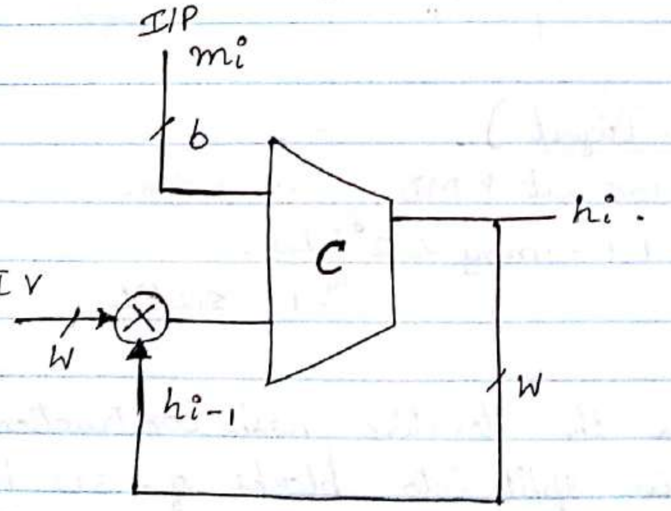
The birthday of randomly chosen individual is analogous to the hash value of randomly chosen string.

Construction of Cryptographic hash.

Generic of cryptographic hash.

C is a ~~composition~~ compression function, IV represents intialization vector, m_i = i^{th} block of message m, h_i=hash value after i^{th} iteration.

Iterative construction of cryptographic hash.



This was introduced by "Merkel & Damgard."

The i/p to a cryptographic function is a message or document to acconodate i/p's of arbitrary length Hash functions uses iterative construction as shown in the figure.

[.

Normally MD5f ~~or~~ & SHA1 ,
C is a ~~comparison~~ compression box which accepts two binary strings of length of b and ω and produces the output of length ω, where b = block size of the i/p & ω = is the width of the hash digest.

The diagram performs operations and produces operations like $h_1 = C(IV, m_1)$
$h_i = C(IV, m_i)$

During first iteration the multiplexer at the second i/p accepts a predefined IV & the top i/p is the first block of the message.

Subsequently for all iterations the partial hash output is fed back as the second i/p to the C box and the top i/p is derived from the successive blocks of message. This is repeated until the complete blocks ~~in~~ of the message is processed.

MD (Message Digest).

SHA-1. ⇒ 160 bit o/p MD. I/P random.

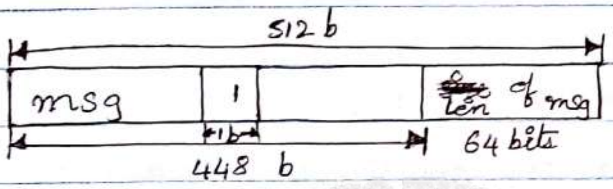
$PT = msg < 2^{64}$ bit.

$(2^{64}-1)$ 512 bits

→ SHA-1 uses the iterative hash construction.
→ The msg is split into blocks of 512 bits.
→ Plain txt or msg should be less than 2^{64} bits.

-> The length of the msg is expressed in binary as ~~to~~ a 64-bit number and is appended to the msg.

-> B/W the msg & the length field, a pad is inserted so that the length of the block is a multiple of 512 block size. i.e (msg + pad + length).



Padding is a process of adjusting the message ~~so~~ so its length is (448 mod 512).

Padding bit '1' followed by remaining zeroes.

Description of SHA-1 Algorithm.

Initialize an array such that each block is split into 16 words each of 32 bits.

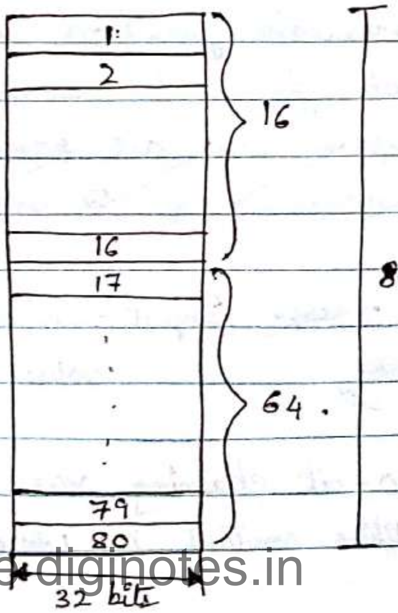
512 / 32 = 16.

These 16 words populate the first 16 positions of an array of 80 words.

The remaining 64 words are obtained from

$$\boxed{W_i = W_{i-3} \oplus W_{i-8} \oplus W_{i-14} \oplus W_{i-16}}$$ where $16 < i \leq 80$.

~~Hash Comp~~



Padding.

Step-1 : append padding bits.

Padding : Given an m-bit message, a single bit '1' is appended as the m+1th bit and then

(448 − (m+1)) mod 512 (b/w 0 & 511) zero bits are appended, making the result as multiple of 512 bits long. (length ≡ 448 mod 512) The padding pattern is 100.....00.

Step-2 : append length.

A 64-bit length in bits of the original message is appended.

Step-3 : Initialize MD buffer.

A 160-bit buffer is used to hold intermediate and final results of the hash function.

The buffer is represented as (5) 32-bit registers (A, B, C, D, E) initialized to the ~~follg~~ initial integers (hex values).

The values are stored in big-endian order, i.e, the most significant byte of a word in the low address byte position.

Step-4 : process msg in 512 bit (16 word) blocks.

A compression function with 4 rounds of processing of 20 steps each for each round operation.

~~The O/P of the last round is added to the input of the first round. (CV$_q$) to produce (CV$_{q+1}$).~~

~~Compression theory~~: Input − 512 bit block Y$_q$, 160-bit buffer
~~[illegible]~~ : value CV$_q$ represented by ABCDE.

Output − 160-bit chaining var. CV$_q$+1 makes use of additive constant K_t where $0 \le t \le 79$.

~~Step.~~ ~~Name~~ ~~Fintion.~~

1) The o/p of the last round is added to the i/p of the
4] first round.
3]

SHA-1 compression function.

Each round consists of 16 steps operating on the buffer ABCDE with each step of ~~t~~ the form:

$$[(E + f(t,B,C,D) \underset{\substack{\downarrow\\ A}}{+} (A<<5) + W_t + K_t), \underset{\substack{\downarrow\\ B}}{A}, \underset{\substack{\downarrow\\ C}}{(B<<30)}, \underset{\substack{\downarrow\\ D}}{C}, \underset{\substack{\downarrow\\ E}}{D})]$$

~~The f 16 words of current block the of arising~~

~~8 The overall~~

where,

A, B, C, D, E = the 5 words of the buffer

t = step no, $0 \leq t \leq 79$..

$f(t, B, C, D)$ = primitive logical function for step t.

w_t = a 32-bit word derived from the 512-bit i/p block.

K_t = an additive constant, 4 distinct values are used.

$+$ = addition modulo 2^{32}.

Primitive functions $f(t, B, C, D)$:

Input is 3 32-bit words.

Output is 1 32-bit word.

Each function performs a set of bitwise logical operations as shown below.

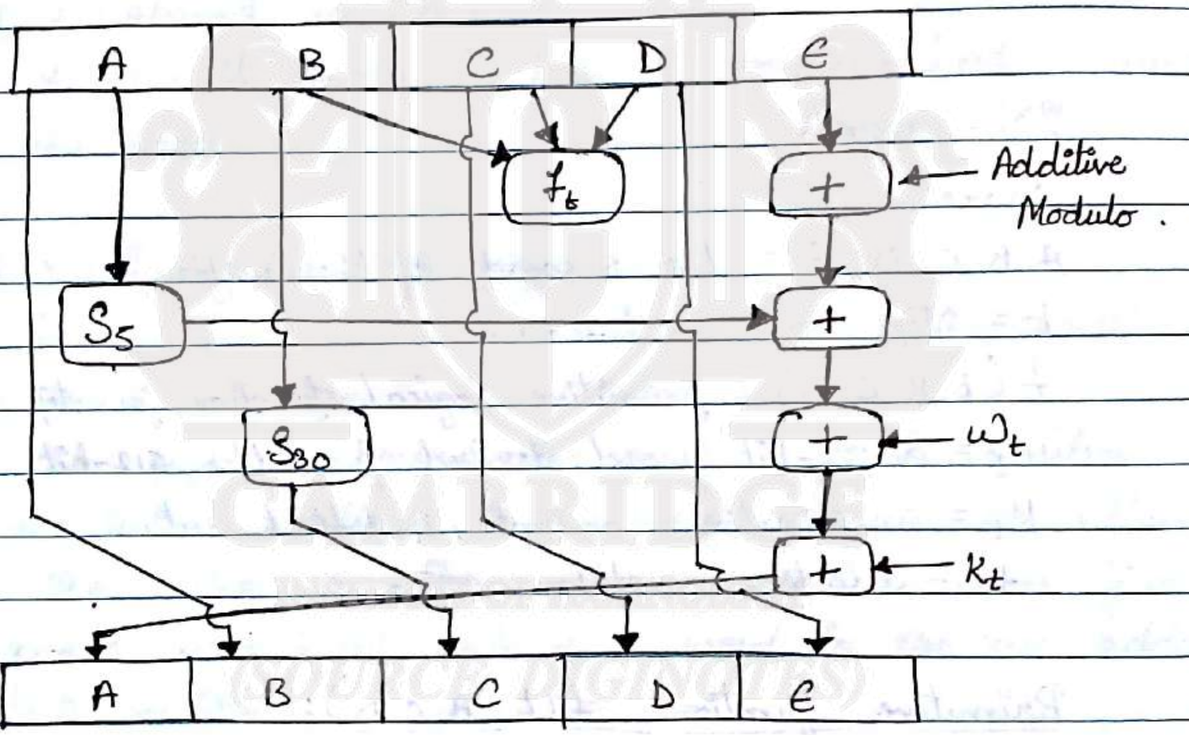
Step	Function name	Function value.
$(0 \leq t \leq 79)$	$f_1 = f(t,B,C,D)$	$(B \wedge C) \vee (\overline{B} \wedge D)$
$(20 \leq t \leq 39)$	$f_2 = f(t, B,C,D)$	$B \oplus C \oplus D$
$(40 \leq t \leq 59)$	$f_3 = f(t,B,C,D)$	$(B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
$(60 \leq t \leq 79)$	$f_4 = f(t, B, C, D)$	$B \oplus C \oplus D$

Derivation of the 32-bit word W_t from the 512-bit i/p block.

The 1st 16-values of W_t are taken directly from 16 words of the current block. The remaining values are defined as follows:

$$W_t = W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}$$

Overall operation of SHA-1



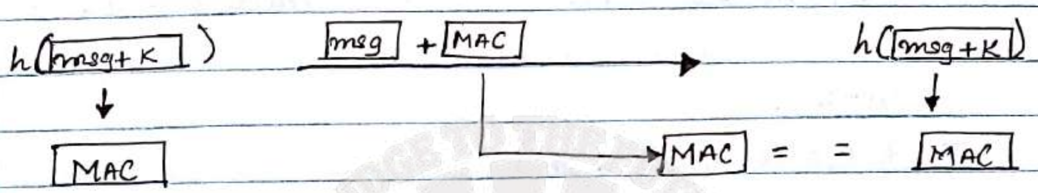
The final value is obtained by adding the initial value with the final value.
(Addition means mod 2^{32}).

2^{32} -> because a 32 bit register can store 2^{32} values.

Applications of Hash.

1] MAC. [Message Authentication Code].

Plaintext.



MAC is used to provide message integrity as well as message authentication.

The cryptographic hash applied on a message creates a digest or digital fingerprint of that message.

The sender & the receiver share a common secret key 'K'.

The message and the key are concatenated and perform hash operation on that string.

This hash value is the fingerprint of that message (M) and key.(K).

That is $MAC = h(M \| K)$

MAC is just a checksum of the message computed and sent to the receiver with the message.

The receiver receives message + MAC, the receiver again computes the MAC with the secret key.

The received MAC and the generated MAC are compared, if its not equal the result is mismatched, he assumes the message is changed.

If the result is matched, the sender of the message is correct i.e source authentication and the message has not been corrupted or tampered within transit which provides message integrity.

$Z = \{1, 3, 5, 7\}$.

$3^1 = 3 \bmod 8 = 3$. $\quad$ $5^1 = 5 \bmod 8 = 5$.

$3^2 = 9 \bmod 8 = 1$. $\quad$ $5^2 = 25 \bmod 8 = 1$.

$3^3 = 27 \bmod 8 = 3$. $\quad$ $5^3 = 125 \bmod 8 = 5$.

$3^4 = 81 \bmod 8 = 1$. $\quad$ $5^4 = 5^4 \bmod 8 = 1$.

$n = 7$.

$Z = \{1, 2, 3, 4, 5, 6, \cancel{7}\}$.

$2 = 2 \bmod 7 = 2$. $\quad$ $3 = 3 \bmod 7 = 3$.

$2^2 = 4 \bmod 7 = 4$. $\quad$ $3^2 = 9 \bmod 7 = 2$.

$2^3 = 8 \bmod 7 = 1$. $\quad$ $3^3 = 27 \bmod 7 = 6$.

$2^4 = 16 \bmod 7 = 2$. $\quad$ $3^4 = 81 \bmod 7 = 4$.

$2^5 = 32 \bmod 7 = 4$. $\quad$ $3^5 = 243 \bmod 7 = 5$.

$2^6 = 64 \bmod 7 = 1$. $\quad$ $3^6 = 729 \bmod 7 = 1$.

$3^7 = 2187 \bmod 7 = 3$.

$\therefore$ 3 is a generator as it contains all elements.

$4 = 4 \bmod 7 = 4$.

$4^2 = 16 \bmod 7 = 2$.

$4^3 = 64 \bmod 7 = 1$.

$4^4 = 256 \bmod 7 = 4$.

$4^5 = 1024 \bmod 7 = 2$.

Diffie Hellman Key Exchange. (DHKE)

DHKE algorithm was invented by Diffie and Hellman in 1976 used to exchange info. b/w two parties shared ~~&~~ with a secret of a particular time duration, which is a private key and a corresponding public key concept. It is symmetric key.

1] Choose two numbers i.e 'p' and 'g' where 'p' is a prime number and 'g' is a generator of that prime number.

2] It is also known that 'g' acts as base value.
'p' acts as modulus.

Sender Side Key generation (A)

Sender generates ~~a~~ or chooses a random integer a such that a lies b/w $1 < a < p-1$ and computes a partial key.

$$K_A = g^a \bmod p.$$

Receiver Side (B)

Receiver chooses a random integer b such that b lies b/w $1 < b < p-1$ and computes a partial key.

$$K_B = g^b \bmod p.$$

-> A sends the computed partial key ~~to~~ ~~B~~ K_A to B and B sends the computed partial key ~~to~~ K_B to A.

-> On receiving the partial keys, A computes $(K_B)^a \bmod p$. and B computes $(K_A)^b \bmod p$.

-> These both will generate a equal value.

Let $p = 131$ and $g = 2$.
choose random number $a = 24$ $b = 17$.
find K_A & K_B.

$(K_A)^b \bmod p$ $\qquad\qquad$ $(K_B)^a \bmod p$.

$(g^a \bmod p)^b \bmod p$. $\qquad\qquad$ $(g^b \bmod p)^a \bmod p$.

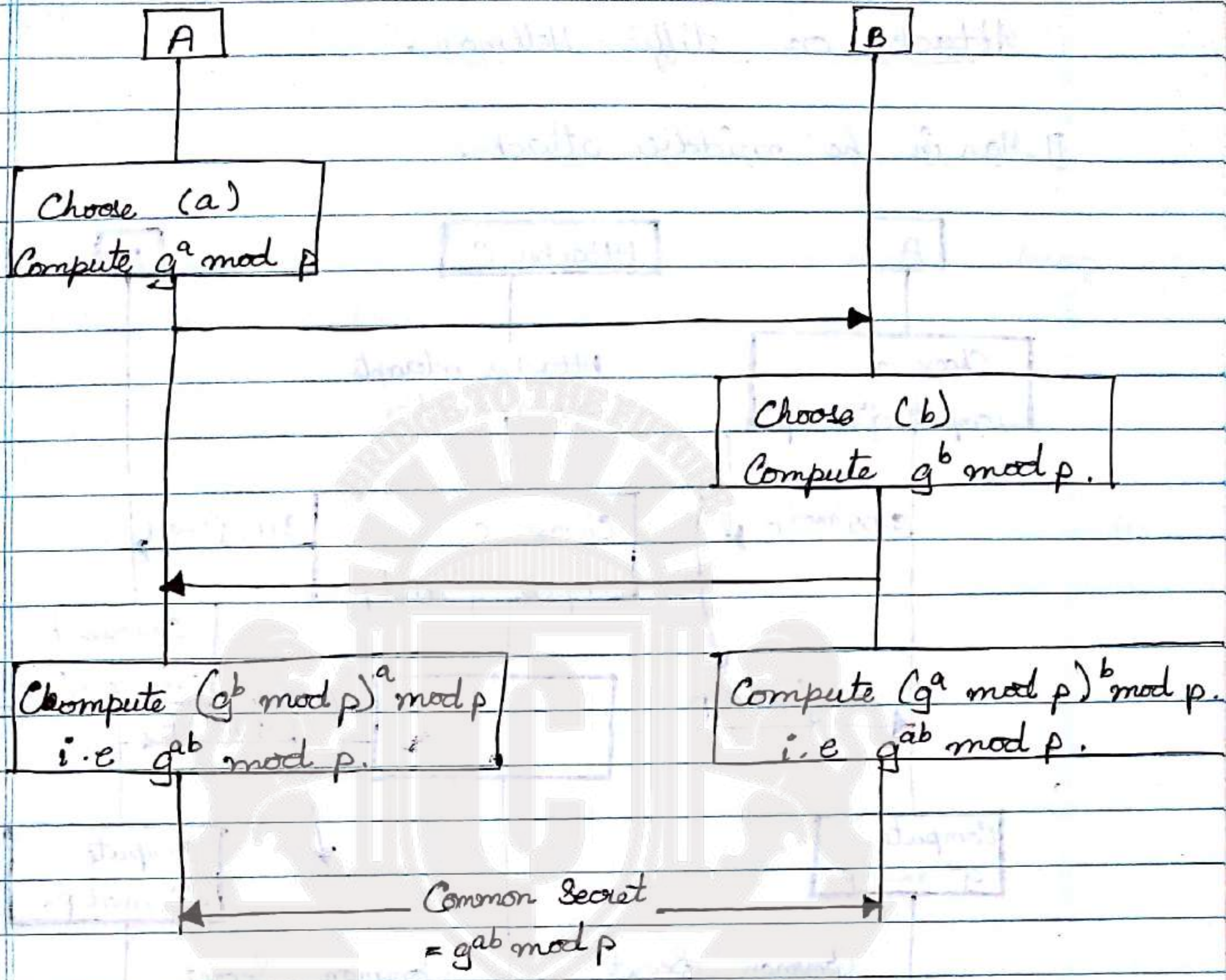
$g^{ab} \bmod p$ $\qquad\qquad$ $g^{ba} \bmod p$.

$g^a \bmod p \Rightarrow 2^{24} \bmod 131$ $\qquad\qquad$ $g^b \bmod p \Rightarrow 2^{17} \bmod 131$.

$= 46$ $\qquad\qquad$ $= 72$.

$(K_A)^b \bmod p$

$= (46)^{17} \bmod 131$.



$p = 11$ $g^a \bmod p = 5$. $y = g^a \bmod p$.

$g = 7$ $g^b \bmod p = 3$. $a = \log_g y \bmod p$.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

$x = \log_7$

$7^1 \bmod 11 = 7$. $a = 2$.

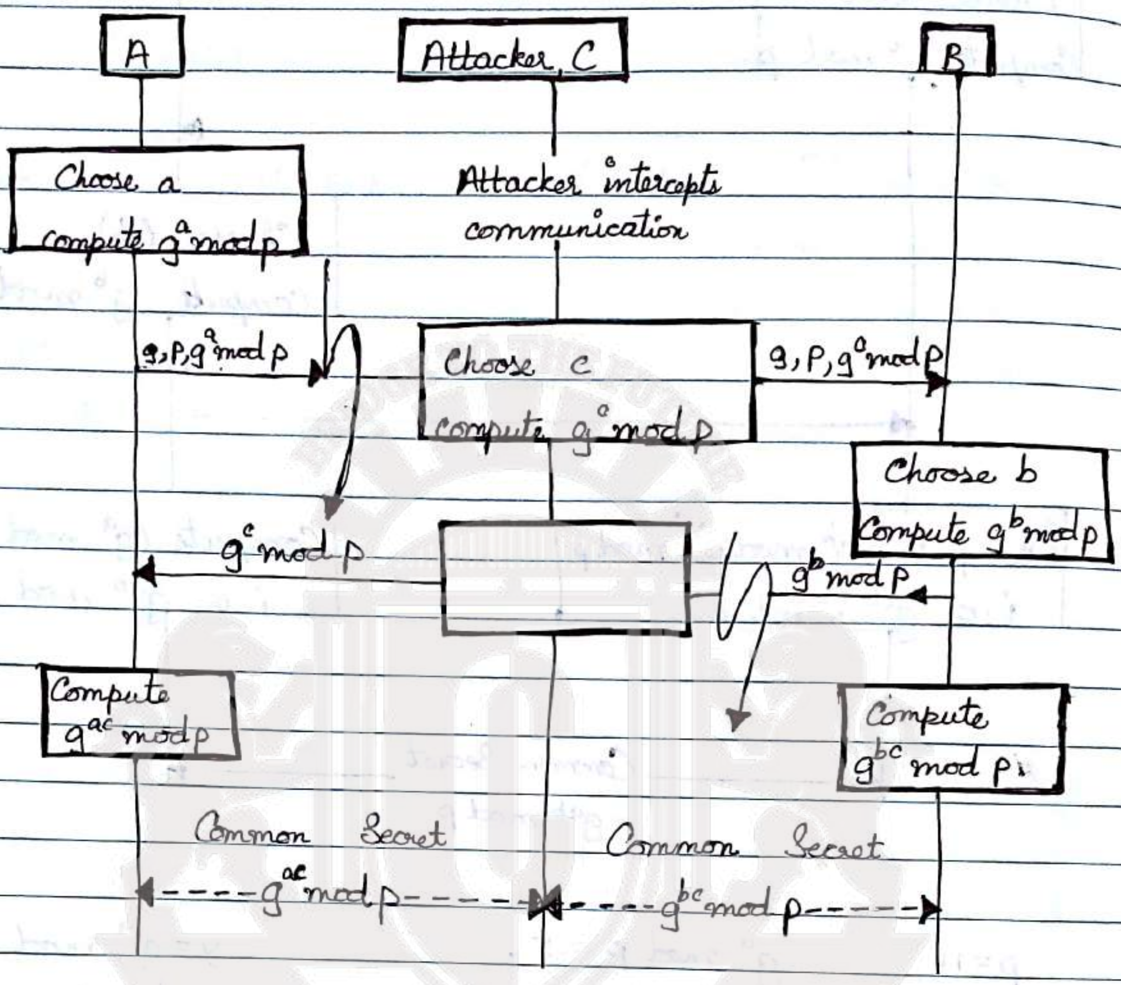
$7^2 \bmod 11 = 5$. $b = 4$.

$7^3 \bmod 11 = 2$.

$7^4 \bmod 11 = 3$.

Attacks on diffie Hellman.

1] Man in the middle attack.



* Sender 'A' chooses a random integer 'a' and computes g^a mod p and sends it to the receiver B.

* Attacker 'C' intercepts the communication and chooses a random integer c and computes g^c mod p and sends it to B.

* ~~B~~ Receiver B unaware of C receives g^c mod p and chooses a random integer b then computes g^b mod p and sends it to ~~B~~ A.

* Again Attacker C intercepts the communication chooses a~~n~~ random integer 'c' then computes g^c mod p and sends it to A.

* ~~&~~ A then ~~sor~~ receives g^c mod p then computes g^{ac} mod p

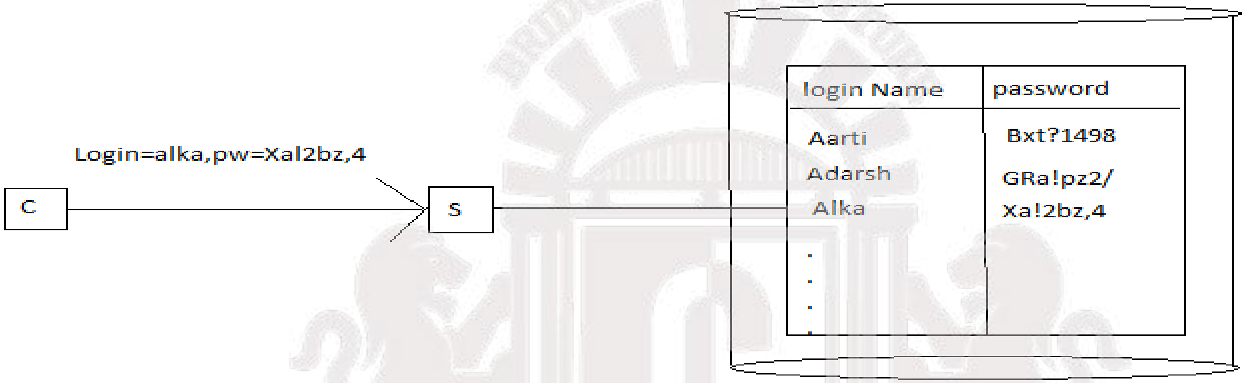
* B also computes g^{bc} mod p.

* Both the keys are secret and are shared between A and B.

AUTHENTICATION -1

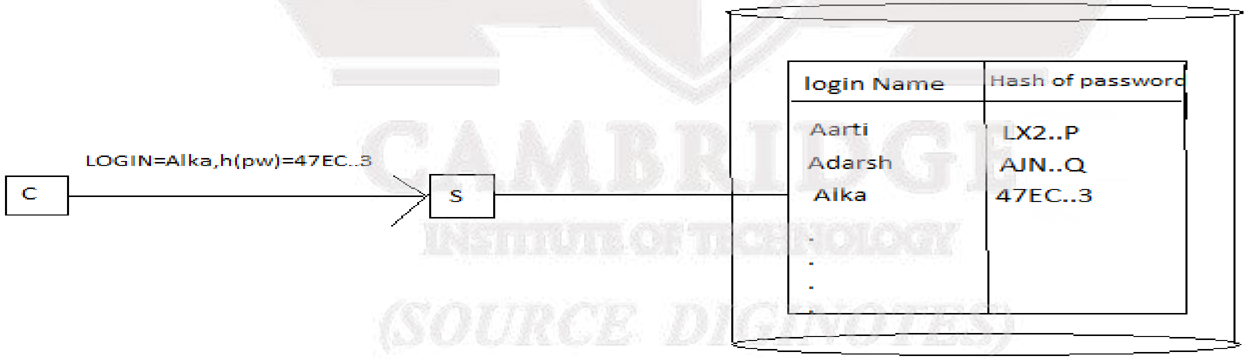
- ONE WAY AUTHENTICATION
- PASSWORD BASED AUHTENTICATION
- CERTIFICATION BASED AUHTENTICATION
- MUTUAL AUHTENTICATION
- DICTIONARY ATTACKS

1.PASSWORD BASED AUHTENTICATION



login Name	password
Aarti	Bxt?1498
Adarsh	GRa!pz2/
Alka	Xa!2bz,4
.	
.	
.	
.	

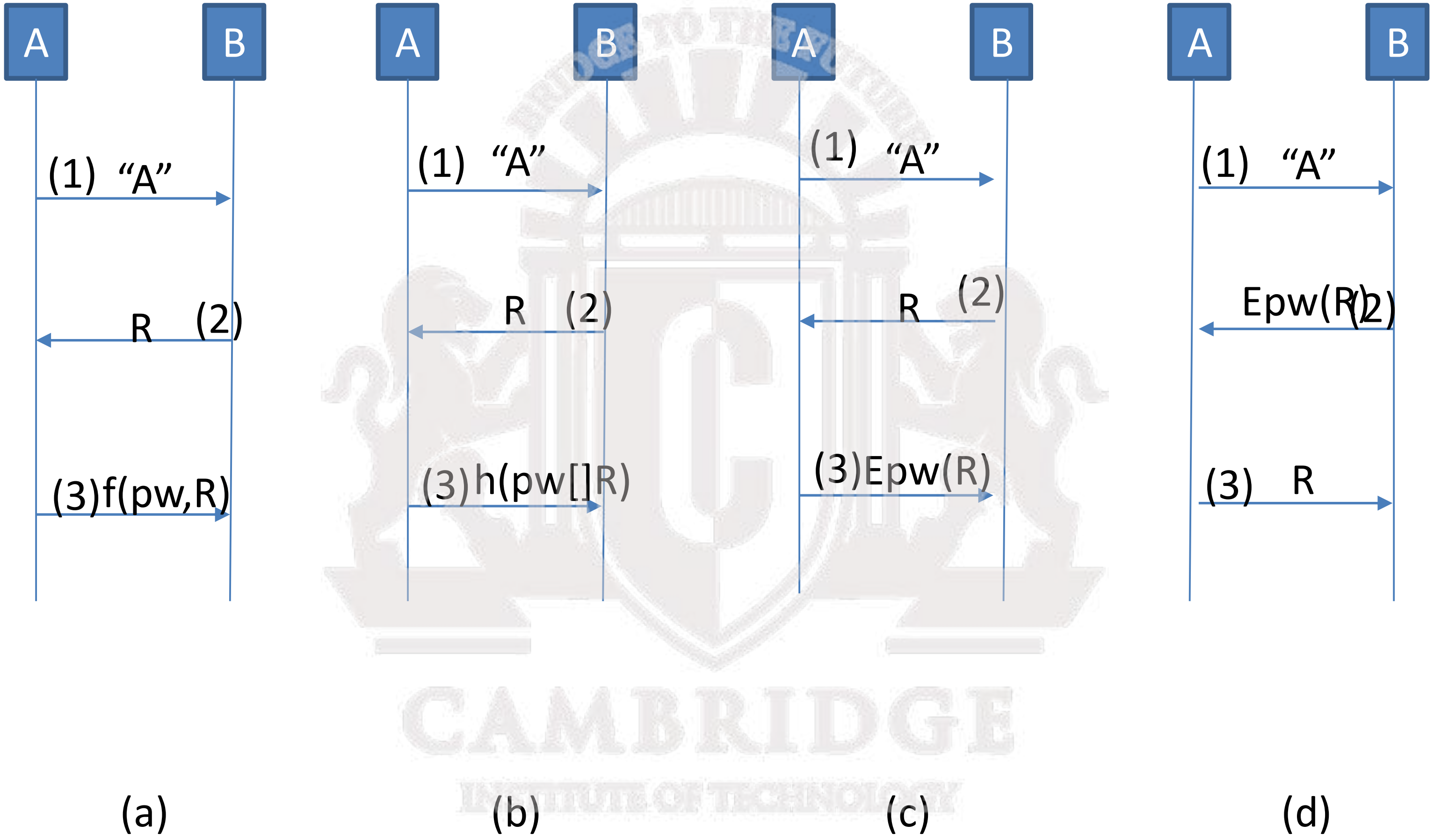
(A) Communicating password



login Name	Hash of password
Aarti	LX2..P
Adarsh	AJN..Q
Alka	47EC..3
.	
.	
.	
.	

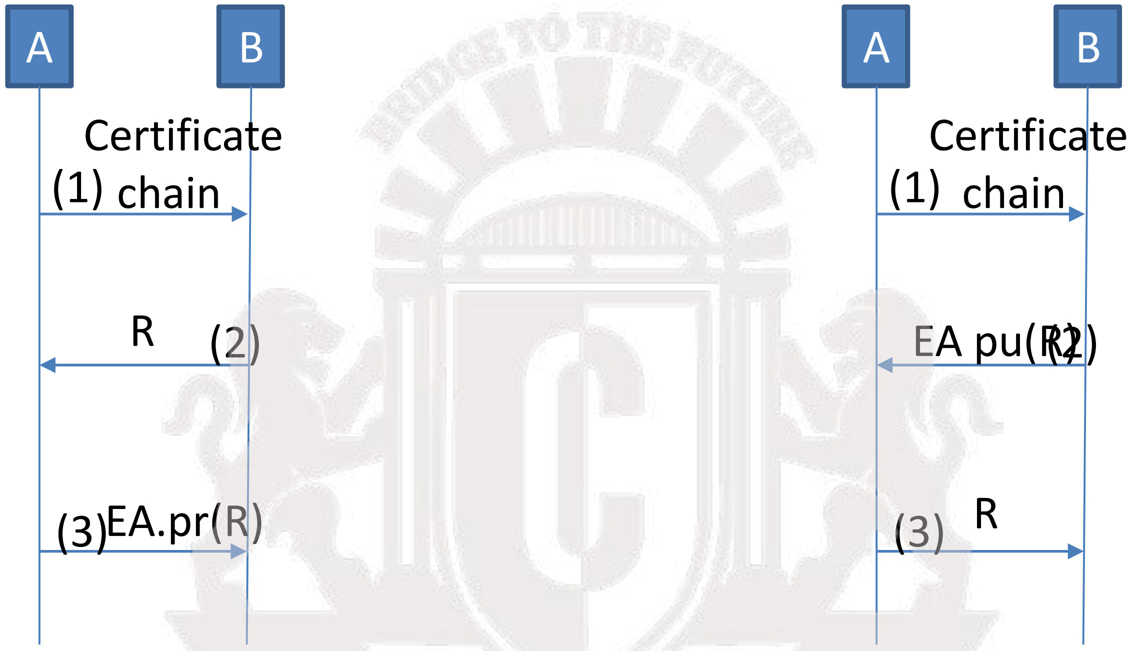
(B) Communicating hash of password

One way authentication using challenge-response protocol



Source diginotes.in

2. Certification –based one way-authentication



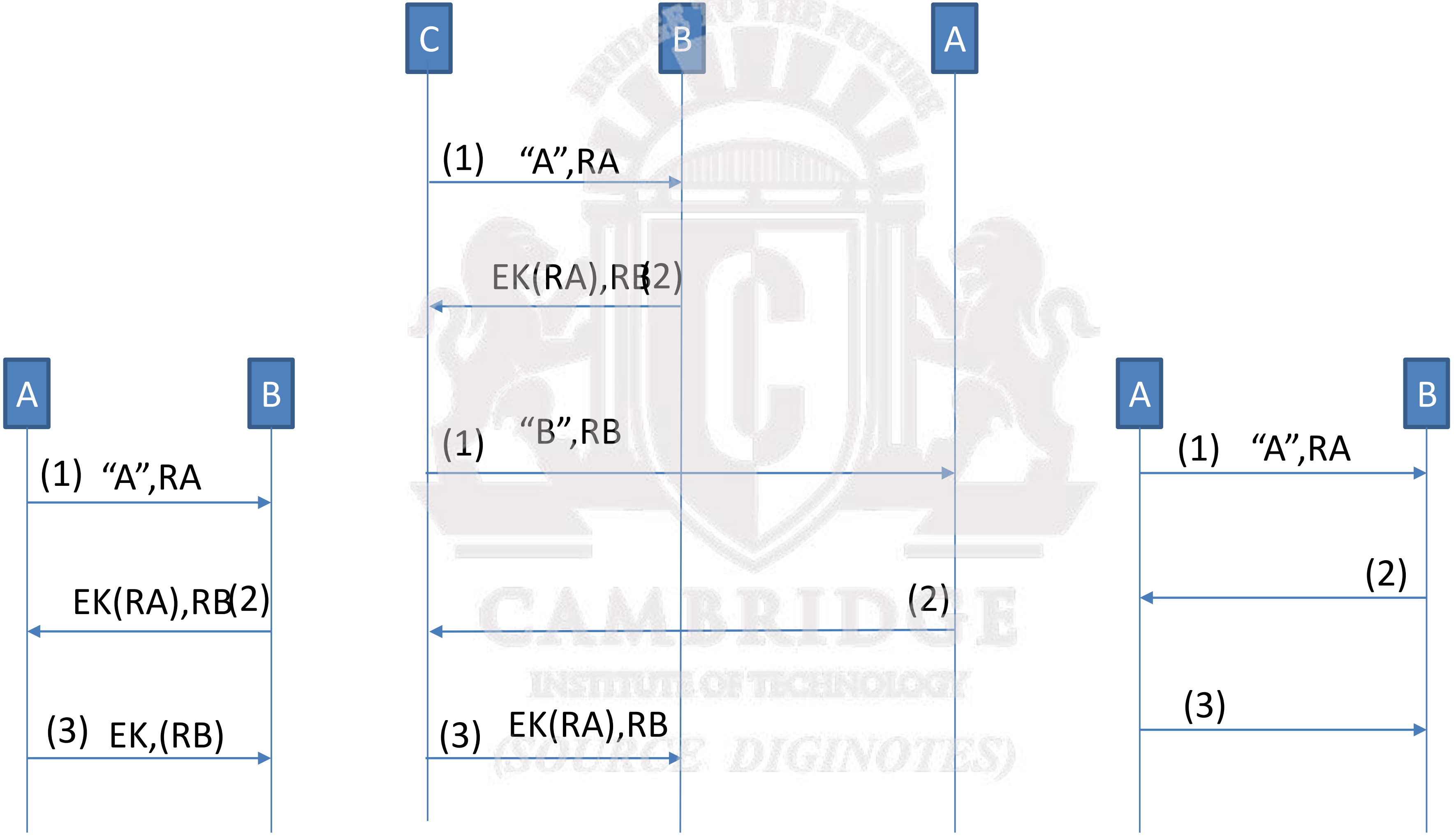
(a)

(b)

Source diginotes.in

MUTUAL AUTHENTCATION

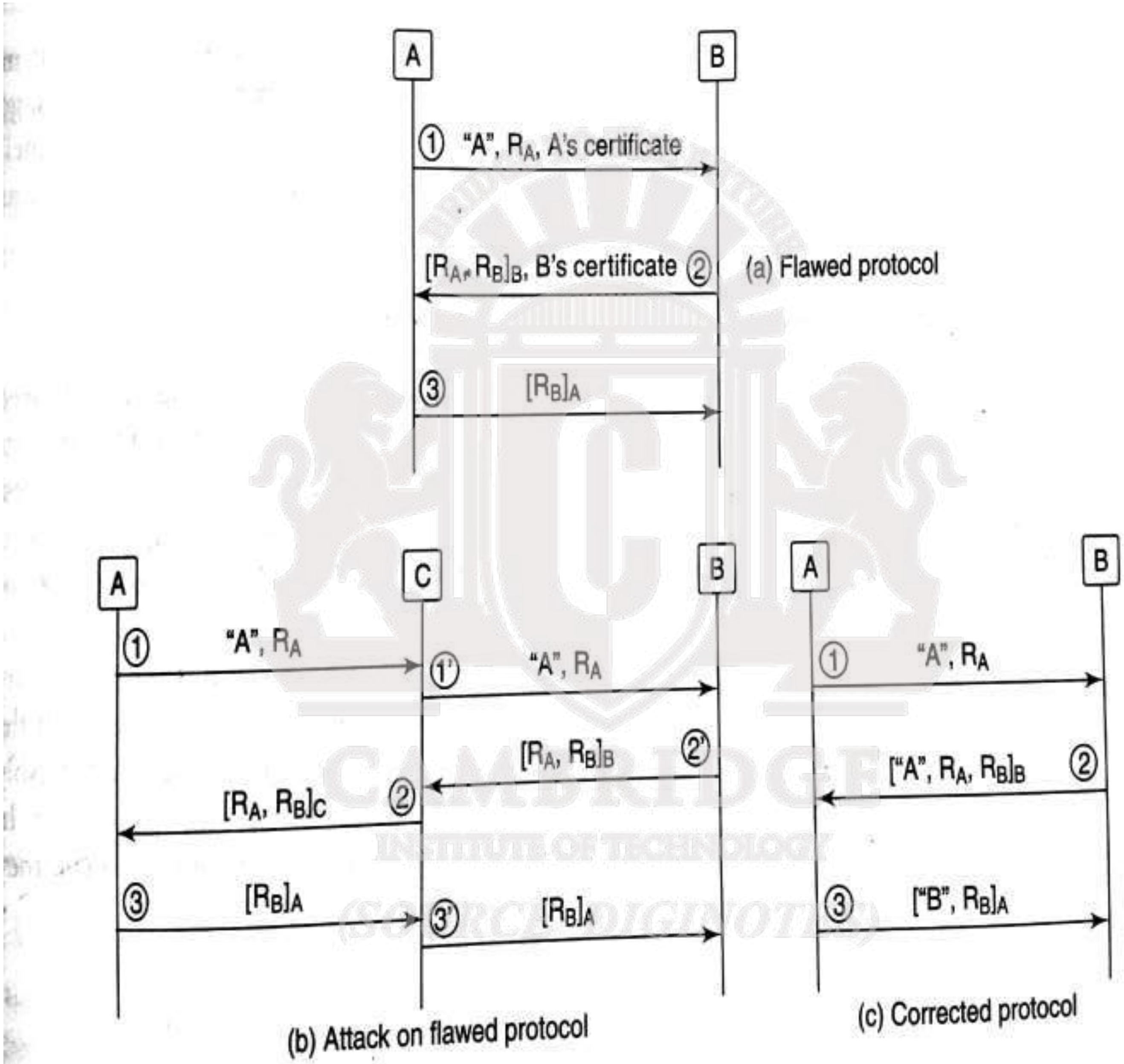
SHARED SECRET-BASED AUTHENTICATION



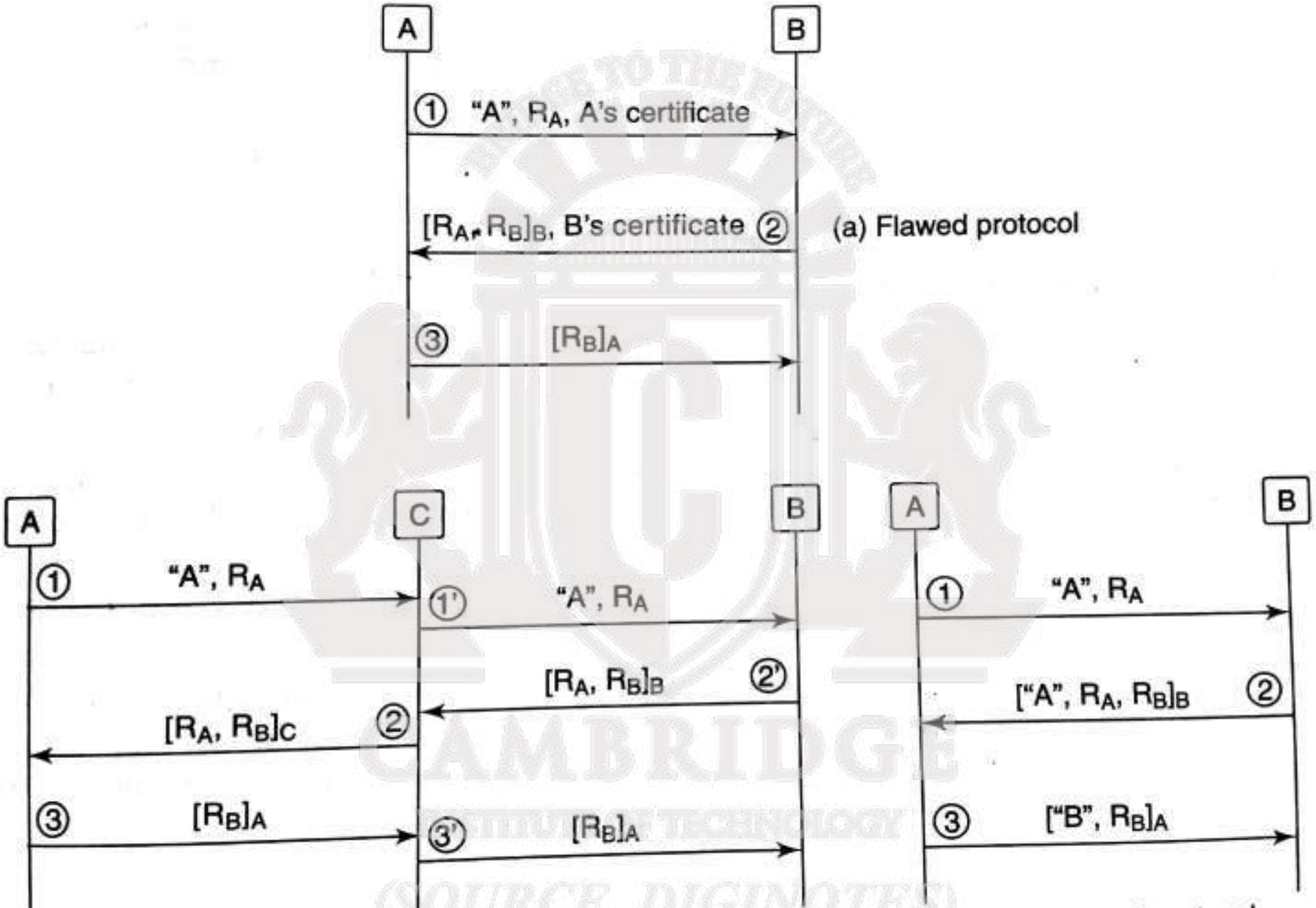
(a) Flawed protocal

(b) Parallel session attack

(c) Corrected protocal



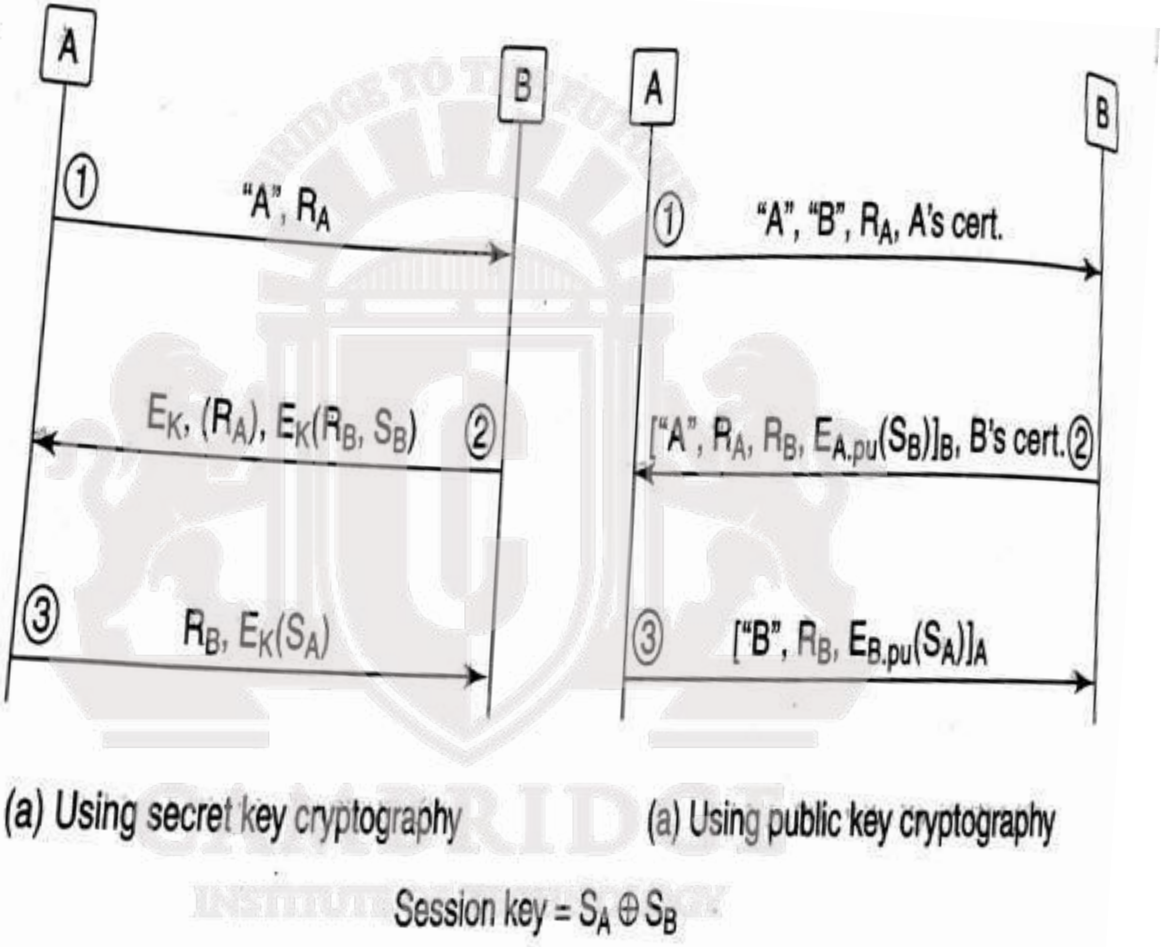
Source diginotes.in



(a) Flawed protocol

(b) Attack on flawed protocol

(c) Corrected protocol


A
B
①
"A", R_A
②
E_K, (R_A), $E_K(R_B, S_B)$
③
R_B, $E_K(S_A)$
A
B
①
"A", "B", R_A, A's cert.
②
["A", R_A, R_B, $E_{A.pu}(S_B)]_B$, B's cert.
③
["B", R_B, $E_{B.pu}(S_A)]_A$

(a) Using secret key cryptography

(a) Using public key cryptography

Session key = $S_A \oplus S_B$

Figure 11.6 *Combined mutual authentication and key exchange*

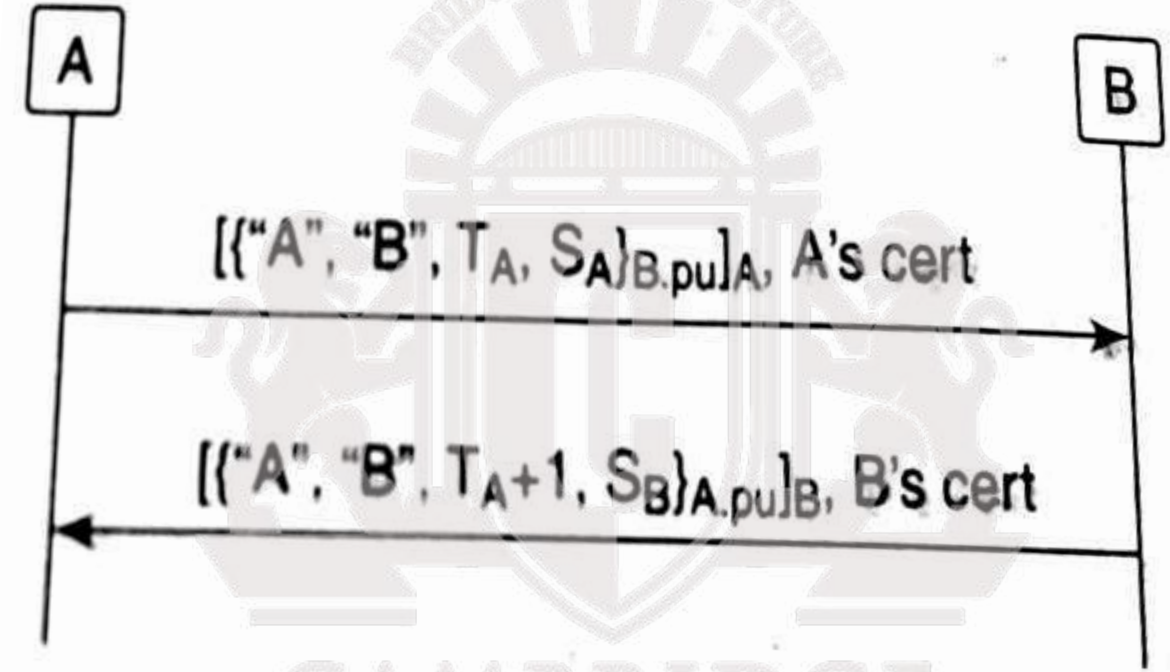

A
B
$[\{``A", ``B", T_A, S_A\}_{B.pu}]_A$, A's cert
$[\{``A", ``B", T_A+1, S_B\}_{A.pu}]_B$, B's cert

Figure 11.7 *Mutual authentication with timestamps*

Source diginotes.in

Dictionary attacks

1. Attack types

- Two types of dictionary attacks are on-line and off-line.
- In online attacks, an intruder attempts to login to the victim's account by using the victim's login name and a guessed password.
- In online there is a limit on the number of failed login attempts.
- In off-line attack leaves few fingerprints.
- One possibility is the attacker to get a hold of the password file.

Cont…

- Another possibility is for the attacker to eavesdrop on the communication link during client authentication.

```
// let D be an array containing the dictionary
// let F denote f(pw,R) where pw is client’s password
// let n be the number of permissible guesses(size of D)
Found=false
i=0
While(~found && i<n)
{
X=f(D[i],R)
If(x==F) {
Print(“CORRECT  PASSWORD is D[i]”)
Found=true
}
}
```

2. Defeating Dictionary Attacks

- One approach is to increase the cost of performing such an attack.
- The cost is the time to successfully complete the attack.
- The most time consuming operation in each iteration of the dictionary attack program is f(D[i],R).
- Hence to decrease the attacker's chance of success, the function f(D[i],R) could be made more computationally expensive.
- H(……..h(h(D[i],R))….)

A protocol that eliminates off-line dictionary attack is theEncrypted Key Exchange(EKE)

- It is a password-based protocol.
- It combines Diffie-Hellman key exchange with mutual authentication based on a shared secret.
- DHKE is vulnerable to a man-in the middle attack which is due to the unauthenticated exchange of partial secrets g^a mod p and g^b mod p.
- In EKE, each side transmits its partial secret after encrypting it. The encryption key, PW, is the hash of the password.
- Fig shows the 4 messages that are exchanged in EKE.

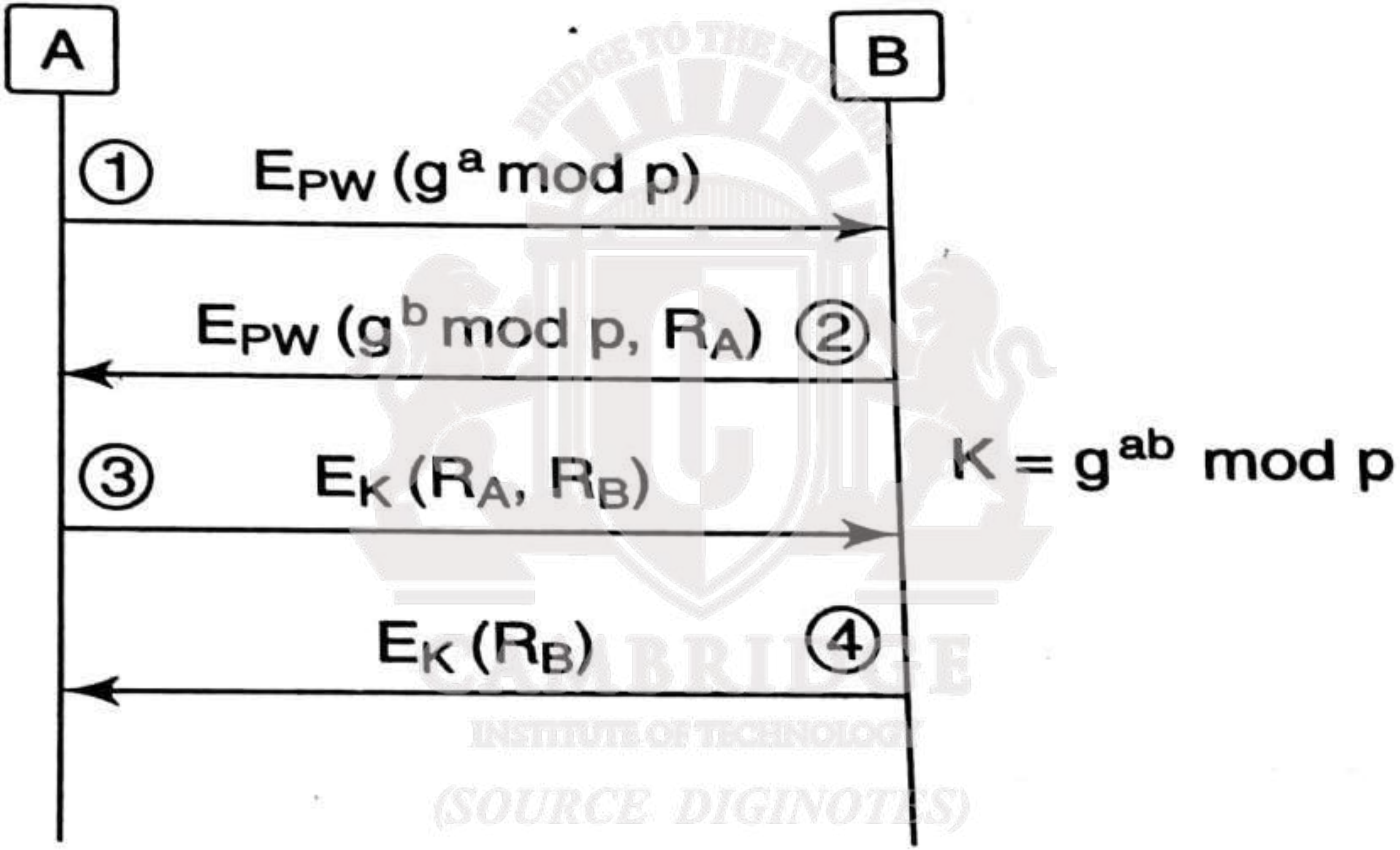


Figure 11.8 *EKE protocol*

AUTHENTICATION –II

Advantages of secret key cryptography over public key cryptography.

- First, DC and PKI are needed in support of public key cryptography. So there is a substantial cost to set up and maintain a PKI.
- Second public/private key operation are relatively slow compared to secret key operations.

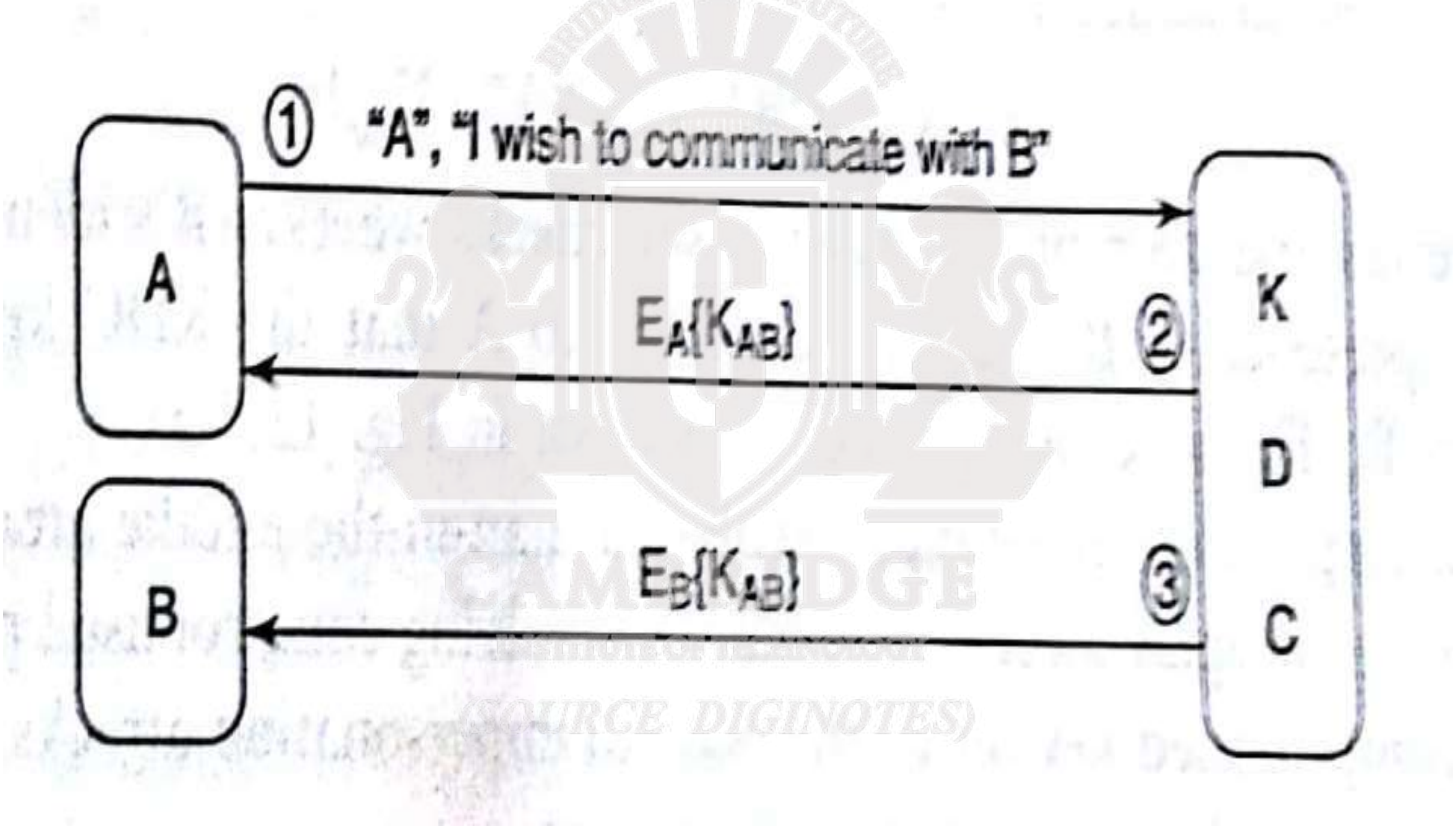
Disadvantages of secret key cryptography

- An entity must share a key with each party it wishes to communicate with.
- Suppose if entity communicates with large number of other entities over time, it must share a secret with each of those parties.
- So managing and securely storing a large number of keys is a non-trival task.

One approach is to use trusted third party

- It function as a key distribution centre(KDC).
- Each user registers with a KDC and chooses a password.
- A long-term secret, which is a function of the password, is to be exclusively shared by that user and the KDC .
- The main function of the KDC is to securely communicate a fresh, common session key to the two parties who wish to communicate with each other.

Message confidentiality using a KDC



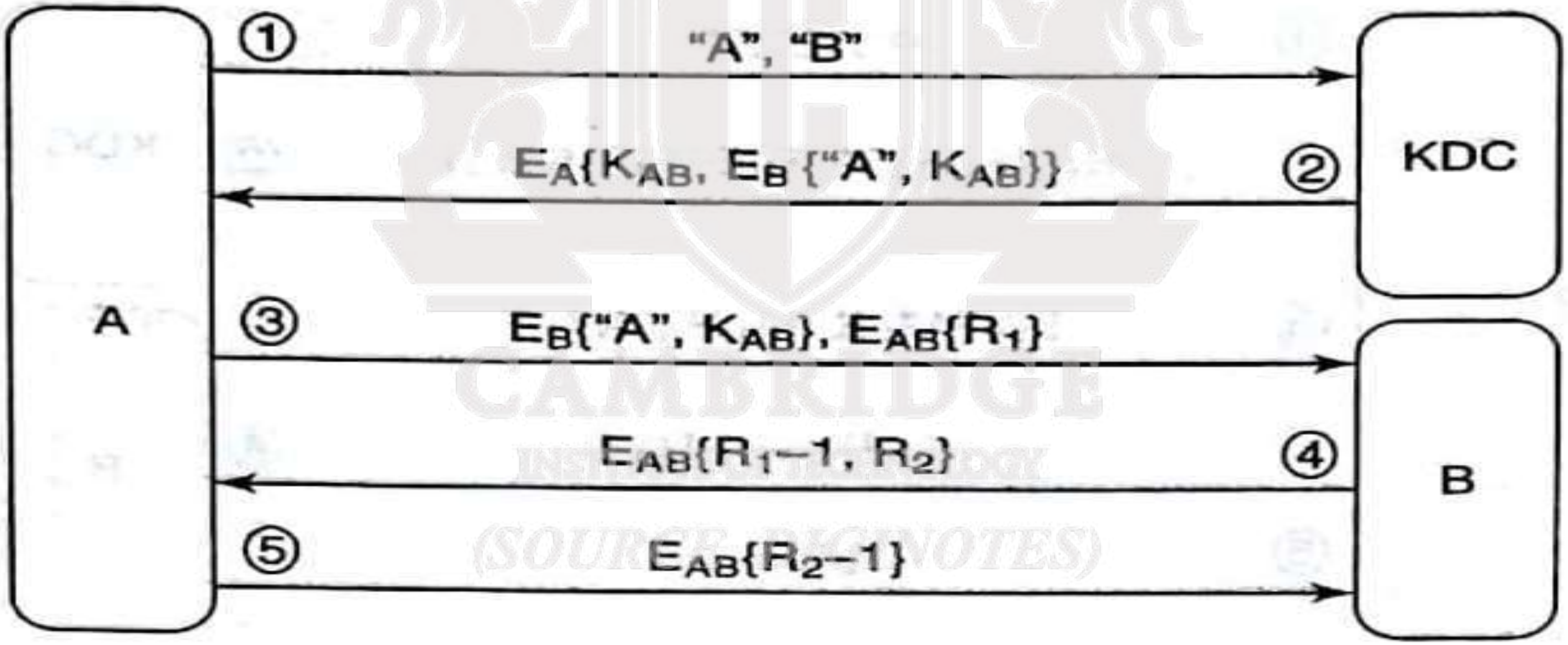
Source diginotes.in

The Needham-Schroeder protocol

- In this protocol, both sides proceed to challenge the other to prove knowledge of the session key.
- The challenge is a nonce.
- The response involves decrementing the nonce and encrypting the nonce with the session key.
- MSG1:A informs the KDC that it intends to communicate with B.
- MSG2:KDC dispatches session key and the ticket to B[Encrypted with long term key shared b/w B & KDC] in its msg to A[Encrypted with long term key shared b/w A & KDC].
- MSG3:A then forwards the ticket together with her challenge to B.
- MSG4:B response involves decrementing the nonce and new challenge to A, both encrypted using a session key.
- MSG5: A response to B by decrementing the nonce encryptrd using a session key.

The Needham-Schroeder protocol

- Provide mutual authentication by including a challenge-response phase.

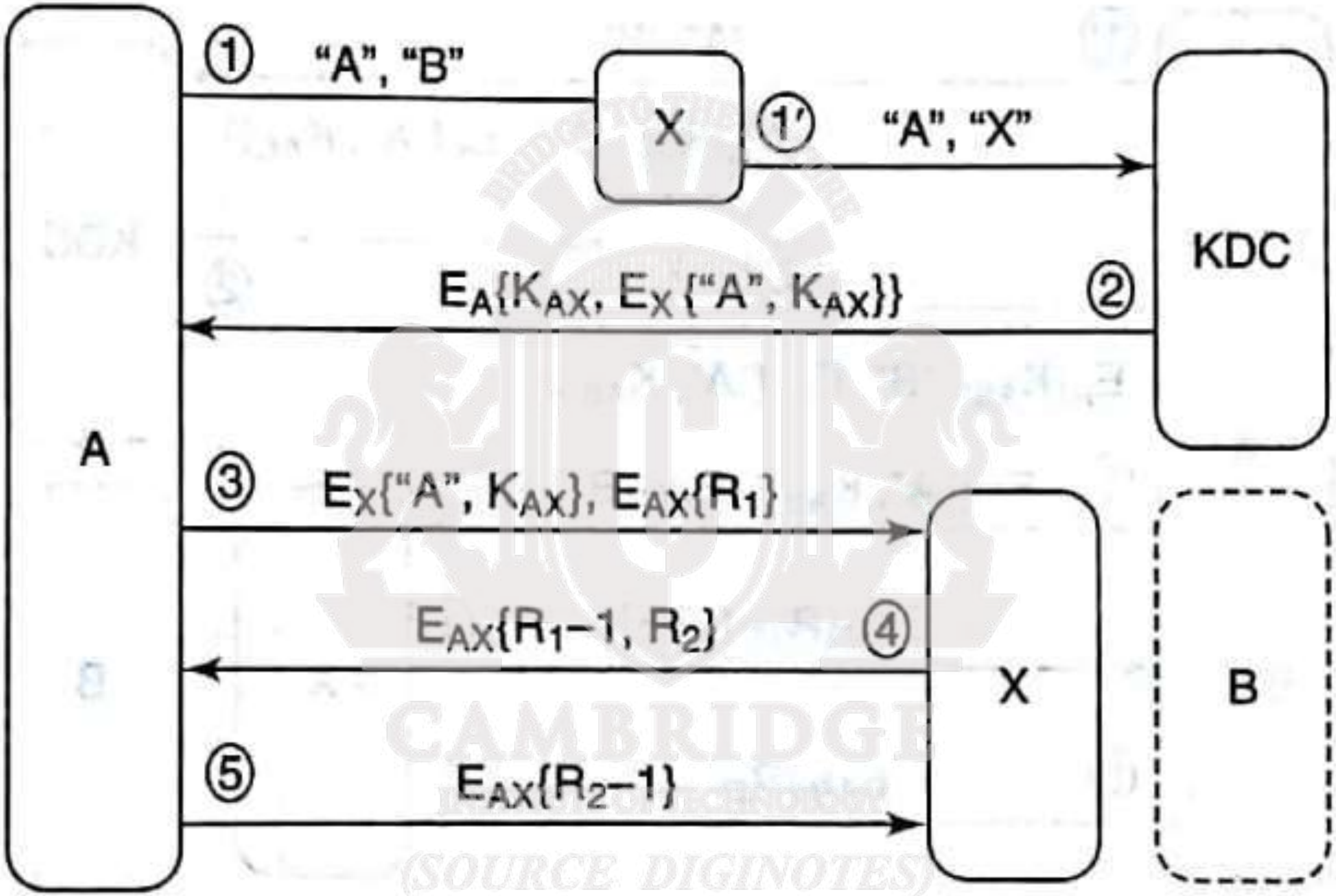

A
KDC
B
①
"A", "B"
②
$E_A\{K_{AB}, E_B\{\text{"A"}, K_{AB}\}\}$
③
$E_B\{\text{"A"}, K_{AB}\}, E_{AB}\{R_1\}$
④
$E_{AB}\{R_1{-}1, R_2\}$
⑤
$E_{AB}\{R_2{-}1\}$

(a) : Preliminary version 1

Source diginotes.in

Man-in-the middle attack on preliminary version1

- The attacker, X, is an insider who shares a long-term key with the KDC.
- The attacker , X, intercepts MSG1, substitutes B for X and sends the modified msg to the KDC.
- In response, the KDC creates a ticket encrypted with X's long-term key and send it to A.
- Now X intercepts MSG3.He decrypts the ticket using the long term secret he shares with the KDC. He thus obtains the session key.
- MSG 3 also contains A's challenge R1.X uses the session key to decrypt the part of the msg containing A's challenge. He successfully responds to A's challenge in MSG 4.
- Thus, X successfully impersonates B to A.



A
①
"A", "B"
X
①′
"A", "X"
KDC
$E_A\{K_{AX}, E_X\{"A", K_{AX}\}\}$
②
③
$E_X\{"A", K_{AX}\}, E_{AX}\{R_1\}$
$E_{AX}\{R_1-1, R_2\}$
④
X
B
⑤
$E_{AX}\{R_2-1\}$

(b) : Man-in-the middle attack on preliminary version 1

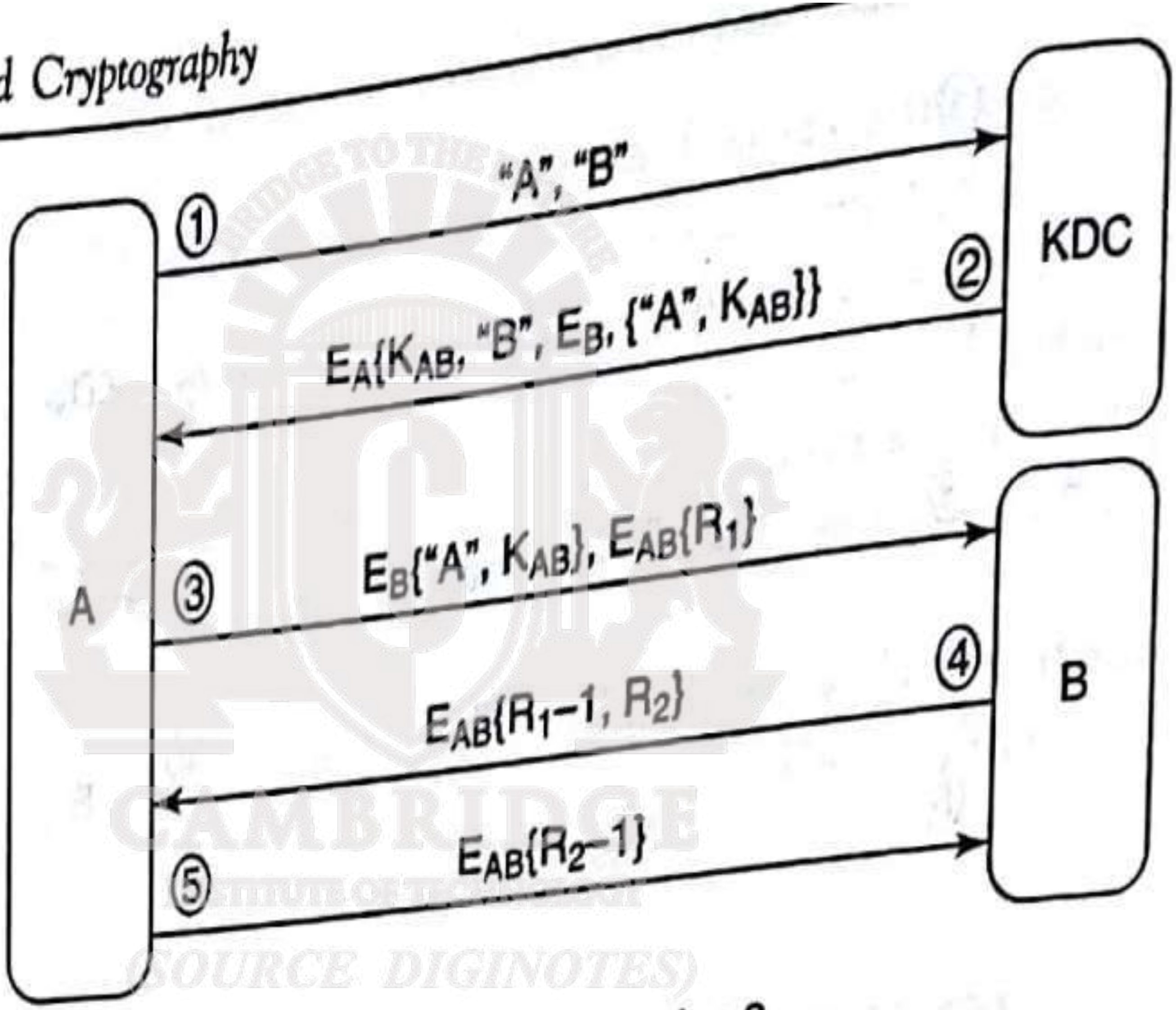
Source diginotes.in

Preliminary Version 2

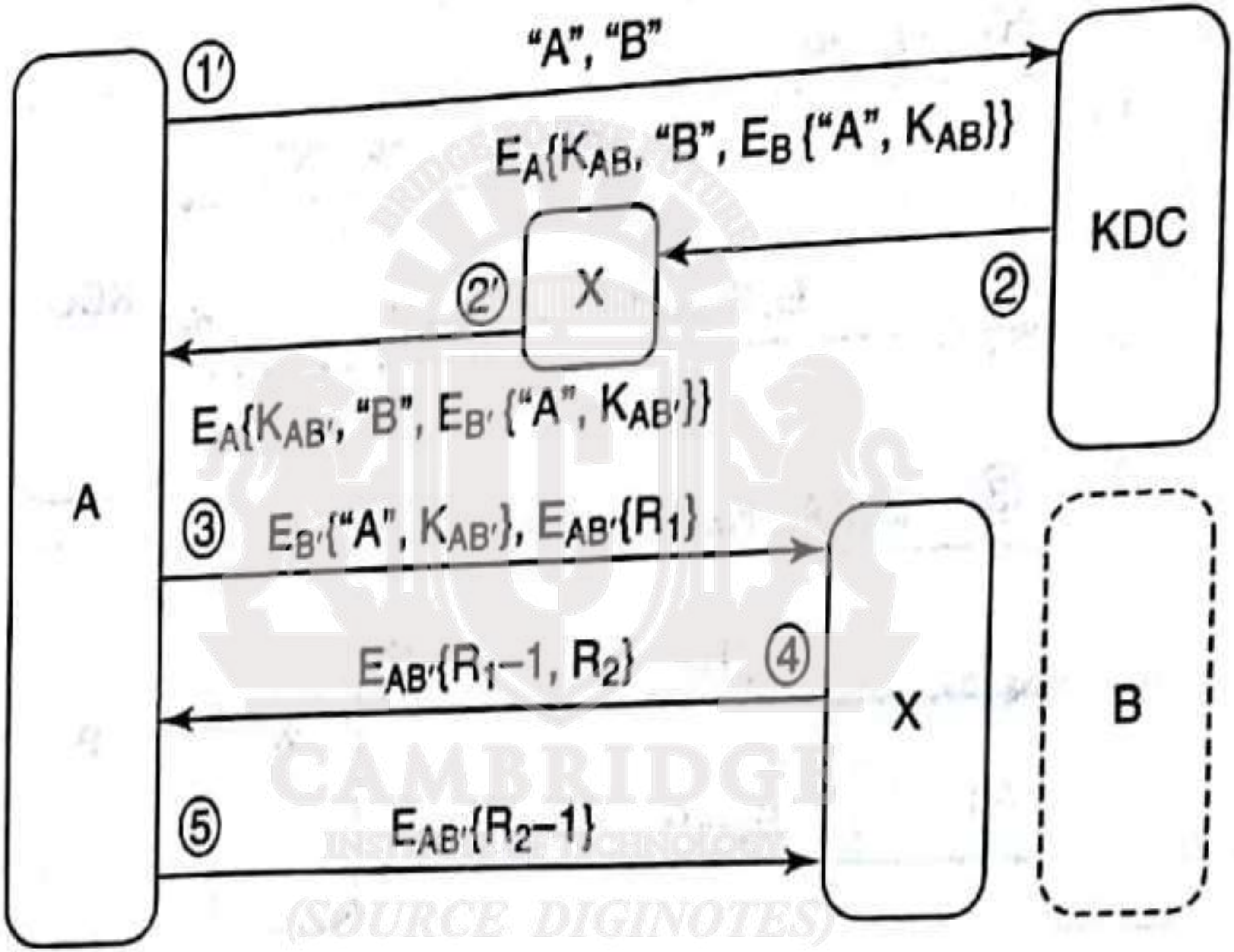
- Solution to previous problem is to include B’s identity in the encrypted message from the KDC to A in MSG 2.

- Now, after A receives and decrypts MSG2, she checks whether B’s identity is contained inside the msg.

- The presence of B’s identity confirms to A that the KDC knows that A wishes to communicate with B.



(a) Preliminary version 2


①′
“A”, “B”
KDC
$E_A\{K_{AB}, “B”, E_B\{“A”, K_{AB}\}\}$
②
X
②′
$E_A\{K_{AB'}, “B”, E_{B'}\{“A”, K_{AB'}\}\}$
A
③
$E_{B'}\{“A”, K_{AB'}\}, E_{AB'}\{R_1\}$
④
$E_{AB'}\{R_1-1, R_2\}$
X
B
⑤
$E_{AB'}\{R_2-1\}$

(b) Man-in-the middle and replay attack on preliminary version 2

Source diginotes.in

A determined attacker X does the following:

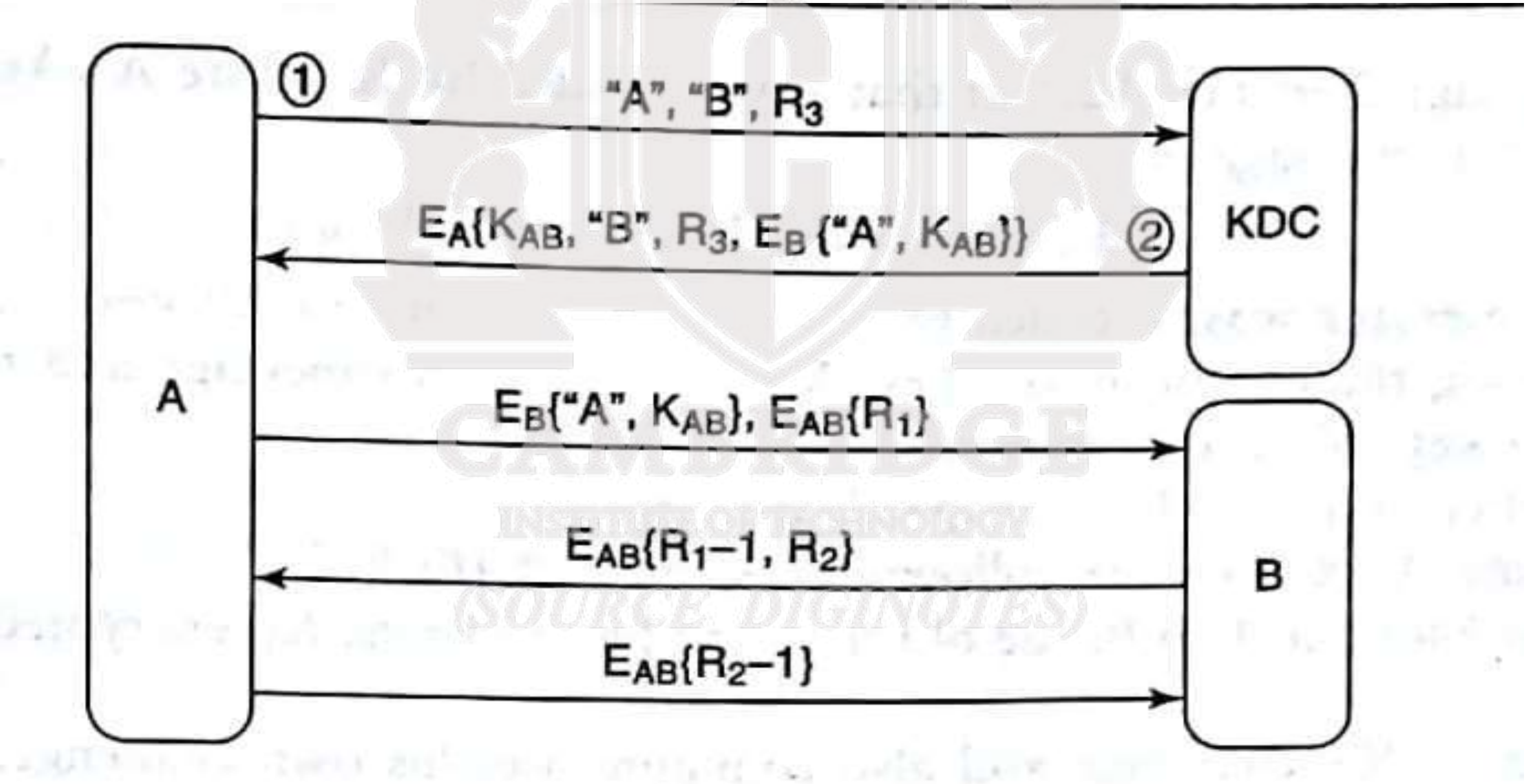
- X eavesdrops upon and meticulously records many of A’s sessions with the KDC and with B over a period of time.
- He then steals B’s password or long-term key.
- B recognizes that his password has been stolen and immediately reports the incident to the KDC. He obtains a new long-term key which he uses subsequently.

The following scenario shows X successfully impersonating B to A.

- A wishes to communicate with B and sends MSG1
- X intercepts the KDC’s response(MSG2) and instead plays a previous recording of MSG2. X is careful to replay a copy of MSG2, which he recorded before B’s key was compromised(contains a ticket encrypted with B’s old key.
- X then intercepts MSG3 from A, which contains the old ticket and a fresh challenge to B. X has B’s old key, he can decrypt this ticket and recover the session key.
- X knows session key , he can respond to A’s challenge in MSG4.
- X’s response is exactly what A expected to receive from B. Hence A is convinced that she is talking to B.

Preliminary Version 3

- Previous problem solved by ensuring the freshness of MSG2.
- A sending a nonce in MSG1 and receiving confirmation of its receipt by the KDC.



A
KDC
B
①
"A", "B", R_3
$E_A\{K_{AB}$, "B", R_3, $E_B\{$"A", $K_{AB}\}\}$
②
$E_B\{$"A", $K_{AB}\}$, $E_{AB}\{R_1\}$
$E_{AB}\{R_1-1, R_2\}$
$E_{AB}\{R_2-1\}$

(a) : Preliminary version 3

- X could still attack the protocol by recording previous messages and selectively replaying them when the right opportunity presents itself.
- He attempts to steal A's password or long-term key and success in it.
- MSG2 was recorded by X before A's key was compromised.

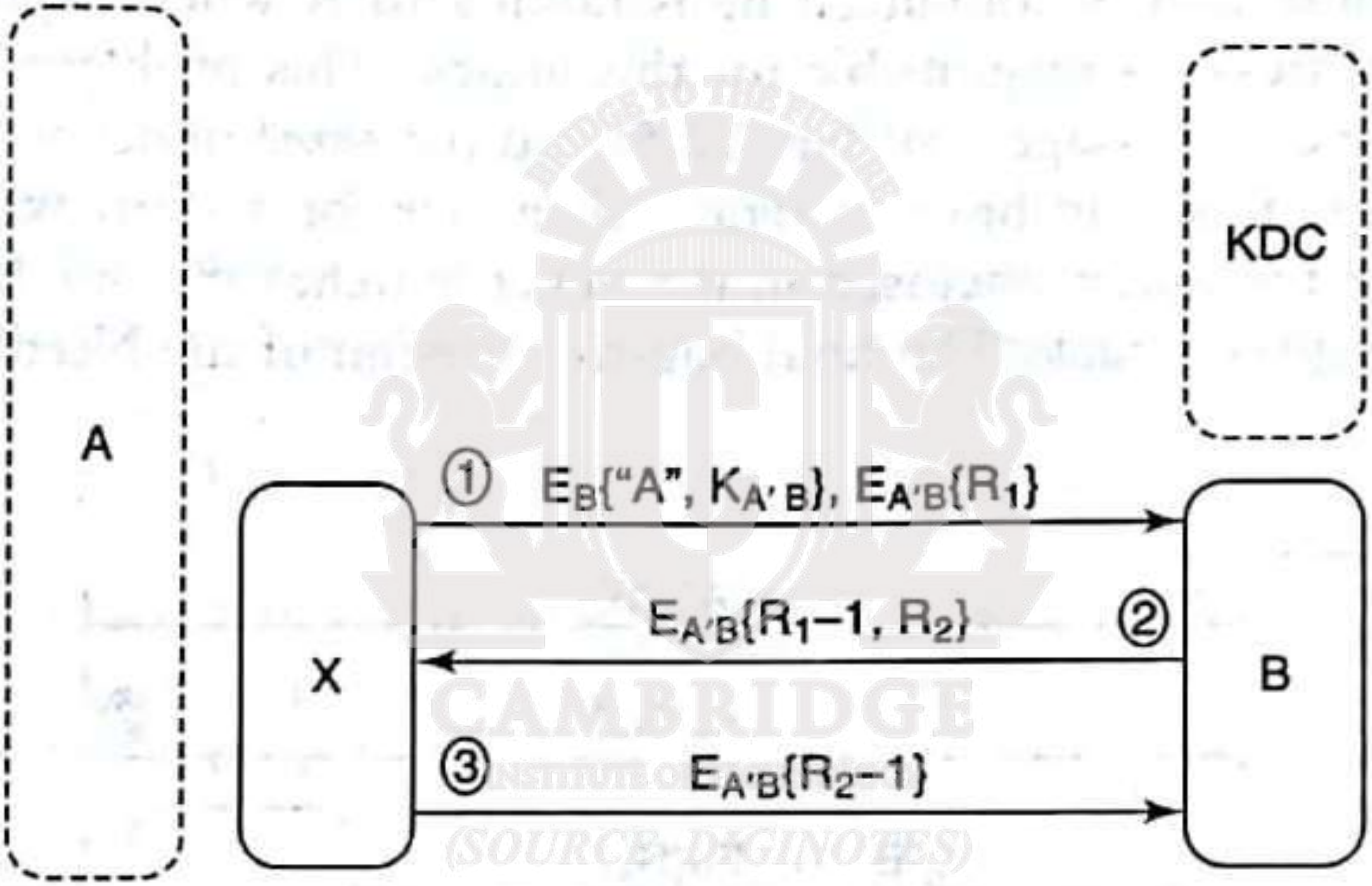
Using the compromised key, X can decrypt this msg and recover the

- Old session key used then and the old ticket dispatched to B.

To impersonate A, X does the following:

- X sends, in MSG1 to B, the old ticket and a challenge R1, encrypted with the old session key.
- B responds to X's challenge and also communicates his own challenge,R2.
- Because X has the session key, he responds to the challenge by encrypting R2 with the old session key.

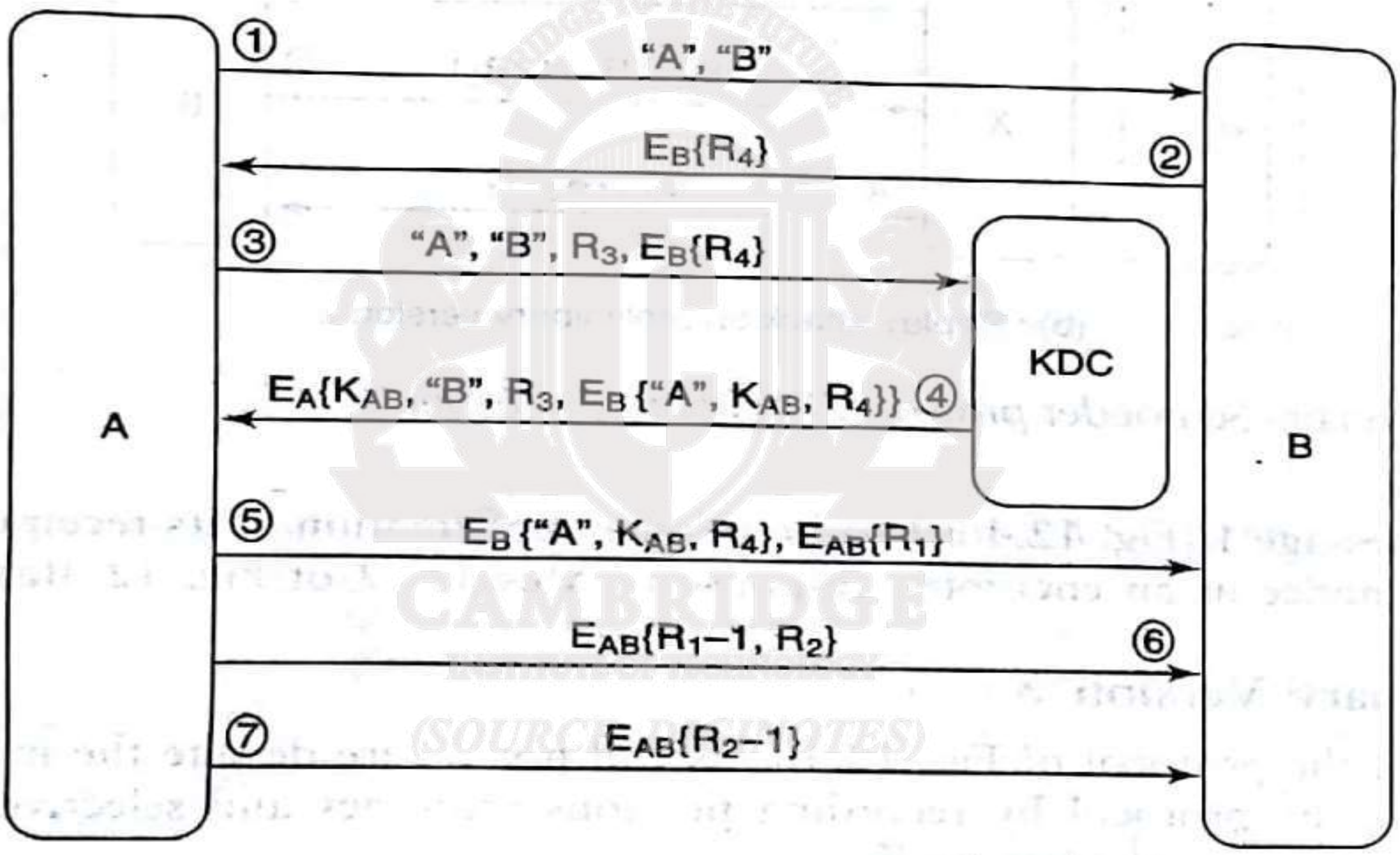
B receives the response and is convinced he is talking to A but he is talking to X.


A
KDC
X
B
① $E_B\{\text{"A"}, K_{A'B}\}, E_{A'B}\{R_1\}$
$E_{A'B}\{R_1-1, R_2\}$ ②
③ $E_{A'B}\{R_2-1\}$

(b) : Replay attack on preliminary version 3

Source diginotes.in

Needham-Schroeder protocol: Final Version


A
B
KDC
① "A", "B"
② $E_B\{R_4\}$
③ "A", "B", R_3, $E_B\{R_4\}$
④ $E_A\{K_{AB}$, "B", R_3, $E_B\{$"A", K_{AB}, $R_4\}\}$
⑤ $E_B\{$"A", K_{AB}, $R_4\}$, $E_{AB}\{R_1\}$
⑥ $E_{AB}\{R_1-1, R_2\}$
⑦ $E_{AB}\{R_2-1\}$

Needham–Schroeder protocol: Final version

Source diginotes.in

KERBEROS

- A scenario with multiple users and multiple servers in an organization.

- A user, once logged in, may then wish to access different resources such as e-mail or a file server in the course of that login session.

- One possibility is for the user to have multiple passwords on each of these servers.

- Humans remember and update multiple passwords is not practical.

- A user could use the same password for all servers but distributing and maintaining a password file across multiple servers is a security risk.

A password-based system should ensure the following:

- The password should not be transmitted in the clear.
- It should not be possible to launch dictionary attacks using the eavesdropped-upon messages containing a function of the password.
- The password itself should not be stored on the authentication server, rather it should be cryptographically transformed before being stored.
- A user enters her password only ONCE during login. Thereafter, she should not have to renter her password to access other servers for the duration of the session. This feature is called single sign-on.
- The password should reside on a machine for only few milliseconds after being entered by the user.

Source diginotes.in

- The KDC is logically split into two entities here- the authentication server(AS) and the Ticket Granting Server(TGS).

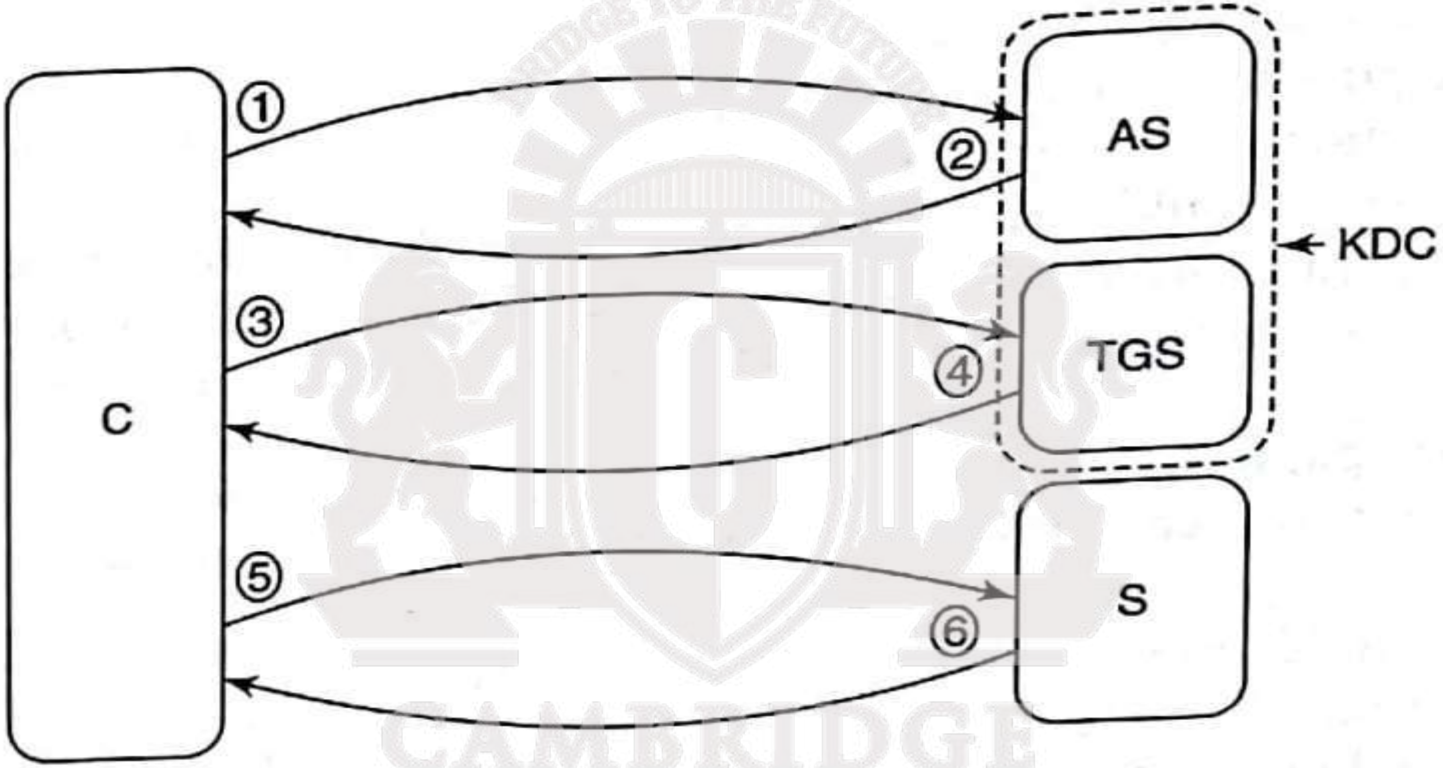
- The Ticket is the mechanism used to safely distribute session keys.

- User A shares a secret Ka with the AS.

- Each server, B shares a secret Kb with the TGS.

- Kerberos also makes use of timestamps.

Kerberos message sequence



① C request Ticket-Granting Ticket

③ C request Service-Granting Ticket

⑤ C authenticates itself to S

② C receives Ticket-Granting Ticket

④ C receives Service-Granting Ticket and session key

⑥ S authenticates itself to C

*Kerberos message sequence*Source diginotes.in

BIOMETRICS

- A biometric is a biological feature or characteristic of a person that uniquely identifies him/her over his/her lifetime.
- Common forms of biometric identification include face recognition, voice recognition, manual signatures and fingerprints.
- More recently, patterns in the iris of the human eye and DNA have been used.
- Biometric forms were first proposed as an alternative or a complement to passwords.
- Passwords are based on what a user knows and are based on what a person has.
- A biometric, on the other hand, links the identity of a person to his/her physiological or behavioural characteristics.

The two main processes involved in a biometric system are:

- **Enrolment:** A subject’s biometric sample is acquired. The essential features of the sample are extracted to create a reference template. Sometimes multiple samples are taken and multiple templates are stored to increase the accuracy of a match in the subsequent recognition phase.

- **Recognition:** A fresh biometric sample of the person is obtained. This is then compared with the reference templates (created during enrolment) to determine the extent of a match.

Biometrics is used in at least two different situations:

Authentication or Identity verification:

- A biometric systems stores login name and biometric sample pairs.

- During a login attempt, a biometric sample (such as a fingerprint scan) of the user is taken.

- The biometric sample is compared with the sample stored on the server.

- The user is authenticated only if a match between the two occurs.

Identification

- Subject’s identity is not presumed to be known beforehand.
- It is assumed that a database of biometric samples of several users already exists.
- The subject’s biometric sample is compared with the samples in the database to determine if a match exists with any one of them.

- Authentication involves a one-to-one match, identification involves a one-to-many match.

A characteristics of a good biometric include the following:

- Universality: All humans should be able to contribute a sample of the biometric.
- Uniqueness: biological samples taken from two different humans should be sufficiently different that they can be distinguished by machine intelligence.
- Permanence: The biometric should not change over time

KEY MANAGEMENT.

* Key management is related to the generation, storage, distribution and backup of keys.

* public key-private key pairs are used for encryption decryption, signature generation/verification and for authentication.

* TO encrypt a session key for use in communication between A and B, A needs to know B's public key.

* TO verify B's Signature on a msg, A needs B's public key

* The key issue here is "How does A know B's public key?"

possibility 1: A may frequently communicate with B in a secure fashion, so she may already have B's public key.

possibility 2: Every entity's public key is securely maintained in a centralized directory.

possibility 3: A receives a document signed by a trusted source C, containing B's public key.

DIGITAL CERTIFICATES.

1. Certificate types

* A digital certificate is a signed document used to bind a public key to the identity of a person.

* The entity that issues certificates is a trusted entity called a certification Authority (CA).

* The CA may have to obtain and verify several details of the applicant including his/her employe e-mail address etc. practically speaking, this task would be delegated by the CA to a Registration Authority.

2. X.509 Digital certificate format.

* certificate serial number and version: Each certificate issued by a given CA will have a unique no

* Issuer Information: The distinguished name of an entity includes his/her/its "common name", email address, organization, country etc.

* subject information: It includes the name of the certificates owner. other information, such as the subject's country, state & organization may be included.

* Subject public key information: The public key, the public key algorithm and the public key paramelers.

* validity period: There are two date fields that specify the start date and end date b/w which the certificate is valid.

* Certificate signature and associated signing algorithm information: It is necessary to verify the authenticity of the certificate. for this purpose, it is signed by the issuer. So the certificate should include the issuer's digital signature and also the algorithm used for signing the certificate.

3. Digital certificate in Action

* Assume that A needs to securely transmit a session key to B. so she encrypts it with B's public key. A will need to retrieve the public key from B's certificate.

* A may already have B's certificate or she may send a msg to B requesting it.

* There are no of checks that A ll have to perform on B's certificate prior to using B's public key.

1. Is this indeed B's certificate?

2. A should check if the certificate is still valid.

3. The certificate must be signed by a CA or RA.

PUBLIC KEY INFRASTRUCTURE.

1. functions of PKI.

* public key infrastructure includes
  a. certificate creation, issuance, storage.
  b. key Generation (if necessary)
  c. certificate/key updation (if necessary)
  d. certificate revocation.

2. PKI Architecture.

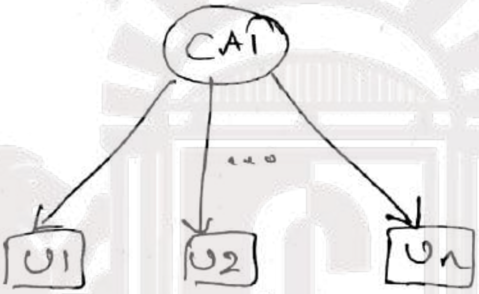


fig: PKI with single CA

* CA1 could issue certificates to multiple users U1, U2, etc. enabling any pair of these users to communicate securely using certificates exchanged b/w them.

* This architecture, however is not scalable)

* Suppose if there are tens of millions of users who may need certificates. It is not pratical for CA1 to issue certificate to them all

* A practical solution to the problem of scalability is to have CA1 certify other CAs who in turn certify other CAs & so on.

* This creates a tree of CAs known as a hierarchical pki architecture.

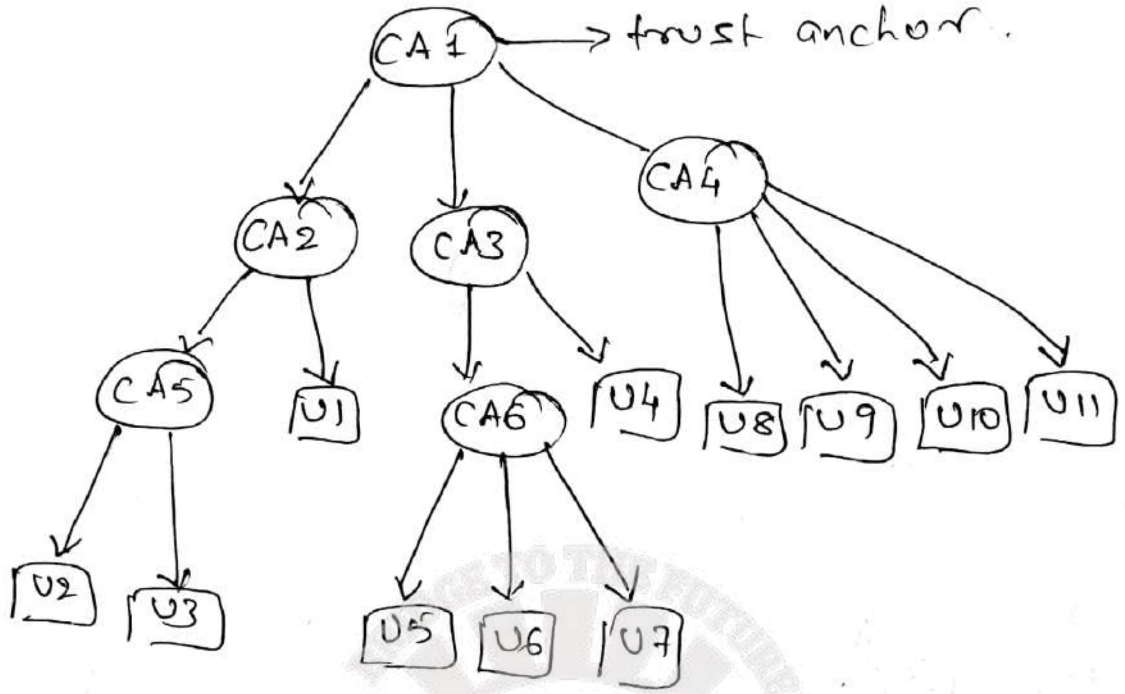
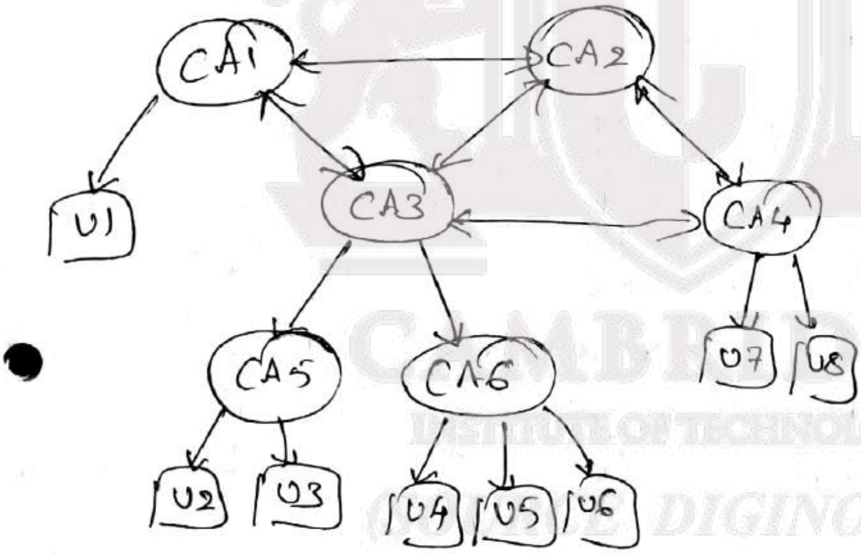


Fig:- Hierarchical (tree-based) PKI architecture.

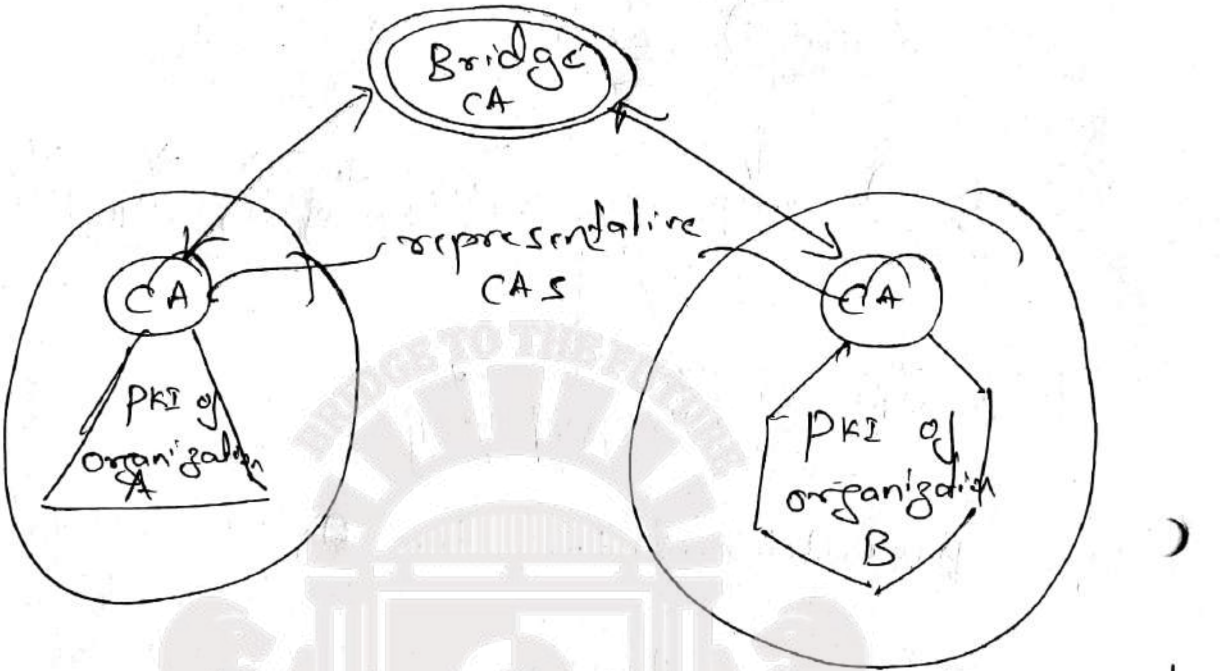
Fig3:- Mesh-based PKI



- * This include mutually trusting CAs - CA1 trusting CA2 & CA2 trusting CA1 depicted by a bidirectional arc b/w CA1 & CA2.
- * There may be multiple trust paths b/w 2 users
- * one trust path b/w user U1 & U7 passes through CA1, CA3 & CA4
- * Another trust path involves CA1, CA2 & CA4.
- * Multiple paths provide greater resilience in the

event of one or more CAs being compromised.

Fig:- Bridge-based PKI



- Motivated by the need for secure communication b/w organization in a business partnership.
- Suppose that the partnering organization already have their own PKIS, A bridge CA is introduced that establishes a trust relationship with a representative CA from each organization. This is accomplished by the bridge CA & the organizational representatives issuing certificates to each other.

3. Certificate Revocation

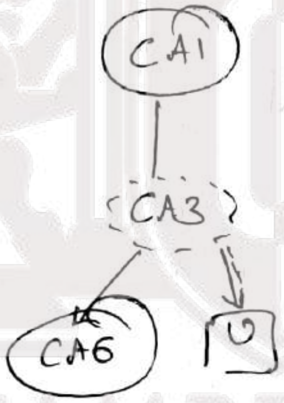
a. Revocation Scenarios.

Scenario 1: The certificate's Subject, prashant was issued a certificate valid b/w Jan 01, 2010, & Dec 31, 2010. However, he quit the organization on April 1, 2010. Assume that prashant's certificate is to be used for key exchange and that he has made a copy of it.

* note that the public key in a key exchange certificate is used by another party to encrypt a random session key. The session key itself is then used to encrypt all msges in both directions for the duration of the ensuing session.

* It is not legal for prashant to act on behalf of ● his company beyond the date of his resignation.

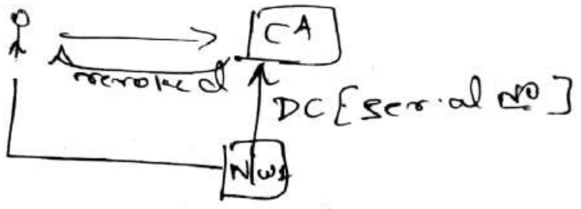
Scenario 2:



● * suppose that the private key of CA3 were compromised. An attacker with access to the compromised private key could then do the following.

->Generate a public key, private key pair (x, y)
->Create a certificate containing the public key
  * with subject name = U.
->Sign the above certificate using the compromised private key of CA3

Handling Revocation

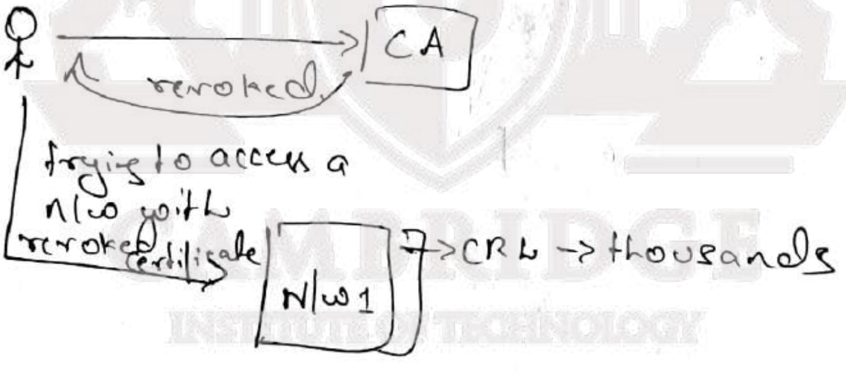


Solution 1:

- Is to use an on-line facility that provides information on the current status of digital certificates
- For this purpose, a protocol called on-line certificate status protocol is employed
- Browser sends D.C to CA for status update.

Solution 2:

- Certificate Revocation lists (CRL)
- If CRLs are distributed too frequently, they could consume considerable bandwidth.
- CRL contains lists of all revoked certificates.



Authentication - I.

* Authentication is a process in which a principal proves that he/she/it is the entity it claims to be.

* The principal is referred to as the prover, while the party to whom proof is submitted for identity verification is called the verifier.

ONE-WAY AUTHENTICATION.

● In client-server communication, the client authenticates itself to the server. The server may or may not be authenticated to the client.

1. Password-based Authentication

* The common mechanisms to implement authentication is the password.

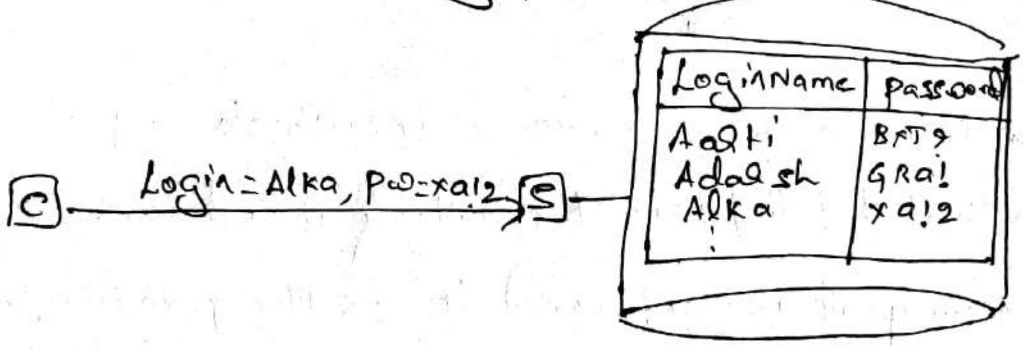
* To login to a server, a user enters his/her

● login name and password.

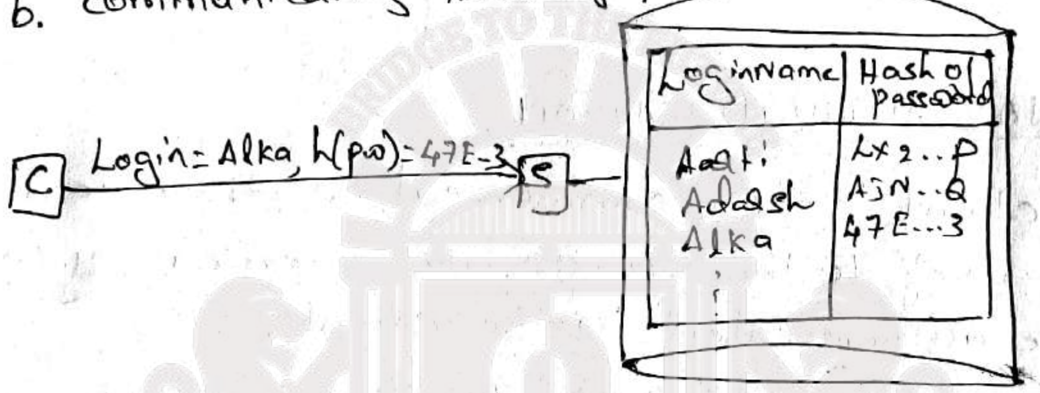
* The password is the secret i.e known only to the user and server

* The login name identifies a user, while the user's knowledge of the corresponding password constitutes proof that he/she is the person with the given login name.

Fig:- a) communicating password.



b. communicating Hash of password.



* Two danger associated with such an implementation
* first, the password is sent in the clear, so an attacker can eavesdrop on the msg containing the password and later impersonate the realuser
* second, the passwords are stored in unencrypted form in a file on the server. If an internal attacker obtains access to that file, all passwords stored on that server could get compromised.

* Solution is the cryptographic hash of the password rather than the password itself is stored on the server.
* The one-way property of the cryptographic hash helps prevent an attacker from deducing user passwords from information in the password file. or from communications on the transmission line.

* However, an attacker could snoop on the communications b/w Alka & the Server and obtain the hash of the password. He can, at a later point in time, replay it to the server thus impersonating Alka. Such an attack in which one play back all or a palt of one or more previous msges with the intent of impersonating a legitimate user, is refered to as a replay attack.

- The solution to replay attack is for the verifier to offer a fresh challenge to the prover. In response, the client does not communicate its password but rather proves that it knows the password. The Server is thus able to verify whether the client is genuine or not. Such an authentication protocol is commonly referred to as a challenge-Response protocol.

- Fig shows a three-msg one-way authentication protocol.

* In the first msg, A conveys its identity. The second msg contains the challenge from the server. The challenge is a random number called a nonce. ~~in~~ ~~[illegible]~~ The third msg is the client's response - a cleverly chosen function of the challenge & the password.

* The function, f(pw, R) has the following properties:

* Given x & y, it should be easy to compute f(x,y).
* f is one-way; so knowing f(pw, R) & R, it should be infeasible to compute pw.
* Given an R, it should be infeasible to compute f(pw, R) even if one knows
    - f(pw, R_1), f(pw, R_2), f(pw, R_3) ....
    - the corresponding R1, R2, R3 ....

* Figb: Another choice for f is the cryptographic hash, which is applied over the concatenation, of the password and the Nonce.

* Figc: Another choice is a secret key encryption function with the key being the password or a function of the password

* Figd: the challenge sent by the server is an encrypted nonce. so the function f is the decryption function the client would need to decrypt the challenge to obtain the nonce and return it to the sender to prove knowledge of his/her password

<u>NONCE</u> : * Nonces are random and nonrecurring.
* Nonce means used only once.
* The size of a nonce is usually large. This provides a large space from which a nonce may be selected
* The large space of nonces means that the probability of choosing the same nonce twice is infinitesimally small.

Fig a:

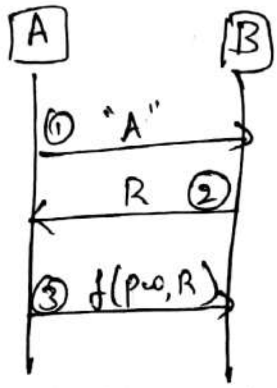


Fig b:

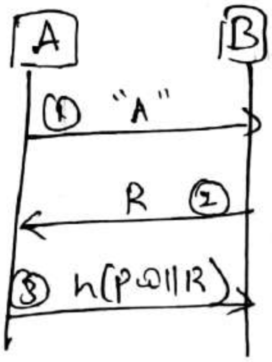


Fig c:

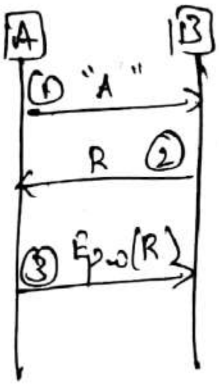
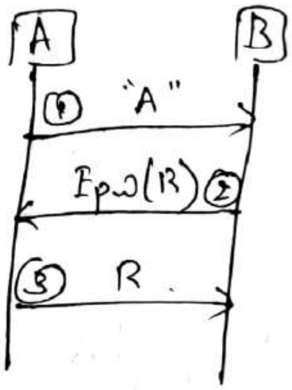
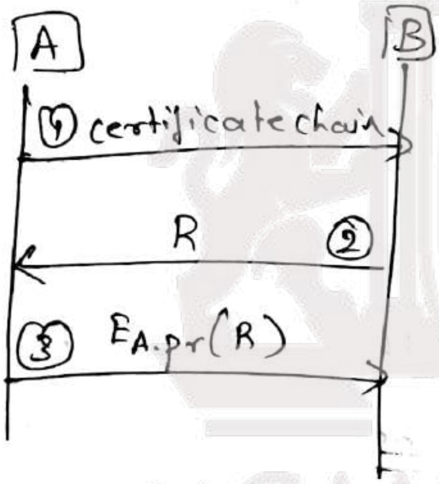


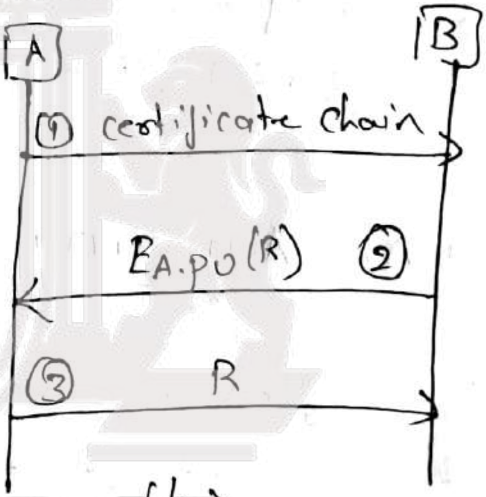
fig d:



2. CERTIFICATE - BASED AUTHENTICATION.



(a)



(b)

* Fig a:

* A sends her certificate in Msg 1.

* B performs certain checks such as on the validity period & name of principal. He also verifies the signature of the CA on the certificate. He then sends his challenge - a nonce R

* A responds by encrypting the challenge with her private key. When B receives $E_{A.pr}(R)$ he decrypts" it with A's public key & compares it with the nonce he transmitted in Msg 2

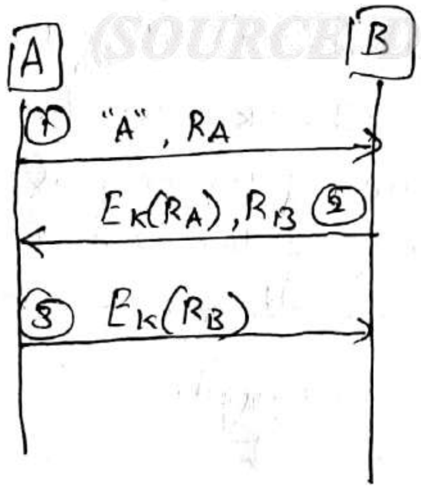
If they match, he concludes that A has used the private key corresponding to the public key in her Certificate. Assuming that A's private key is safely protected, she must be the entity who created the correct response in Msg 3.

* Fig b:
  * Here B Chooses a nonce, R and encrypts it with A's public key to create the challenge. A decrypts the Challenge and sends it to B. Authentication of A to B Succeeds if what B receives in Msg3 is R, the nonce he just Chose.

MUTUAL AUTHENTICATION

* It is often necessary for both communicating parties to authenticate themselves to each other.

1. Shared Secret-based authentication.

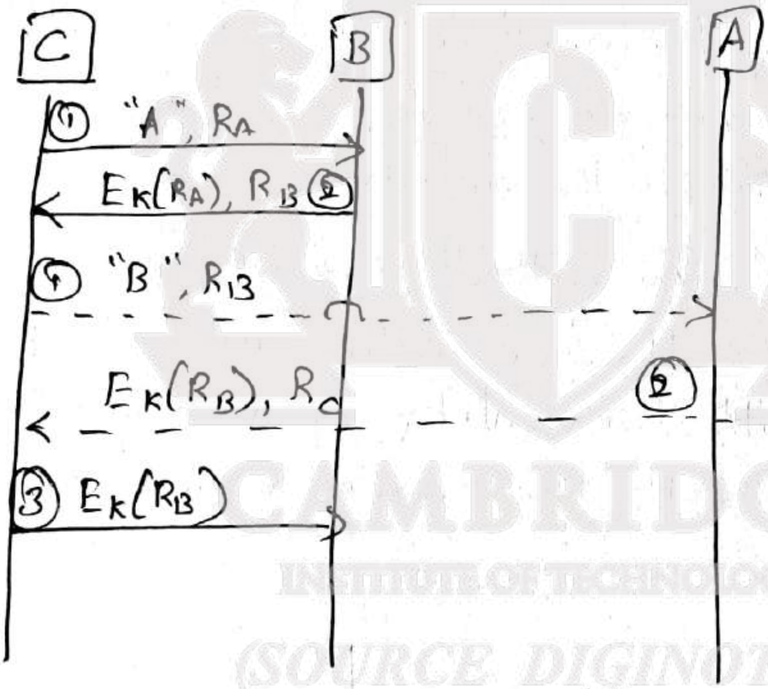


a) Flawed protocol.

* Fig a: In Msg 1, A communicates its identity and its challenge in the form of a nonce R_A.

* In msg 2, B responds to the challenge by encrypting R_A with the common secret, K that A & B Share.

* B also sends its own challenge, R_B to A. A's response to B's challenge in the third message appeals to complete the protocol for mutual authentication.



(b) parallel session Attack.

* fig b : Attack scenario is as follows;

* Msg 1 : An attacker, C, sends a msg to B containing a nonce R_A and claiming to be A.

* Msg 2: B responds to the challenge with $E_K(R_A)$ and its own challenge R_B as required by the above protocol.

- * Msg1: Now "C" attempts to connect to A claiming it is B with a challenge R_B. Note that this is the same challenge offered to it by B in Msg 2.

- * Msg2 : A responds to the challenge with $E_K(R_B)$ and a nonce of its own.

- * Msg3 : C uses A's response $E_K(R_B)$ to complete the 3 msg authentication protocol with B.

C has successfully impersonated A to B.

- * This attack is termed a Reflection Attack since a part of the msg received by an attacker is reflected back to the victim.

- * This attack is also called a parallel session Attack since the attacker, in the midst of a protocol run with one entity, opens another protocol run or session with the same or another entity.

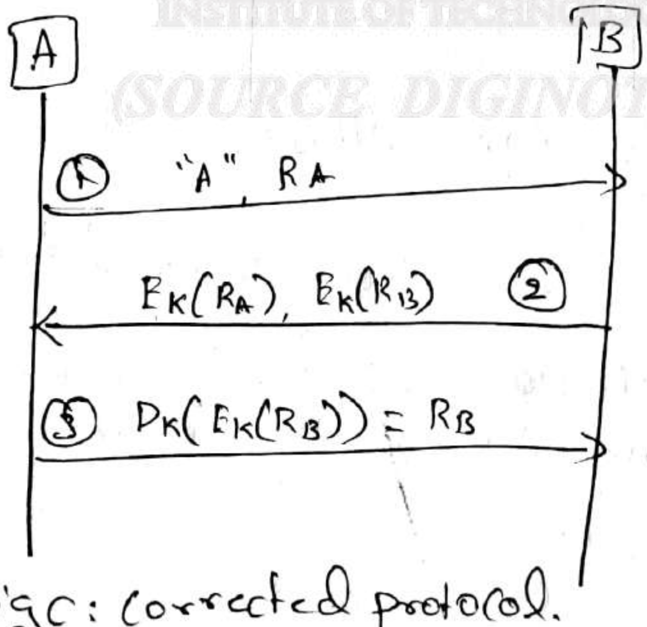


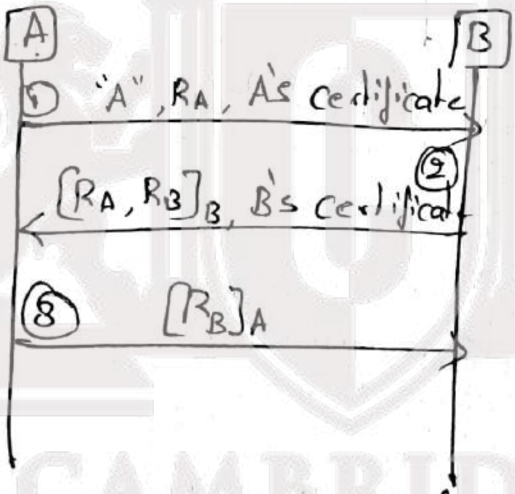
Fig c: corrected protocol.

* Fig c: possibility is to have the initiator and responder handle challenges differently.
For example, the protocol might require the responder to encrypt his challenge, while the initiator would be required to decrypt her challenge.

2. Asymmetric key-based authentication.

* Assume that both A & B have public/private key pairs.

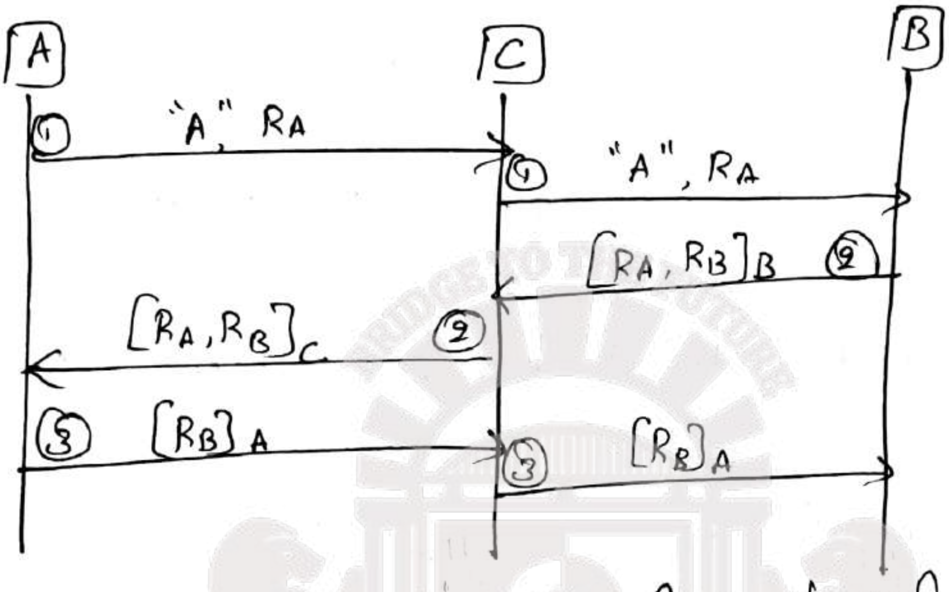
*



a) flawed protocol.

* Fig a: Each party transmits its own nonce & challenges the other to sign it.
* Notation $[m]_A$ => m, sent in the clear together with A's signature on m.
* Msg2: The string obtained by concatenating nonces RA & R_B is signed by B. Both the nonces and the signature are sent.

* Msg 3: Nonce R_A is the challenge provided by A. R_B is the challenge provided by B and signed by A in response.



b) Attack on flawed protocol.

Fig b:

Msg 1: A initiates communication with C, sending her challenge R_A.

Msg 1: C initiates communication with B using the same nonce R_A supplied by A.

Msg 2: B responds to "A"s challenge & includes a challenge of his own R_B.

Msg 2: C responds to A's challenge and uses B's nonce, R_B as his challenge to A.

Msg 3: A responds to C's challenge (which was actually generated by B). A thus completes the mutual authentication protocol with C.

Msg 4: C forwards A's response to B.

- Analyze the above protocol(fig b)

- A does intend to communicate with C(otherwise A would not have responded in msg 3 to C's challenge that was transmitted in msg 2).

- B wishes to communicate with A. Otherwise B would not have responded in msg2 to the nonce presented in msg1.

note: msg 1 is sent by C but it includes , A's identity, who is C? .
C is probably known to A. After all, A intends to talk to C. But C is also the attacker here. when A initiates communication with C, the later seizes the opportunity & attempts to convince B that A intends to talk to him. B responds to what appears to be A's intention to communicate with him. note that, in the current scenario, A may not wish to communicate with B & is not aware that C is attempting to do so on her behalf. yet after B receives msg 3, he feels A intends to communicate with him since msg 3 contains her signature on a nonce chosen by him.

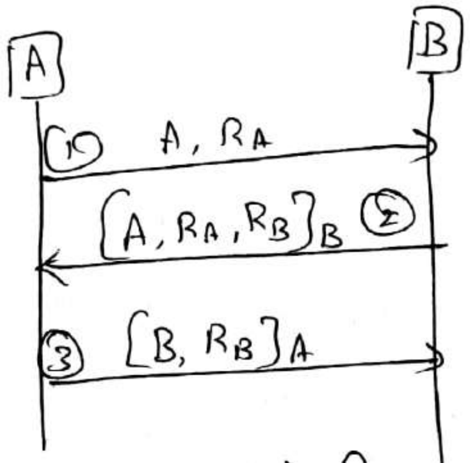


Fig c: corrected protocol.

* Fig c: soln is for the sender to include the identity of the recipient in all msges signed by him. note that with this modification, msg 3) would be $[C, R_B]_A$ in fig b. If C tries to forward this msg to B, the latter ll smell a rat since it is C's identity that is included in the msg. so B ll realize that the msg was intended for C, not for him.

3. Authentication and Key Agreement.

* shows protocols providing both mutual authentication and key agreement.

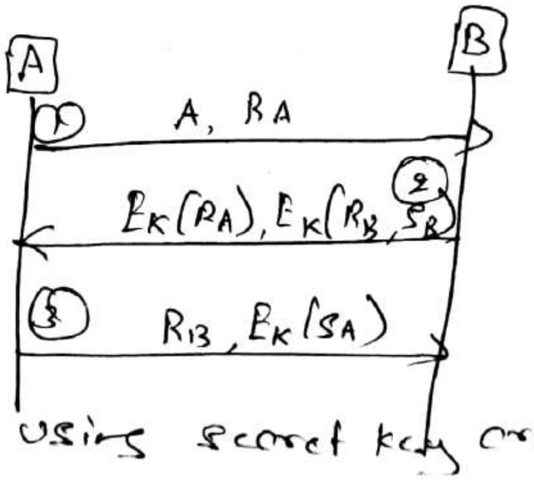
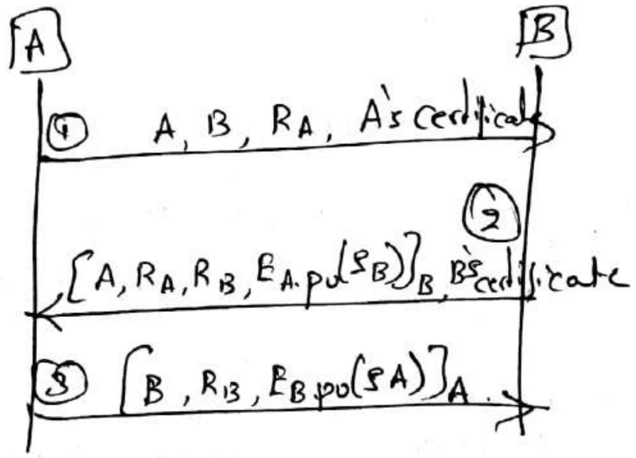


Fig a: using secret key cryptography


A
B
① A, B, R_A, A's certificate
② [A, R_A, R_B, $E_{A.pu}(S_B)$]$_B$, B's certificate
③ [B, R_B, $E_{B.pu}(S_A)$]$_A$

b. using public key cryptography.

- Session key = $S_A \oplus S_B$.

* Fig a: uses secret key cryptography
Fig b: uses public key cryptography.

* In both the figures, S_A & S_B are the contributions to the secret key by A & B respectively.

* They are freshly chosen random numbers that are encrypted & sent so that they cannot be earesdropped upon.

* In fig a, they are encrypted in msg 2 & 3 by the shaled secret k.

* In fig b, they are encrypted in msg 2 & 3 using the recipient's public key.

* The key finally chosen could be a simple function of S_A & S_B for example $S_A \oplus S_B$.

4. Use of Timestamps.

* The use of nonces was introduced as a means to prevent replay attacks.

* An alternative to nonces are timestamps.

* Timestamps : Stamping a msg with the current time, we convince the receiving party of its freshness.

* Figure shows the use of timestamps in conjunction with public key cryptography for authentication.

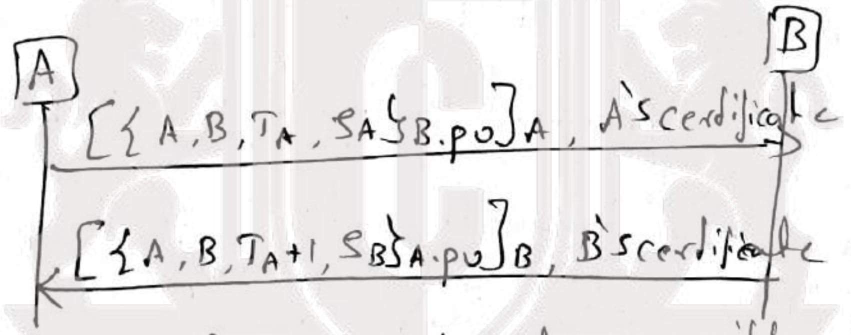

A
B
$[\{A, B, T_A, S_A\}_{B.pu}]_A$, A's certificate
$[\{A, B, T_A+1, S_B\}_{A.pu}]_B$, B's certificate.

Fig:- Mutual authentication with timestamps.

* Msg 1: A inserts a timestamp, T_A, in her msg & signs it.

* B, on receiving the msg, checks whether the timestamp is sufficiently recent and then verifies the signature. He increments the received timestamp inserts it into his response msg to A & signs the msg.

Notation $\{m\}_{x.pu}$ — m encrypted using the public key of x.

IPsec- Security at the Network Layer

- Security at different layers: Pros and Cons.
- IPsec in Action.
- Internet Key Exchange (IKE) protocol.
- Security Policy and IPsec.
- Virtual Private Networks.

IPsec in action

- IP-level security encompasses three functional areas:

1. **Authentication:** Assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header.
2. **Confidentiality:** Assures that the packet has not been altered in transit.
3. **Key management:** It is concerned with the secure exchange of keys.

Applications of IPsec

- IPsec provides the capability to secure communication across a LAN, across private and public WANs, and across the Internet.

Examples:

- **Secure branch office connectivity over the Internet:** A company can build a secure VPN over the internet.
- **Secure remote access over the Internet:** An end user whose system is equipped with IP security protocols can make a local call to an ISP and gain access to a company network.
- **Establishing extranet and intranet connectivity with partners:** It can be used to secure communication with other organizations, ensuring authentication, confidentiality & providing key exchange.
- **Enhancing electronic commerce security:** Even though some web and electronic commerce applications have built in security protocols the use of IPsec enhances that security.

Benefits of IPsec

- IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- There is no need to change software on a user or server system when IPsec is implemented in the firewall or router.
- IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying materials or revoke keying material when users leave the organization.
- IPsec can provide security for individual users if needed.

Source diginotes.in

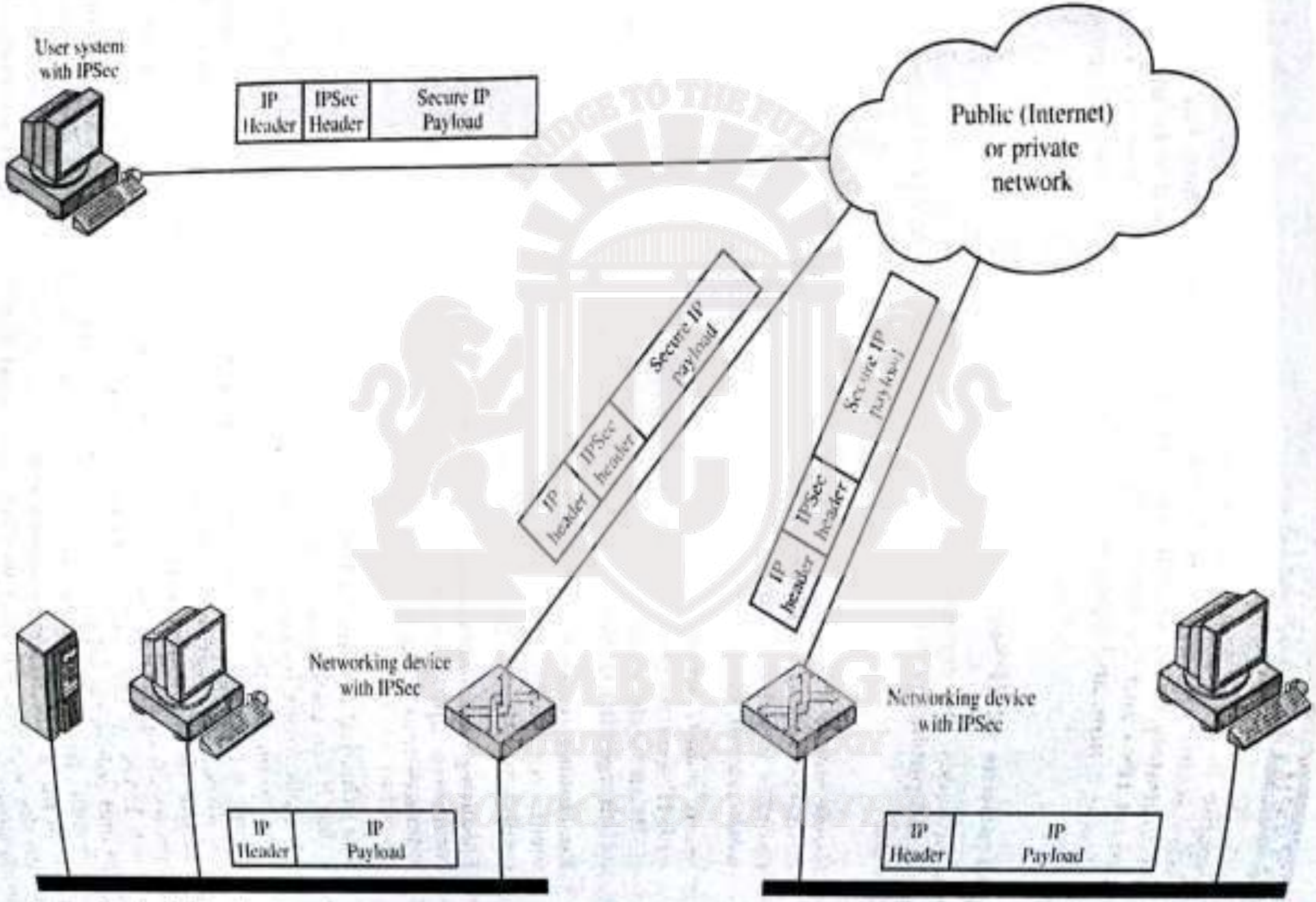


Figure 6.1 An IP Security Scenario

IPsec Services

- The services are

1. Access control.
2. Connectionless integrity.
3. Data origin authentication.
4. Rejection of replayed packets.
5. Confidentiality.
6. Limited traffic flow confidentiality.

Security Associations

- An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.
- If a peer relationship is needed, for two-way secure exchange, then two security associations are required.
- Each node has a database of SAs for all connection originating from or terminating at it. This database is referred as SA database.

- A SA is uniquely identified by three parameters:

1. **Security Parameters Index(SPI):** SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
2. **IP Destination Address:** This is the address of the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.
3. **Security Protocol Identifier:** This indicates whether the association is an AH or ESP security association.

SA Parameters

- Sequence number counter.
- Sequence counter overflow.
- Anti-replay window.
- AH Information.
- ESP Information.
- Lifetime of this security association.
- IPsec protocol mode.

Transport mode

- Transport mode is used for end-to-end communication between two hosts.
- When host runs AH or ESP over IPv4, payload is the data that normally follow the IP header.
- For IPv6, the payload is the data that normally follow both the IP header and any IPv6 extensions headers that are present, with the possible exception of the destination options header, which may be included in the protection.
- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- AH in transport mode authenticates the IP payload and selected portions of the IP header.

Tunnel mode

- Tunnel mode provides protection to the entire IP packet.

- To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP header.

- The entire original or inner packet travels through a tunnel from one point of an IP network to another: no router along the way are able to examine the inner IP header because the original packet is encapsulated, the new larger packet may have totally different source and destination addresses adding to the security.

- Tunnel mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPsec.

IPsec protocols: AH and ESP

- The authentication header provides support for data integrity and authentication of IP packets.

- AH consists of the following fields

1. **Next header:** Identifies the type of header immediately following this header.
2. **Payload length:** Length of AH in 32-bit words, minus 2.
3. **Reserved:** For future use.
4. **Security parameters index:** Identifies a SA.
5. **Sequence number:** A monotonically increasing counter value.
6. **Authentication data:** A variable length field that contains the integrity check value or MAC for this packet.

Source diginotes.in

ESP format

- Encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentiality.

- ESP contains the following fields:

1. **Security parameters Index:** Identifies a security association.
2. **Sequence number:** A montonically increasing counter value, this provides an anti-replay function.
3. **Payload data:** This is a transport level segment or IP packet that is protected by encryption.
4. **Padding:** If an encryption algorithm require the plaintext to be a multiple of some number of bytes, the padding field is used to expand the plaintext to the required length.

Source diginotes.in

5. Pad length: Indicates the number of pad bytes immediately preceding this field.

6. Next header: Identifies the type of data contained in the payload data field by identifying the first header in that payload .

7. **Authentication data:** A variable length field that contains the integrity check value computed over the ESP packet minus the authentication data field.

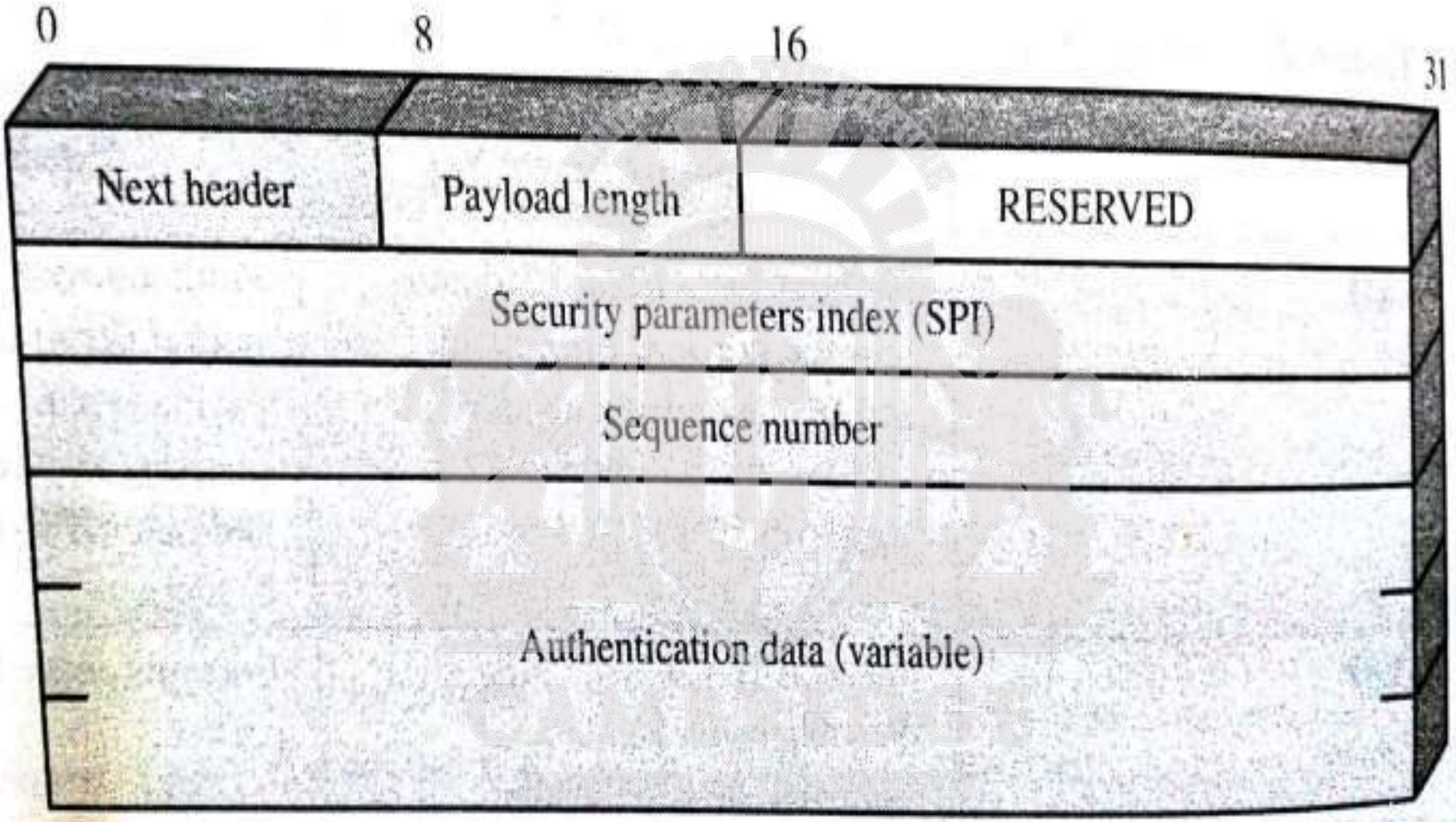

0
8
16
31
Next header
Payload length
RESERVED
Security parameters index (SPI)
Sequence number
Authentication data (variable)

Figure 6.3 IPSec Authentication Header

Source diginotes.in

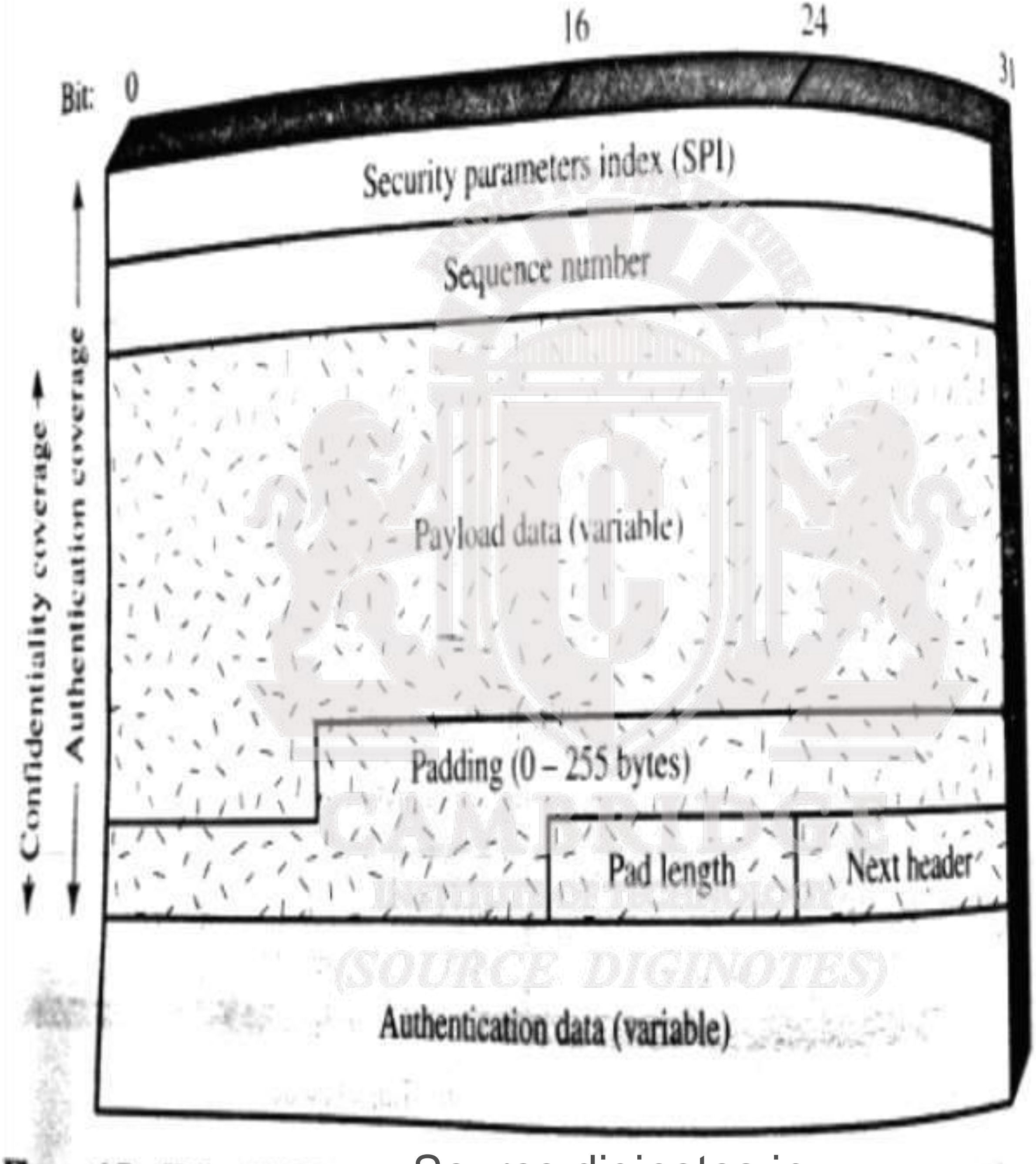
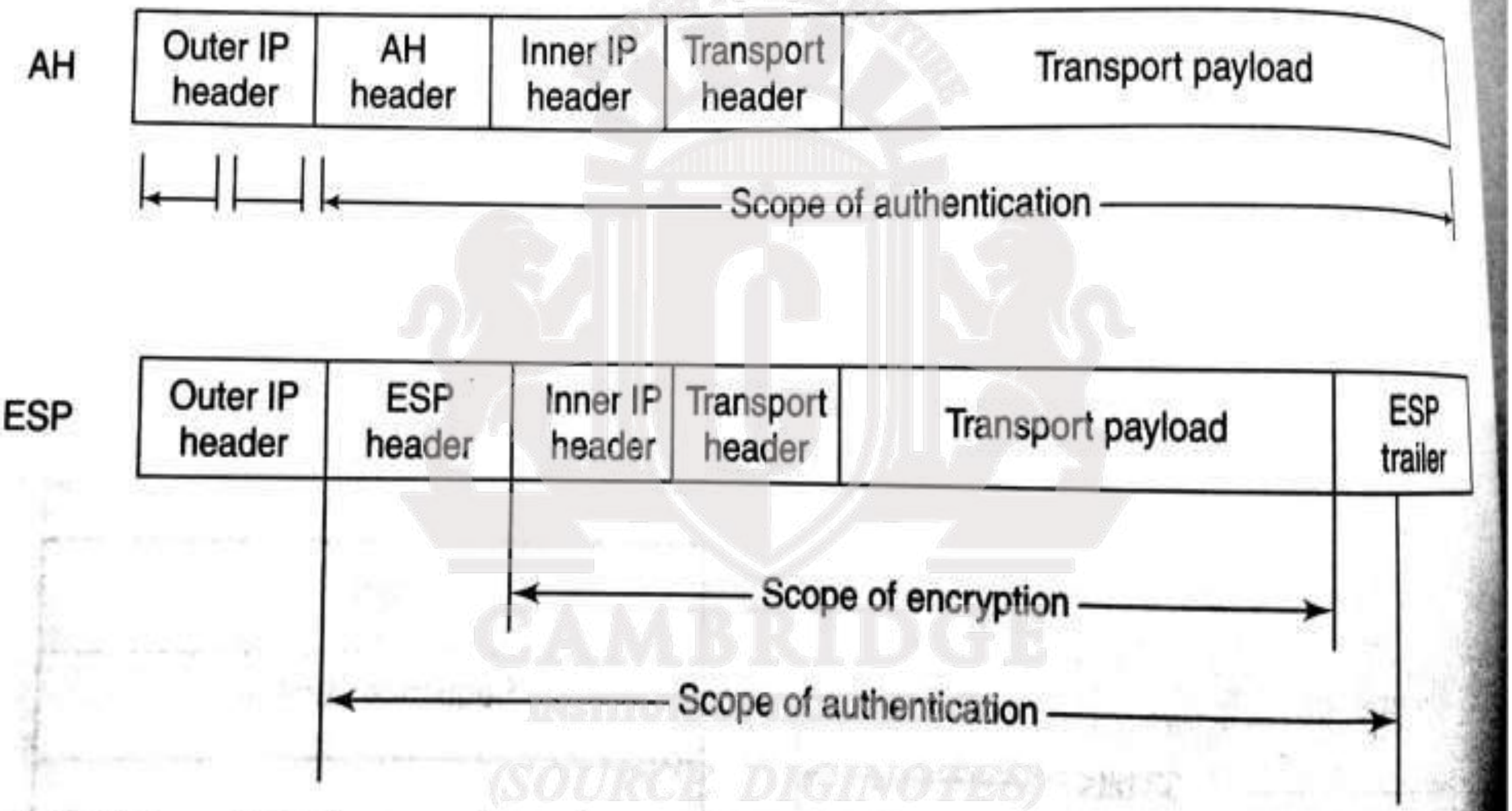


Figure 6.7 IPSec ESP format



3.2 *AH and ESP in tunnel mode*

Source diginotes.in

Internet key exchange protocol

- The main goal of IKE is to establish an SA between two parties that wish to communicate securely using IPsec.
- IKE is an application layer protocol using the connectionless UDP protocol.
- IKE borrows heavily from two major sources- the Internet security association and key management protocol (ISAKMP) and oakley.
- ISAKMP defines formats of various entities such as the digital signature and the digital certificate.
- It also specifies the rules for stringing payloads together to form a valid msg.
- Oakley specifies the kind of information to be exchanged in each message that is part of IKE.

Internet key exchange

- Purpose

1. Mutual authentication.
2. Shared secret establishment.
3. Crypto algorithms negotiation.
4. Security association establishment.

IKE is composed of two phases.

- In the first phase, an IKE SA is established. This creates a secure channel upon which the communicating parties can then established multiple IPsec SA instances over time.
- It is good security practice to periodically change cryptographic keys used by two communicating parties.
- In phase 1, long term keys are derived.
- In phase 2, shorter term keys are derived for use between two parties. This key is a function of the long term keys computed in phase 1 together with nonce exchanged in phase 2.
- Key agreement use DHKEP, unauthentication key exchange is vulnerable to man-in middle attacks and session hijacking.
- Attacker could induce its victim to compute useless modular exponentiation leading to a DOS attack.
- It is designed to withstand these attacks while at the same time offering a menu of different cryptographic algorithms and authentication methods.

IPsec Cookies

- To thwart DOS attack, IKE makes extensive use of cookies.
- One cookie is created by the initiator A and another by the responder B.
- Phase 1 of IKE uses DHKE, an attacker creates many spurious messages each one being a request to set up an IKE SA with B.
- A spoofed IP source address is used in each of these messages.
- The responder would have no ways of knowing that the message are spoofed.
- To frustrate such attacks, IKE mandates that B should compute a 64-bit integer called a cookie.
- **Cookie:** It is a hash function of many variables including the IP address of A, an secret know only to B and possibly the time.

- A required to send this cookie to B in all subsequent messages.
- In general this cookie will be different for different IP address.
- On receipt of a message from A, B will check to see whether the cookie corresponds to A’s IP address.
- If the check fails, B will abort session establishment and hence avoid performing the modular exponentiation.
- The attacker will have no way to spoof the cookie created in response to a request from A.
- The pair (Ca, Cb) plays the role in IKE.

IKE phase 1

- The following are accomplished in IKE phase 1:

1. The authentication method, encryption and hash algorithms together with the diffie- hellman group to be used are negotiated.
2. Both parties authenticate themselves to each other.
3. Keys, key(a) and key(e) are computed. These keys are used for message integrity protection and encryption respectively in both phase 1 and phase2.
4. Cookies are created at the start of phase 1 and serve the purpose of an IKE connection identifier.

Phase 1 use one of two modes

- Main mode: 6 messages, mutual authentication, session key establishment, hiding endpoint identity, negotiating cryptographic algorithms.
- Aggressive mode: 3 messages, mutual authentication, session key establishment.

- The motivation for introducing main mode is to hide the identities of sender and receiver from eavesdroppers.
- The main mode of IKE seeks to protect the confidentiality of these alternative forms of identification through encryption.
- To perform mutual authentication, IKE assumes that either A and B share a secret or A and B each have a public key private key pair.
- There are two ways in which A and B might prove knowledge of their private keys by signing a message(signature private key) or by decrypting a challenge(decryption private key).

Main mode

1. Option 1: A and B share a secret key(s).

2. Option 2: A and B each have private signing keys.

3. Option 3: A and B each have private decryption keys.

Option 1:

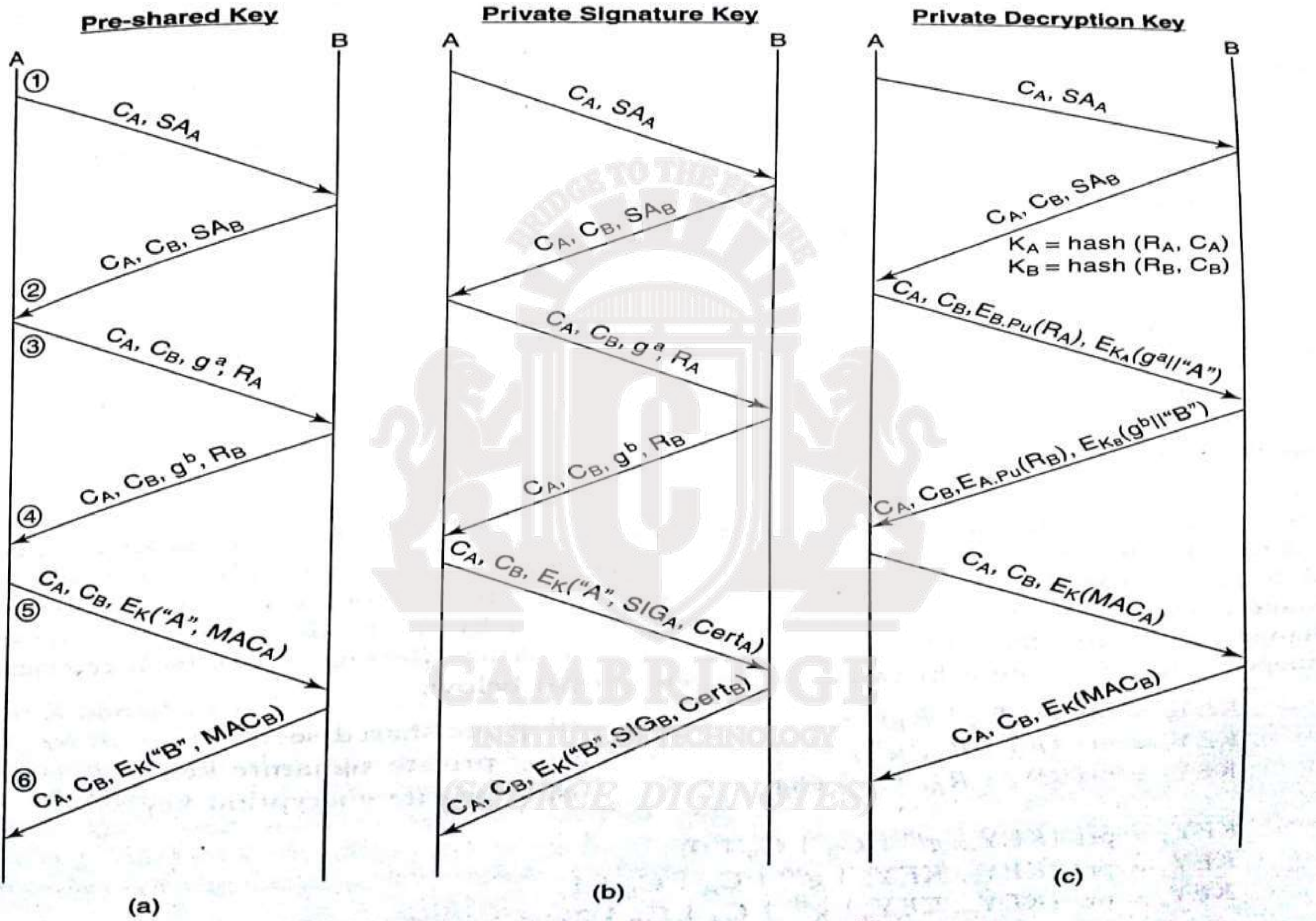
- The sequence of messages exchanged between A and B under the assumption that A and B share a secret keys.
- MSG1: Contains the cryptographic algorithms proposed by A for use in the IKE SA in addition to the cookie Ca, denoted by Sa.
- MSG2: Cryptographic algorithms accepted by B.
- MSG 3 & 4: Both side exchange nonce and the diffie- hellman partial keys.
- MSG 5 & 6: A and B independently compute a hierarchy of secrets.
- Both A and B use a MAC for message authentication and integrity.
- MSG 5 & 6, both sides reveal their identities to one another.
- Messages are encrypted with Key(e) .
- Major drawback is with shared secret.
- Alternatively B, could keep track of all entities that it expects to communicate with from each IP address.

Option 2:

- The main difference is that authentication and integrity protection of messages is by digital signature on MAC(a) and MAC(b) using their private keys.
- A and B dispatch their signing key certificate in MSG 5 and MSG 6 so that other party can perform signature verification.

Option 3:

- Both sides exchange their identities earlier in message 3 &4.
- Each side generate a nonce and encrypts it with the other side’s public key.
- Each side encrypts its identity together with its DH partial key with temporary keys K(a) and k(b).
- MSG 5 & 6, each side transmits a MAC.
- An incorrect MAC would be detected by the other party and would result in the IKE exchange being aborted.


Pre-shared Key
A
B
①
C_A, SA_A
C_A, C_B, SA_B
②
③
C_A, C_B, g^a, R_A
C_A, C_B, g^b, R_B
④
⑤
$C_A, C_B, E_K(\text{“A”}, MAC_A)$
⑥
$C_A, C_B, E_K(\text{“B”}, MAC_B)$
(a)
Private Signature Key
A
B
C_A, SA_A
C_A, C_B, SA_B
C_A, C_B, g^a, R_A
C_A, C_B, g^b, R_B
$C_A, C_B, E_K(\text{“A”}, SIG_A, Cert_A)$
$C_A, C_B, E_K(\text{“B”}, SIG_B, Cert_B)$
(b)
Private Decryption Key
A
B
C_A, SA_A
C_A, C_B, SA_B
$K_A = \text{hash}(R_A, C_A)$
$K_B = \text{hash}(R_B, C_B)$
$C_A, C_B, E_{B.Pu}(R_A), E_{K_A}(g^a||\text{“A”})$
$C_A, C_B, E_{A.Pu}(R_B), E_{K_B}(g^b||\text{“B”})$
$C_A, C_B, E_K(MAC_A)$
$C_A, C_B, E_K(MAC_B)$
(c)

13.4 *IKE phase 1 (main mode)*

Aggressive mode

- Identities of the communicating parties are no longer hidden from passive eavesdroppers.
- Diffie – hellman group used and the group parameters are decides by A.
- A chooses a group, computes its partial key and sends it to B in MSG 1.
- B has no choice but to accept the group chosen by A.

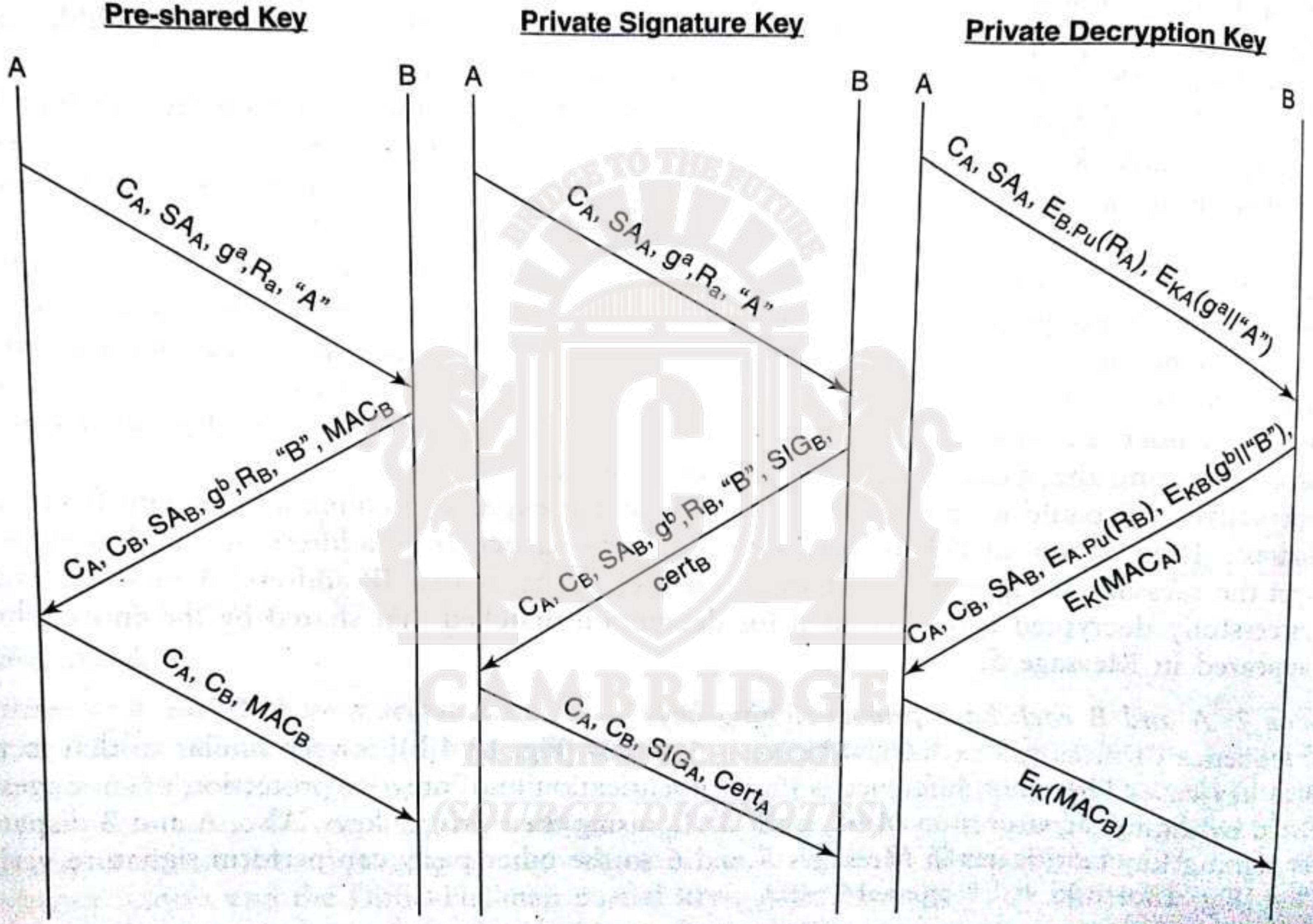

Pre-shared Key
A
B
C_A, SA_A, g^a, R_a, "A"
C_A, C_B, SA_B, g^b, R_B, "B", MAC_B
C_A, C_B, MAC_B
Private Signature Key
A
B
C_A, SA_A, g^a, R_a, "A"
C_A, C_B, SA_B, g^b, R_B, "B", SIG_B, $cert_B$
$C_A, C_B, SIG_A, Cert_A$
Private Decryption Key
A
B
$C_A, SA_A, E_{B.Pu}(R_A), E_{KA}(g^a||$"A"$)$
$C_A, C_B, SA_B, E_{A.Pu}(R_B), E_{KB}(g^b||$"B"$)$, $E_K(MAC_A)$
$E_K(MAC_B)$

Figure 13.5 *IKE phase 1 (aggressive mode)*

IKE phase 2

- With existing IKE SA, two parties participate in an IKE phase 2exchange in order to establish a new IPsec SA.
- Fig shows the 3 messages exchanged in quick mode.
- All messages are encrypted using the secret key(e) computed in the previous phase.
- Message integrity and data source authentication is provided by using an HMAC. The key for the HMAC is key(a) also computed in phase 1.
- A 32-bit message ID (MID) together with the two cookies Ca and Cb are dispatched as part of each of the three messages.
- Both sides send their proposals of cryptographic algorithms to be used in the IPsec SA. These are denoted SA(a) and SA(b).
- To guarantee freshness both sides also generate and transmit nonces, Na and Nb.
- Is to agree on the secrets to be used for authentication and encryption as part of the IPsec SA. These secrets are computed simultaneously by both sides and are a function of KEY(d) computed in phase 1 and the nonces.

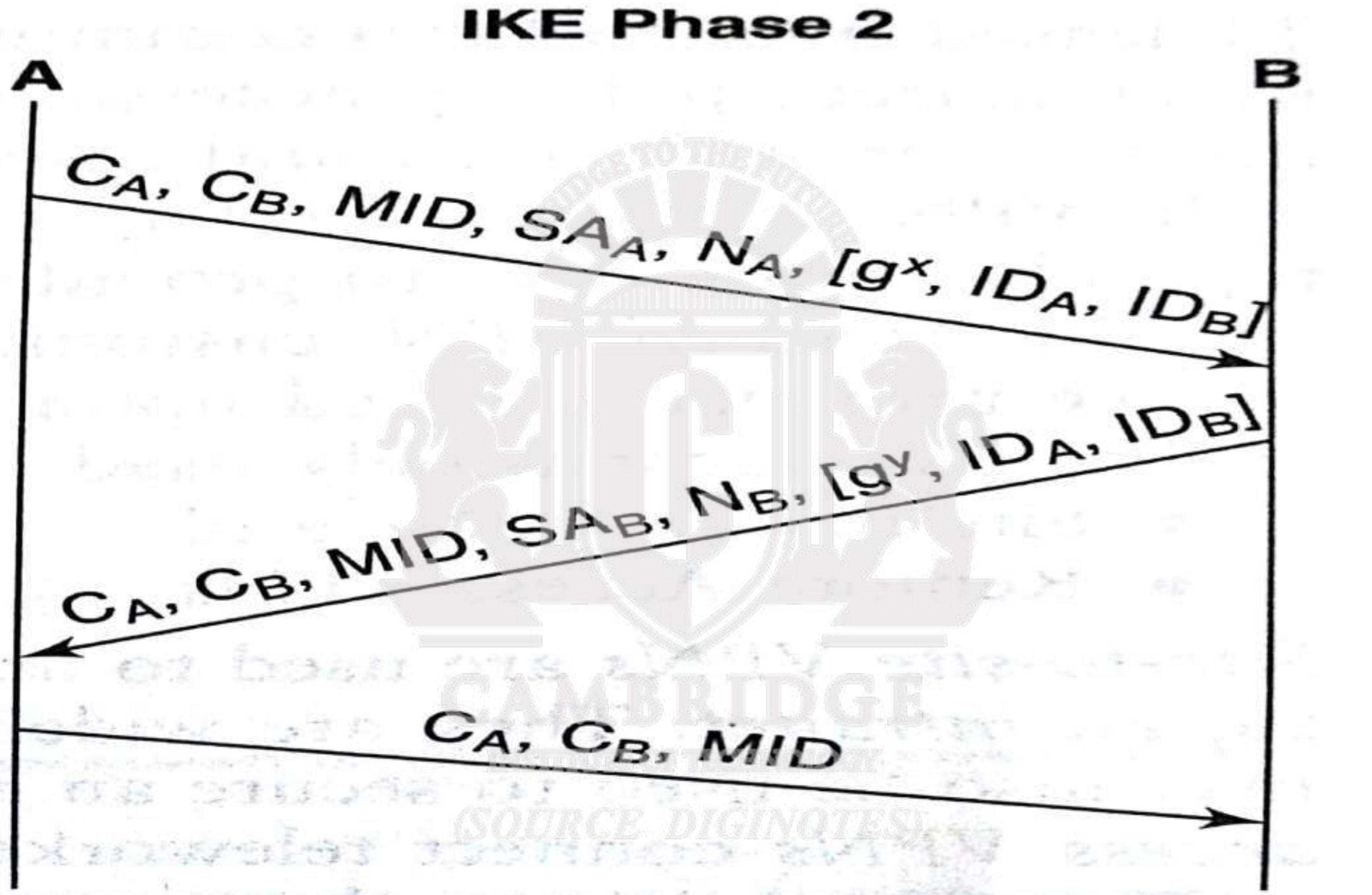

IKE Phase 2
A
B
C_A, C_B, MID, SA_A, N_A, [g^x, ID_A, ID_B]
C_A, C_B, MID, SA_B, N_B, [g^y, ID_A, ID_B]
C_A, C_B, MID

Figure 13.6 *IKE phase 2*

Source diginotes.in

Security policy and IPsec

- Security policy database(SPD) is used to determine whether a packet sent or received should pass through, bypass it, or simply be dropped.
- Decision is made based on fields in the IP and transport headers.
- These fields called selectors include the destination IP address, the type of transport layer protocol and the type of application.
- Selectors are used to index into the SPD.
- The output indicates whether security should be applied.
- If the packet is part of the IP traffic that already has an existing SA, then the SPD returns a pointer to that SA.
- If an SA does not exist or has expired, the IKE protocol is used to establish an SA between the sender and receiver.

Virtual private networks

- VPN enables organizations to communicate securely over a public, shared network such as the internet.

- One possibility is to use dedicated point-to-point lines such as T1 leased lines to keep communications confidential.

- IPsec is just the protocol that helps secure IP traffic over such open and insecure networks.

- A secure VPN uses cryptographic techniques to provide not just confidentiality but also authentication and message integrity.

- In trusted VPN, customer traffic is not usually encrypted. Instead the infrastructure of the service provider is relied upon to guarantee confidentiality of the traffic.

- The two most widely used VPNs are

1. Site-to-site VPNs
2. Remote access VPNs.

- Site-to-site VPNs are used to link multiple offices of an organization in, commonly referred to as intranet.

- It is also used to secure an extranet- a network connecting multiple business partners.

- Remote access VPNs connect teleworkers(mobile users or users from home) to their offices.

IEEE 802.11 wireless LAN Security

* There are two principal types of WLANs

* Adhoc networks, where stations communicate directly with each other.

* Infrastructure WLANs, which use an access point.

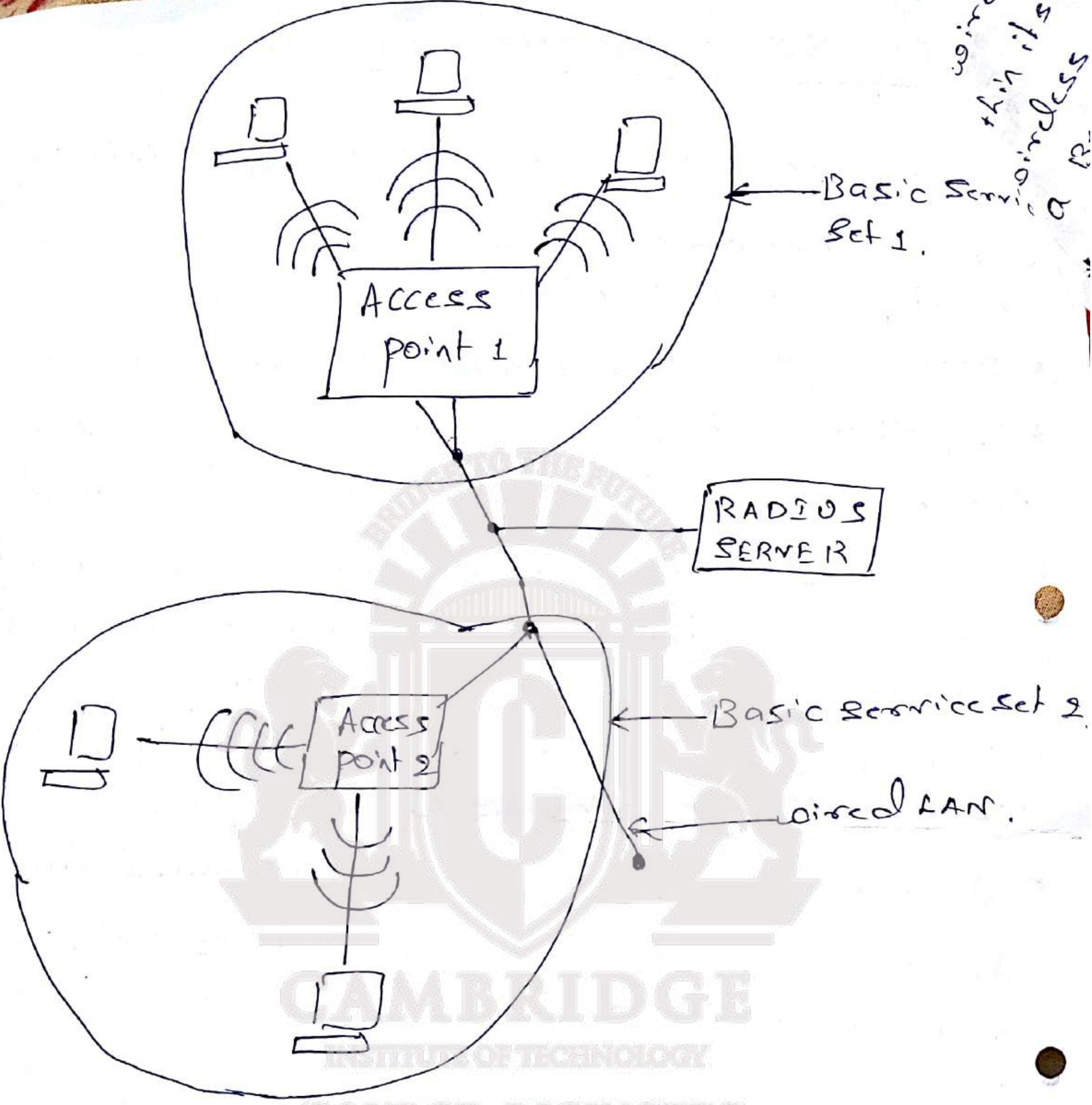
* A station first sends a frame to an Ap and the Ap then delivers it to its final destination.

* The destination may be another wireless statio Alternatively, it may be a station on the wired network that the Ap is connected to.

* The Ap thus serves as a bridge b/w the WLAN & the existing wired n/w.

* A n/w of wireless stations associated with an Ap is referred to as a basic service set. such a n/w may be adequate for a home or small enterp se.

* In a large building or campus all stations may not fall in the range of a single Ap. It ll be necessary to have several Aps to cater to the stations dispersed over a set of buildings. For example: The Aps in the different basic service sets are often connected over a wired n/w.



Fig!- Infrastructule wireless LAN.

- The union of the basic service sets comprises an extended service set (ESS).
- Each station and AP in the ESS is uniquely identified by a MAC address, a 48-bit quantity.
- Each AP is also identified by an SSID (service set ID), which is a chalacter string of length at most 32 chalacters.

wireless station, needs to first discover an AP within its range. This can be done by monitoring the wireless medium for a special kind of frame called a Beacon, which is periodically broadcast by the AP.

* The Beacon usually contains the SSID of the broadcasting AP.

* Alternatively a station may send a probe Request frame. An AP, on healing such a request, responds with a probe Response frame. The probe Response frame contains the SSID of the AP and also information about its capabilities, supported data rates etc.

* To become part of the WLAN, a station ll have to associate with an AP. At any point in time a station can associate with only one AP.

* A station that wishes to associate with an AP sends it an Associate Request frame. The AP replies with an Associate Response frame if it accepts the request for associating with it.

AUTHENTICATION.

1. pre-WEP Authentication.

* knowledge of the SSID sufficed for a station to be authendicated to the AP.

* However, an attacker could easily sniff the value of SSID from frames such as the beacon or probe response & then use it for authentication.

* Another approach was to restrict admission to the WLAN by MAC address. The AP would maintain a list of MAC addresses of stations permitted to join the WLAN.

* valid MAC addresses could be obtained by sniffing the wireless medium. The attacker could then modify his nic card to spoof a valid MAC address. so neither of these approaches helped.

2. Authentication in WEP.

* The station authenticates itself to the AP using a challenge-response protocol.
* The AP Generates a challenge (nonce) and sends it to the station.
* The station encrypts the challenge and sends it to the AP.
* The stream cipher, RC4 is used for encryption.
* The station computes a keystream, which is a function of a 40-bit Shared secret s and a 24-bit IV.
* The Challenge is then XORed with the keystream to create the response.

$$\text{RESPONSE} = \text{CHALLENGE} \oplus \text{KEYSTREAM}(S, \text{IV})$$

* All an attacker needs to do is to monitor a challenge-response pair. From this, he can compute the keystream. To authenticate himself to the Ap, he needs to XOR the challenge from the Ap with the computed keystream.

* It may also be possible for an attacker to obtain S itself. By eavesdropping on several challenge-response pairs b/w the Ap and various stations, an attacker could launch a dictionary attack & eventuall obtain S.

* Note: There is no support for authenticating the Ap to a station, so door to man-in-the-middle addacks.

3. Authentication and key Agreement in 802.11i.

a. Authentication.

* 802.11i uses IEEE 802.1x - a protocol that supports authentication at the link layer. Three entities are involved:

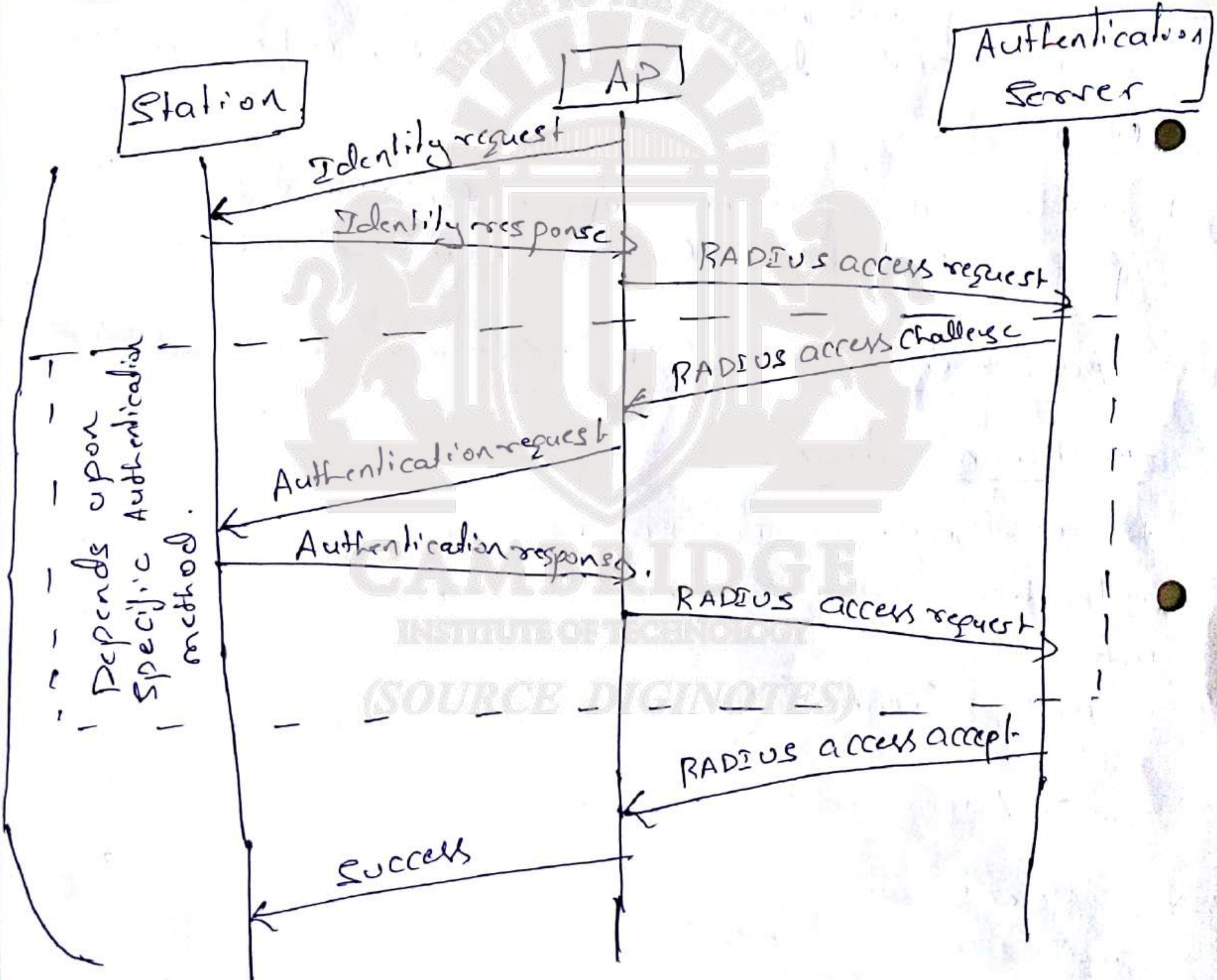
a. supplicant (the wireless station)

b. Authenticator (the Ap)

c. Authentication server.

* Different authentication mechanisms and message types are defined by IETF's Extensible Authentication protocol (EAP).

- EAP is not really an authentication protocol but rather a framework upon which various authentication protocols may be supported.
- EAP exchanges are mostly comprised of requests and responses.
- The Generic authentication messages in IEEE 802.11i are shown below.



EAPOL = EAP over LANs
EAP = Extensible Authentication protocol.

Fig:- Authentication and master session key exchange in 802.11i.

* The protocol used b/w the station and the Ap is EAP but that used b/w the Ap & the As depends upon the specifics.

* As is often a RADIUS Server which uses its own message types & formats.

* RADIUS stands for Remote authentication Dial in User Service. It is a client-Server protocol used for authentication, authorization and accounting.

● The main authentication methods supported by EAP include the following:

EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP.

* EAP-MD5: The Most basic of the EAP authentication methods.

1. The authentication Server challenges the station to transmit the MD5 hash of the user's password

● 2. The station prompts the user to type his/her password. It then computes the hash of the password & sends this across.

3. Attacker could eavesdrop on such a msg exchange and then replay the hashed password thus impersonating the owner of the password. This method does not support authentication of the Ap to the Station.

* EAP-TLS: 1) It is the most secure and provides mutual authentication and agreement on a master session key.

2) It requires the AP as well as the user(station) to have digital certificates.

3) It is relatively straightforward to equip each AP with a DC and a corresponding private key but extending the PKI to each user of the WLAN may not be feasible.

* EAP-TTLS:

1) It requires certificates only at the AP end.

2) The AP authenticates itself to the station & both sides construct a secure tunnel b/w themselves.

3) over this secure tunnel, the station authenticates itself to the AP.

4) The station could transmit attribute-value pairs such as

user_name = ramesh

password = 4rp#mNaS27

5) Note: the station really authenticates itself to the RADIUS server - the AP merely forwards the authentication information to the RADIUS server.

* EAP-protected EAP (PEAP):

1) In PEAP, the secure tunnel is used to start a second EAP exchange wherein the station authenticates itself to the authentication server.

b. Key Hierarchy.

* Two types of keys used in WLANs.

1) pairwise keys: used to protect traffic between a station and an AP.

2) Group key: used to protect broadcast or multicast traffic between an AP and multiple stations.

* The root of the key hierarchy is the pairwise Master key (PMK). This is obtained in one of two ways.

1) MSK [Master Session key]

2) PSK [pre-shared key]

MSK: The station and the authentication server may agree on a MSK. The authentication server then communicates this key to the AP. The AP and station then derive the PMK from the MSK.

PSK: An alternative to computing a fresh PMK for each session is the pre-shared key (PSK), which is used as the PMK.

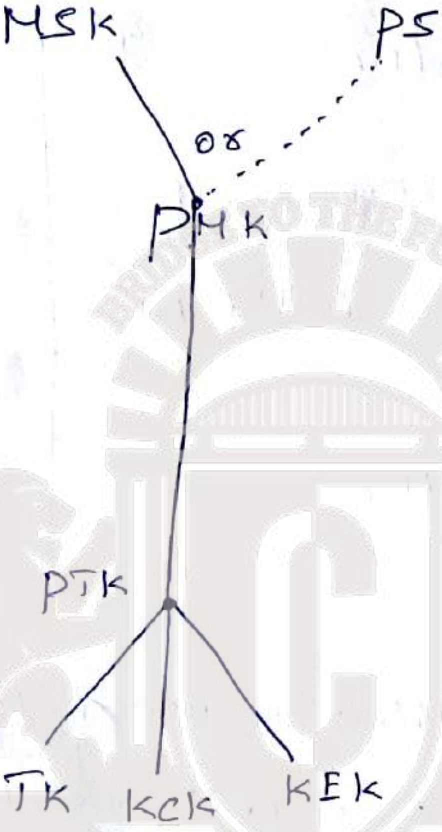
- The 256-bit PMK is used to derive a 384-bit pairwise Transient key (PTK).
- PTK is a pseudorandom function of the PMK, two nonces chosen by the AP, and the station and their MAC addresses.
- By deriving the PTK in this fashion, key refreshing can take place without the overhead of negotiating a new PMK.
- Three 128-bit chunks are extracted from the 384-bit PTK for the following purposes:

1) A Temporal key (TK): It is used for both encryption and integrity protection of data between the AP and the station.

2) A key confirmation key (KCK): It is used to integrity-protect some of the messages in the four-way handshake. Integrity protection is supported by a MAC computed as a function of the message and the KCK.

3) A key Encryption key: It is used to encrypt the message containing the group key.

*Figure: The key hierarchy in 802.11i is Summari



KEK = key confirmatio key.

MSK = Master session key.

PSK = pre-shared key

PMK = pairwise Master key.

PTK = pairwise transien key.

TK = Temporal key.

KCK = key confirmation key.

Four-way handshake.

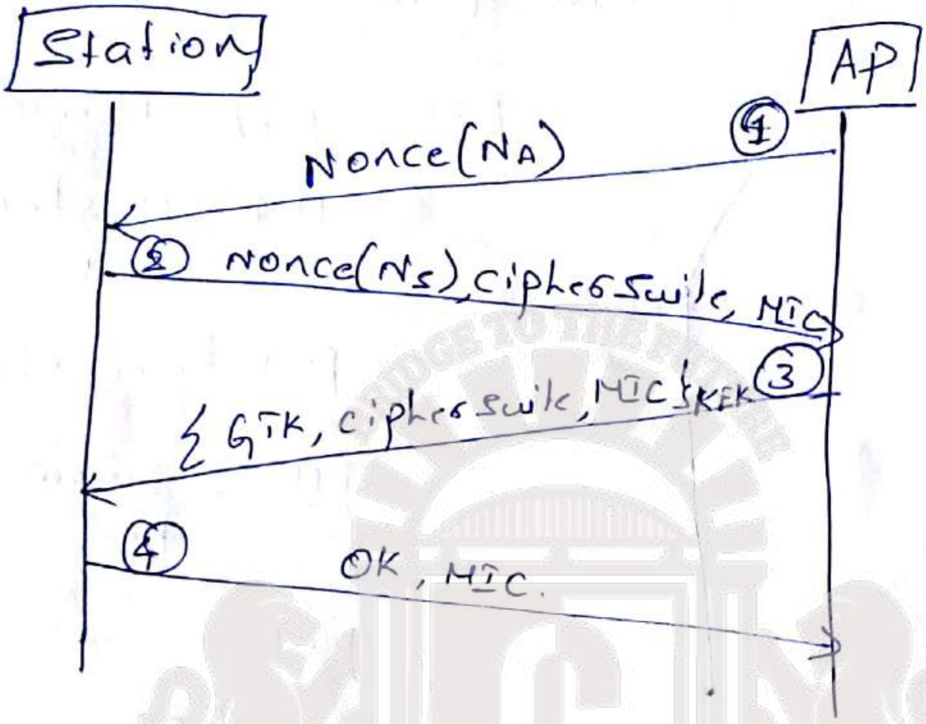
* The main goals of the four-way handshake are to

1) derive the PTK from the PMK.

2) verify the cipher suites communicated in the Beacon and associate Request frames and

3) communicate the group keys from the AP to the Station.

* Figure: shows the messages comprising the four-way handshake.



1. The AP first sends a nonce, N_A, to the station.
2. The station chooses a nonce, N_S. The station computes the PTK as follows

$$PTK = prf(PMK, N_A, N_S, MAC_A, MAC_S)$$

The station sends its nonce together with its choice of cipher suite to the AP. It uses the kck to compute a msg integrity check (MIC). Such protection thwarts a possible man-in-the middle attack intended to replace cryptographic algorithms in the cipher suite for possibly weaker options.

On receiving the msg containing N_S, the AP computes the PTK from the expression used by the station.

It then extracts TK, KCK, and KEK. In addition, the Ap verifies the integrity and soulce of Msg2 using the key, KCK.

3. Msg 3 from the Ap to the Station contains the cullent Group Transient key (GTK). This is the key used by the Ap and all Stations to integrity protect all multicast or broadcast msges. Msg3 also contains the cipher suite chosen by the Ap.

- The msg is encrypted using the KEK and is integrity protected using KCK.

4. Msg 4 is an acknowledgement from the station that it has received the previous msges without error. It is a signal to the Ap that henceforth all messages ll be integrity-protected and encrypted with the TK.

Confidentiality and Integrity.

Data protection in WEP

* It is designed to provide msg confidentiality Integrity and access control but it failed on all three counts.

*.

WEP encryption and Integrity checking

* WEP uses the stream cipher, RC4, for encrypting messages.

* It generates a pseudo-random keystream ks, which is a function of secret shared b/w the two communicating parties.

* In order to have ks vary from msg to msg, a random per-msg initialization vector IV, is also used to generate ks.

* ks is $\oplus$ed with the plaintext p, to obtain the ciphertext c or

$$c = p \oplus ks(s, IV) \quad \text{— (1)}$$

*

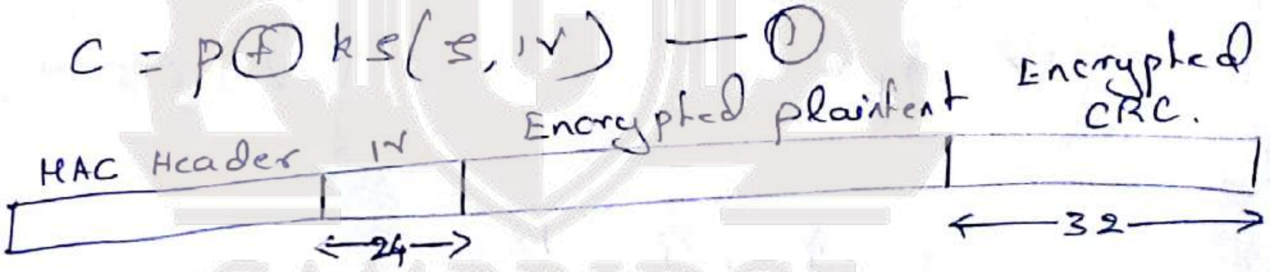


Fig: WEP frame.

* 32-bit CRC checksum computed on the msg and encryption performed on plaintext & CRC using RC4, the IV chosen by the sender is included in each frame.

* TO decrypt the msg, the receiver generates ks from the shared secret s, and the IV retrieved from the received frame. It recover the plaintext from the following equation

$\oplus$ ks

known plaintext Attack.

* The first problem with WEP is the possibility of keystream re-use.

* Since the IV is 24 bits in length, there are only 2^{24} distinct keystreams that could be constructed given a secret s.

* Suppose an attacker finds two frames which were encrypted using the same IV.

* Let their ciphertexts be c & c'. Let the corresponding plaintexts be p & p'.

* using equation 1, it follows that

$$p \oplus p' = c \oplus c'$$

so

$$p' = p \oplus c \oplus c'$$

knowing c, c' & p we can obtain p'.

Msg modification.

* The sender's plaintext be $M_1 F M_2$ where M_1, F & M_2 are each binary strings.

* The attacker wishes to substitute the substring F, with another substring F'. so that the decrypted msg seen by the receiver is $M_1 F' M_2$.

* The msg integrity check should detect any modification to an existing msg.

* The ciphertext computed by the sender is

$$((M_1 F M_2) \| CRC(M_1 F M_2)) \oplus ks.$$

* The attacker intercepts the ciphertext and performs the following operations.

1. He first constructs the string.
2. He then computes the CRC on this string.
3. He finally XORs the original ciphertext with the constructed string.

* The computation yield.

$$((M_1 F' M_2) \| CRC(M_1 F' M_2)) \oplus ks$$

* The last step follows from the fact that the CRC is a linear operation i.e.

$$CRC(m_1 \oplus m_2) = CRC(m_1) \oplus CRC(m_2)$$

* The receiver, on decrypting the ciphertext, obtains

$$(M_1 F' M_2) \| CRC(M_1 F' M_2)$$

* The modified msg has a valid CRC & so passes the integrity check at the receiver. Hence the receiver accepts the msg, unaware that it has been modified by an attacker.

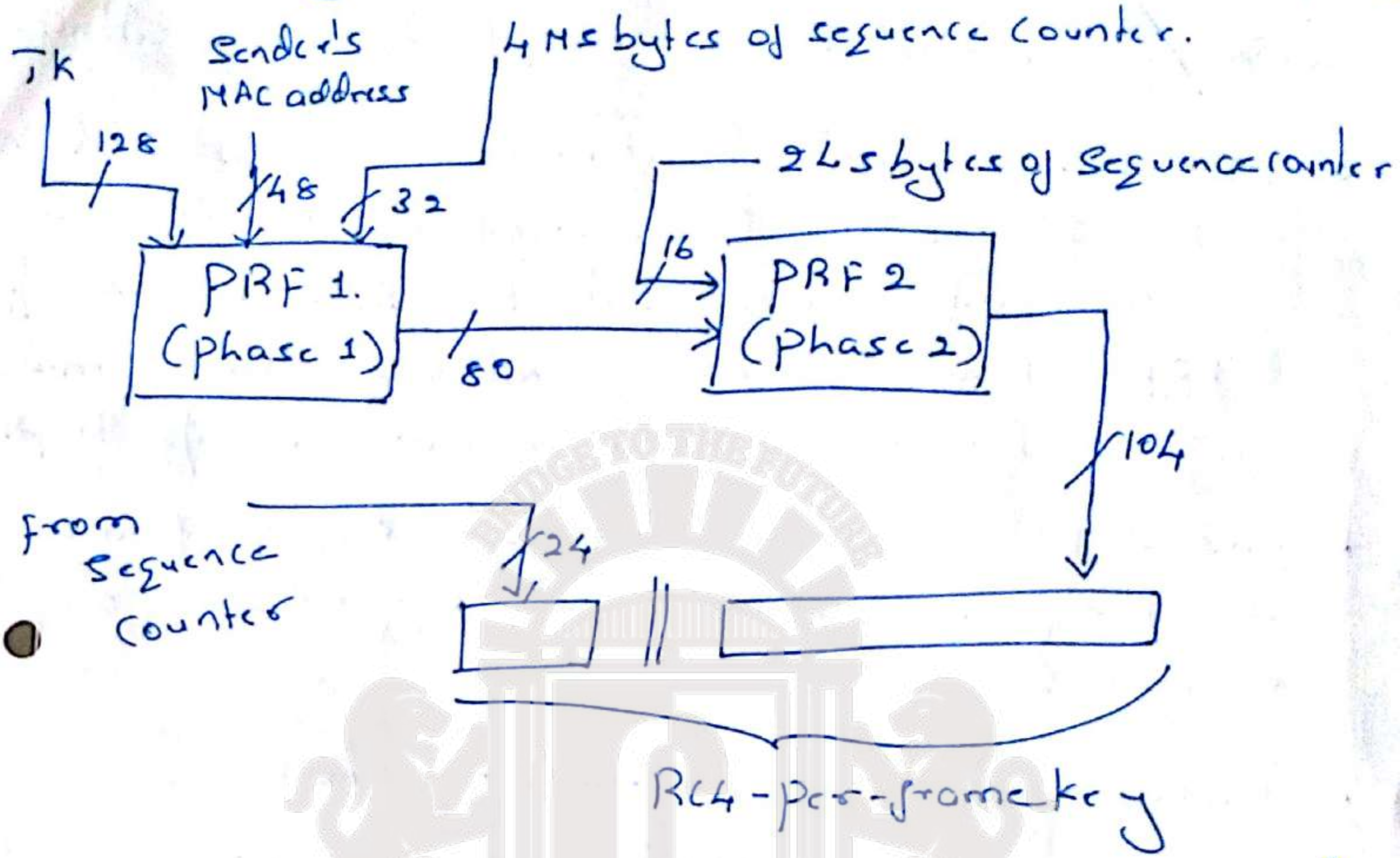
Data protection in TKIP and CCMP.

- * There are many more attacks on RC4 as used in WEP.
- * A well-known example is the FMS attack named after fluhrer, Mantin and Shamir.
  1. By collecting a sufficient no of frames over the air bearing specific IVs, the encryption key used in WEP can be deduced.
- * sol^n for easily Weakness are wireless protected Access (WPA), the technical name for WPA is Temporal key Integrity protocol (TKIP) and counter Mode with CBC MAC protocol (CCMP) (uses AES).

TKIP.

- *. The problem is that the variable part of the WEP key is too small, so the per-frame keystream repeats frequently.
- + In TKIP, the encryption key in TKIP is 128 bits, so there was much randomness in most of the 128 bits of the key and that the probability of keystream collisions was negligible.
- + TKIP Generates a random and different encryption key for each frame sent.

* It employs a process called two-phase key mixing.



* The inputs to this process are the 128-bit temporal key, TK, the sender's MAC address and the 4 most significant bytes of a 48-bit frame sequence counter.

* The randomizing capabilities of the key mixing function and the large size of the key space virtually guarantee that "keystream collisions" never occur. Thus, known plaintext attacks that could be successfully launched on WEP have no chance of success with TKIP.

* The sequence counter is incremented for each frame sent. It is also carried in the header of each frame. It is extracted by the receiver and used to compute the RC4 key for decryption. Both sender and receiver keep track of the sequence no of the last frame sent/received. The receiver accepts a fresh frame only if the

frame's sequence no is greater than that of the previous frame received from the same sender. This helps protect the receiver from replay attacks.

* Two pseudo-random functions are employed in the two phases. The least significant 16 bits of the sequence counters are inputs to PRF2. So, the o/p of PRF2 changes for each frame sent. The 32 most significant bits of the sequence counter are i/p to PRF1

* This i/p changes after every 2^{16} = 65,536 frames sent. Hence, PRF1 is executed very rarely & overall computation time is saved.

* CRC checksum as an integrity check.

* The 64-bit msg integrity check in TKIP, called MIC

MIC is non-linear i.e

$$MIC(m_1 \oplus m_2) \neq MIC(m_1) \oplus MIC(m_2)$$

* MIC is computed as a function of the data in the frame and also some fields in the MAC header such as the source and destination addresses. It also uses as i/p a key derived from the PTK.

* Due to design constraints on WEP cards, MIC's implementation uses simple logical functions shifts etc. Hence, it is not as secure as a keyed cryptographic hash.

CCMP

* It uses the AES for both encryption and for providing msg source authentication/integrity.

* AES is a block cipher, there is no need to re-compute a fresh key for each frame, so the 128-bit temporal key, TK is used for encryption and MAC computation.

* The count is referred to as a packet number (PN) The count is maintained at both sender and receiver ends.

* The PN is included in a special CCMP header field in a CCMP frame.

* The PN is incremented by the sender after each frame is sent.

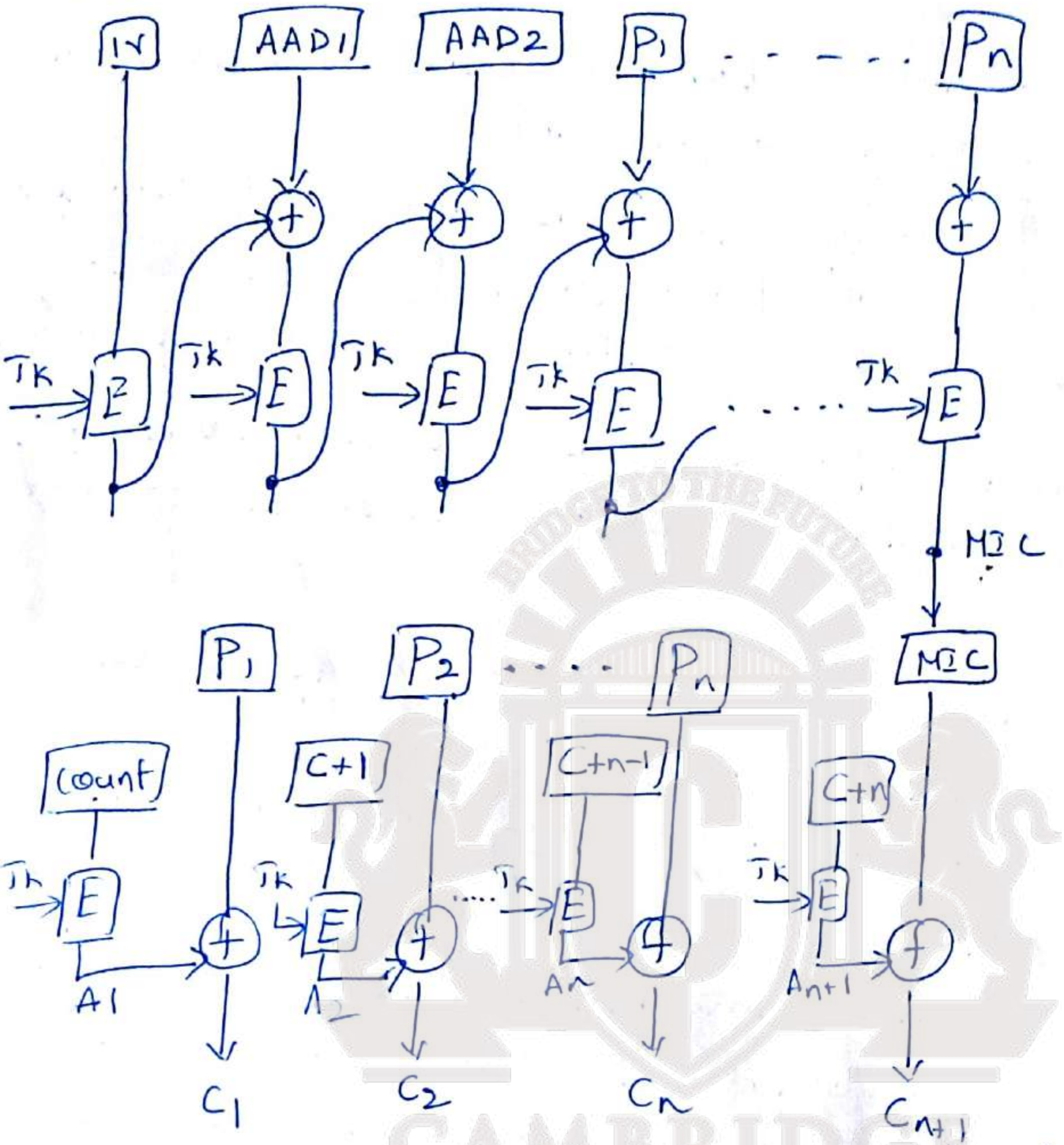
* Receipt of a fresh frame in that session, the receiver compares the value of PN in the CCM header versus the value stored by it. If the former is less than the stored value, the frame is likely to be a replayed frame and is hence discarded.

* The first task in preparing a frame for transmission is to compute a MIC.

* MIC is the frame data & several immutable fields in the MAC header.

* MIC is computed using AES in cipher Block Chaining (CBC) mode with block size = 128 bits.

Fig:- MAC Generation and encryption in CCMP.



IV = initialization vector (includes 48-bit packet no)

AAD1, AAD2 = Additional Authentication Data (includes Certain immutable fields of the MAC header)

COUNT is a function of the packet no.

* The key for performing encryption in each stage is TK.

*. The IV for the MIC computation is a nonce, which includes the 48-bit PN..

* The second & third blocks used in the MIC computation are specific fields in the frame header such as the MAC addresses, sequence control & frame type.

* The blocks in the frame data are sequentially processed resulting in an 8-byte MIC.

* . Encryption:

1. The frame data and the MIC are concatenated and then encrypted using AES in countermode

2. Let n be the total no of blocks in the frame body + MIC.

3. The procedure for encrypting the i-th block is
   a. compute $A_i = E_{TK}(pn + i * j)$. Here, pn is the packet number and j is a constant known to both sender and receiver.
   b. compute i-th block of ciphertext $= A_i \oplus P_i$. Here P_i is the i-th block of plaintext.

4. The frame now includes two new fields - the CCMP header and the MIC.

5. upon receipt of the frame, the receiver reverses the operations performed by the sender. It performs decryption followed by MIC verification.

Firewalls.

1. BASICS

1.1. firewall functionality

* The main functions of a firewall are listed as follo

a. Access control: A firewall filters incoming (from the Internet into the organization) as well as outgoing (from within the organization to the outside) packets. A firewall is said to be configured with a ruleset based on which it decides which packets are to be allowed and which are to be dropped.

b. Address / Port translation.

* NAT was initially devised to alleviate the serious shortage of IP addresses by providing a set of private addresses that could be used by system administrators on their internal n/w but that are globally invalid.

* publicly accessible m/c within an organization, such as web servers, may or may not have public Internet addresses.

* It is possible to conceal the addressing schema of these m/c from the outside world through the use of NAT. NATing is often done by firewalls

c. Logging

* In the process of filtering internet traffic, all

firewalls have some type of logging feature that documents how the firewall handled various types of traffic.

* It are very useful for studying attemple at intrusion. together with various worm and DDos attacks.

* Authentication, caching:

* Some types of firewalls perform authentication of external machines attempting to establish a connection with an internal m/c.

* A special type of firewall called a web proxy authenticates internal users attempting to access an external service.

* web proxy firewall also used to cache frequently requested webpages. This results in decreased response time to the client while saving communication bandwidth

2. policies and Access control lists.

High level policies for access to various types of services

1. All received email should be filtered for spam & viruses.

2. All HTTP requests by external clients for access to authorized pages of the organizations website should be permitted.

3. The organizations employees should be allowed to remotely log into authorized internal machines. However all such communication should be authenticated and encrypted.

4. only two types of outgoing traffic are permitted. First, all e-mail from within the organization to the outside world are permitted. Second, requests from within the organization for external webpages are permitted.

5. DNS queries made by external clients should be allowed provided they pertain to addresses of the organization's publicly accessible services such as the web server or the external e-mail server.

- High-level policies are translated into a set of rules that comprise an ACL.

1. The packet's source IP address and port number.
2. The packet's destination IP address and port no.
3. The Transport protocol in use (TCP or UDP)
4. The packet direction - incoming or outgoing.

NO	(I) or (O)	Transport protocol	S IP addr	Src port.	Destn IP add.	Dest port	Action	comment
1.	I	TCP	ANY	ANY	MS	25	permit	Allow incoming e-mail.
2.	I	TCP	ANY	ANY	WS	80	permit	Allow request for organization webpages
3.	I	UDP	ANY	ANY	NS	53	permit	Allow DNS queries
4.	I	IPsec	Any	ANY	*	*	permit	Allow incoming VPN traffic.
5	I	ANY	ANY	ANY	ANY	Any	Deny	Deny all other incoming traffic.
6.	O	TCP	ANY	ANY	ANY	25	Permit	Allow outgoing email.
7.	O	TCP	"	"	*	80	Permit	Allow request for external webpages

5. 0 Any Any Any Any Any Deny. Deny all other outgoing traffic

* Two types of policy.

1. permissive policy: permit all packets except those that are explicitly forbidden.

2. Restrictive policy: Drop all packets except those that are explicitly permitted.

3. <u>Firewall types.</u>

1. packet filters and stateful Inspection

* processing the ruleset involves checking from matches in the IP, TCP or UDP headers.

* For examples it may be necessaly to check whether a packet callies a certain specific source or destination IP address or port no.

* The ealliest firewall designed to perform this task was referred to as a packet filtering firewall.

* It is often performed by the border router or access router that connects the organization's network to the Internet.

* The border router becomes the first line of defence against malicious incoming packets.

* consider an external MS (IP = ABC) that wishes to deliver mail to an organization. for this purpose, it should first establish a TCP connection with the organization's mail server. SIPAd = ABC, Dest = MS TCP Destion port = 25 ACK flag set

* Suppose such a connection has not yet been establishe Should the packet still be allowed in?

* The simple packet filter will allow the packet to enter even if no prior connection b/w ABC & MS was established Hence it ll not be able to filter out such packets arriving from ABC.

* Stateful packet inspection firewall: It uses a packet's TCP flags and sequence/acknowledgement no to determine whether it is part of an existing, authorized flow.

* If it is participating in the establishment of an authorized connection or if it is already part of an existing connection, the packet is permitted, otherwise it is dropped.

2. Application level firewalls.

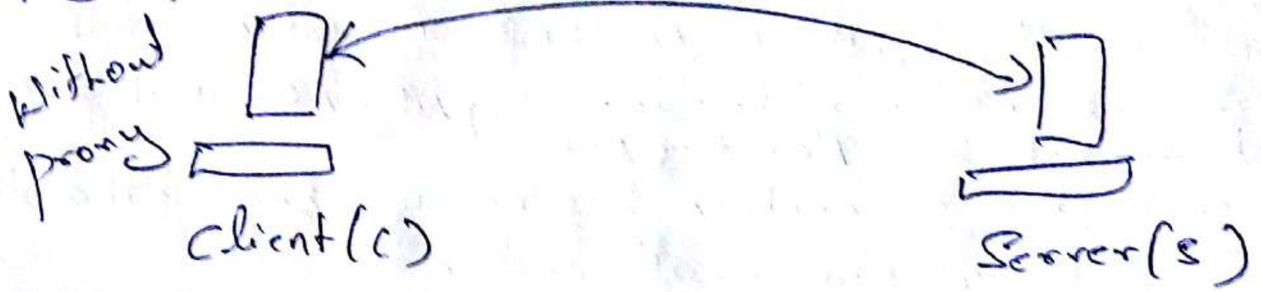
* A packet-filtering firewall, even with the added functionality of stateful packet inspection, is still severely limited.

* It understands the n/w & transport layer headers

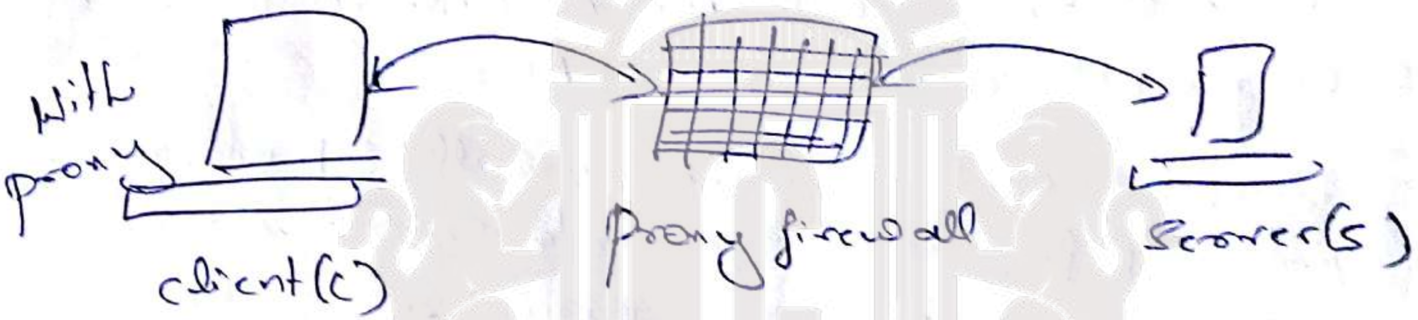
* needed is a firewall that can examine the application payload and scan packets for worms

viruses, spam mail & inappropriate content .such a device is called a deep inspection firewall.

Fig:- proxy firewall.



Direct TCP connection b/w C & S.



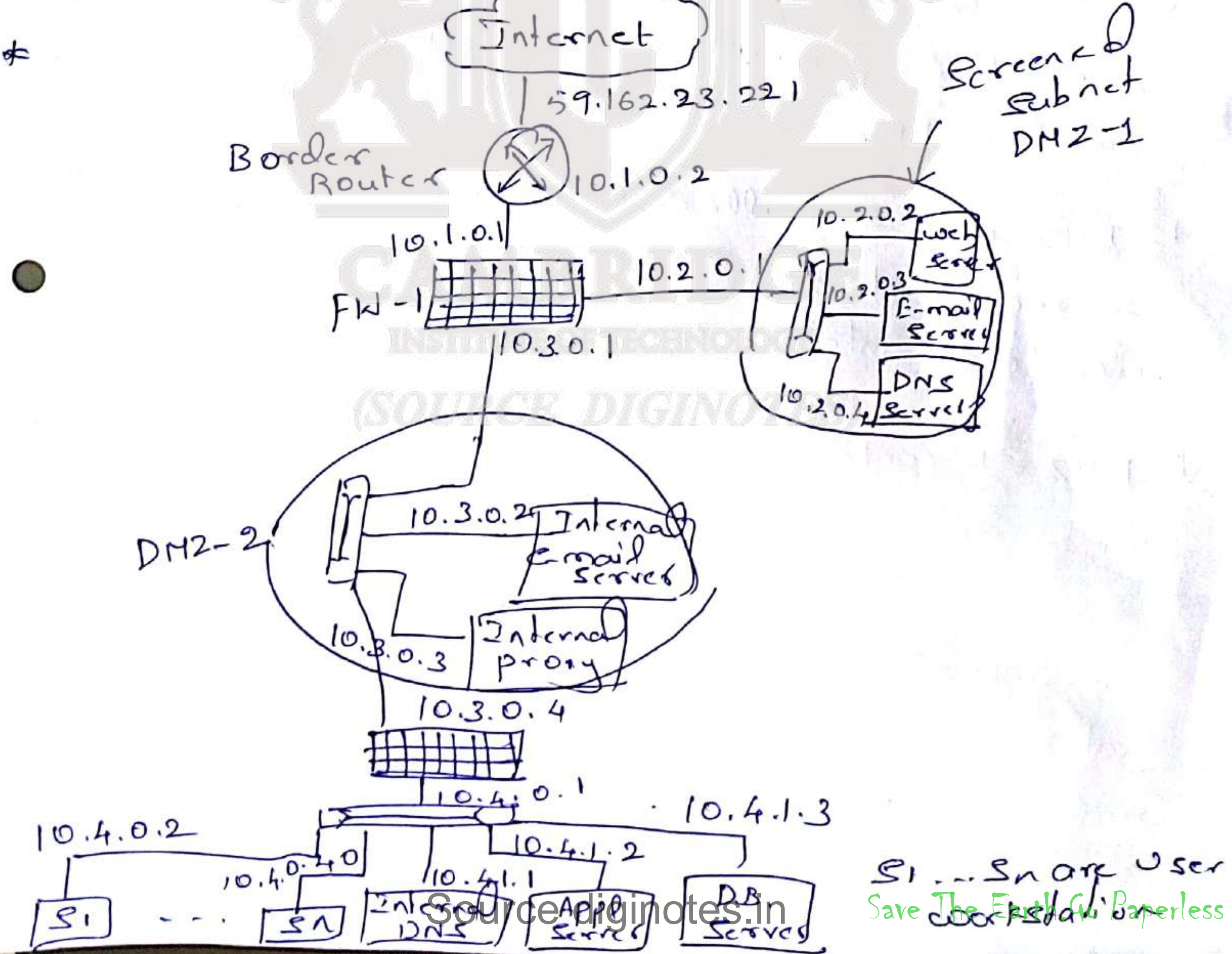
Two TCP connections b/w C & proxy & b/w proxy & S.

- * There are proxy agents for many application layer protocols includis HTTP, SMTP & FTP.
- * In addition to filtering based on application layer data, proxies can perform client authentication & logging.
- * HTTP proxy can also cache webpages.
- * Caching has a major impact on performance.

PRACTICAL ISSUES.

1. placement of firewalls.

- * firewalls help segregate or isolate the n/w into multiple security zones.
- * Each firewall in the organization enforces rules that control the transfer of packets between different security zones.
- * There are three zones - the internet, the region containing the publicly accessible servers and the internal network.
- *



* Fig: depicts a four-zone layout using three firewalls.

* Border Router with some packet-filtering capability This is the access router that interfaces with the Internet. It is connected to a stateful firewall, FW-1, which has three interfaces.

* Firewalls that have more than two interfaces are referred to as multi-homed.

* The zone connected to the right interface of FW-1 referred to as a screened subnet or De-Militarized zone (DMZ).

* A DMZ, is the area b/w two firewalls. The zone b/w firewalls FW-1 & FW-2 is a real DMZ labelled DMZ-2.

* DMZ are so called because they often host servers that are accessible to the Internet & also to the internal n/w.

* DMZ-1 contains the publicly accessible servers. These include the web server, the external e-mail server & the DNS server. All incoming mail from the Internet is received by this e-mail server, which checks for virus signatures and spam mail. The DNS server resolves names of publicly accessible servers.

* DMZ-2 contains the internal e-mail server. This is the server that hosts the mailboxes of the company employees. It handles the sending and receiving of all mail b/w internal parties. It periodically establishes a connection to the external mail server (in DMZ-1) to retrieve all incoming mail. Outgoing mail (from the internal n/w to the internet) can be handled in several ways. The internal mail server can set up an SMTP connection to a remote mail server to transfer mail. Alternatively, it can connect to the external mail server (in DMZ-1) & use it to relay all outgoing mail.

* DMZ-2 also contains an Internet proxy server. All internal users who wish to access external webpages connect to the proxy. The proxy authenticates the internal user & decides whether a page can be accessed. The proxy scans incoming webpages for virus signatures & objectionable content. Finally, the proxy also performs caching of webpages.

* Internal n/w contains application servers, database servers, the user workstations. It also has an internal DNS server. This DNS server is different from the external DNS server in that it provides

mapping b/w the domain names of the internal m/cs & their Ip addresses.

Firewall configuration.

Table: simplified ruleset for firewall, fld-2.

NO	From Ip Addr.	From port	To Ip Addr.	To port	protocol	Action.
1	*	*	Internal	*	*	Drop
2.	user	*	Int_Mail_S	25	SMTP	Accept
3	user	*	proxy	80	HTTP	Accept
4.	*	*	DMZ-2	*	*	Drop

* The first rule states that no m/c from any other security zone is permitted to establish a TCP connection to any internal m/c.

* Rules 2-4 assert that, other than connections from internal stations to the internal mail server (on port 25) & web proxy (on port 80), no other connections are permitted to DMZ-1, DMZ-2 or the internet.

Table: simplified ruleset for firewall, F1.

NO	from Ip Addr.	from port	TO Ip Addr.	TO port	protocol	Actio
1	*	*	DMZ-2	*	*	Drop
2.	Int_Mail_s	*	Ext_Mail_s	25	SMTP	Accept
3.	Internet	*	"	"	"	"
4.	"	*	web_s	80	HTTP	"
5	"	*	DNS_s	53	UDP	"
6.	*	*	DMZ-1	*	*	Drop
7.	proxy	*	Internet	80	HTTP	Accept
8.	Ext_mail_s	*	"	25	SMTP	"
9.	*	*	"	*	*	Drop.

* Rule 1 states that no TCP connection is to be established to any m/c in DMZ-2 from any m/c in DMZ-1 or the Internet.

* Rule 2 states that the external mail server can accept connections from the internal mail server to receive incoming mail or to send outgoing mail.

* Rule 3 allows connections to the external mail server from mail servers on the internet to deposit incoming mail.

* Rule 4 & 5 permit connections from the internet to the organization's web server & external DNS server respectively.

* Rule 6 states that no other connections may be set up to any m/c in DMZ-1 for any other purpose

* The internet proxy in DMZ-2 & the external mail server are permitted do make connections to m/cs on the Internet do access webpages & to send outgoing mail (Rules 7 & 8).

* Rule 9 confirms that no other connection from the organization's m/cs to the internet for any other purpose is allowed.

The Information Technology Act, 2000

IT ACT: AIM AND OBJECTIVES :

- To give legal recognition to transactions done by electronic way or by use of the internet.
- To grant legal recognition to digital signature for accepting any agreement via computer.
- To provide facility of filling documents online.
- To authorise any undertaking to store their data in electronic storage.
- To prevent cyber crime by imposing high penalty for such crimes and protect privacy of internet users.
- To give legal recognition for keeping books of account by bankers and other undertakings in electronic form.

SCOPE OF THE ACT

SCOPE: The Act attempts to address the following issues :

1. Legal recognition of electronic documents.
2. Legal recognition of digital signatures.
3. Offences and contraventions.
4. Justice dispensation system for cybercrimes.

The Act is not applicable for following documents or transaction :-

1. A negotiable instrument as defined in the Negotiable Instruments Act, 1881.
2. A power of attorney as defined in the Power-of-Attorney Act,1882.
3. A trust as defined in the Indian Trust Act 1882.
4. A will as defined in clause (h) of Section 2 of the Indian Succession Act,1925 including any other testamentary disposition by whatever name called.
5. Any contract for the sale or conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central government in the Official Gazette.

Major concepts

- **Access:** Gaining entry into, introduction or communicating with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.
- **Addressee:_**is a person who is intended by the originator to receive the electronic record but does not include any intermediary.
- **Adjudicating Officer:** means an adjudicating officer appointed under Section 46(1).
- **Affixing Digital signature** : means adopting of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature
- **Appropriate Government:_** means any matter

➔Enumerated in List II of the Seventh Schedule to the Constitution.

➔Relating to any State law enacted under List III of the Seventh Schedule to Constitution, the State Government, and in any other case, the Central Government

- **Asymmetric Crypto System:** is a system of source key pair consisting of a private key for creating a digital signature and public key to verify the digital signature.
- **Certifying Authority:** is a person who has been granted a licence to issue a Digital Signature Certificate under Section 24.
- **Certification Practice Statement:** is a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates.
- **Computer:** refers to means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic, or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are related to computer in a computer system or computer network.

- **Computer Network:** implies the interconnection of one or more computers through:

➔The use of satellite, microwave, terrestrial line or other communication media.

➔Terminals or a complex consisting of two or more interconnected computers whether or not interconnection is continuously maintained.

- **Computer Resources:** refer to a computer, computer system, computer network, data, computer database or software.
- **Computer System:** refers to a device or collection of devices, including input and output support devices, and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other function.
- **Data:** implies a representation of information, knowledge, facts, concepts or instructions which is being prepared or has been prepared in a formalised manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form or stored internally in the memory of the computer.

- **Digital Signature:** refers to the authentication any electronic record by a subscriber by means of an electronic method or procedure in accordance with section 3.
- **Electronic Form:** with reference to information refers to any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- **Electronic Gazette:** refers to the Official Gazette published in the electronic form.
- **Electronic Record:** refers to any data record or data generated, image or sound stored, received, or sent in electronic form or micro film or computer generated micro fiche.
- **Information:** includes data, text, images, sound, voice, codes, computer programs, software and database or micro film or computer generated micro fiche

- **Intermediary:** with respect to any particular electronic message, is any person who, on behalf of another person, receives, stores or transmits that message or provides any service with respect to that message.
- **Key, pair:** in an asymmetric crypto system, implies a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.
- **Originator:** refer to a person who sends, generates, stores, or transmits any electronic message or causes any electronic message to be sent, generated, stored, or transmitted to any other person, but does not include an intermediary.
- **Private key:** refers to key of a key pair used to create a digital signature.
- **Public key:** refers to the key of a key pair used to verify a digital signature, which is listed in the Digital Signature Certificate.

- **Secure System:**

➔Refers to computer hardware, software, and procedure that is reasonably secure from unauthorised access and misuse.

➔Provides a reasonable level of liability and correct operation,

➔Is reasonably suited to performing the intended functions.

➔Adheres to generally accepted security procedure.

Important provisions

1.Digital Signature :Authentication of electronic records

- Any subscriber may authenticate any electronic record by affixing the Digital signature.
- The authentication of the electronic record shall be effected by the use of the asymmetric crypto system and hash function which envelop transform initial electronic record into another electronic record.
- Any person by the use of a public key of the subscriber can verify the electronic record.
- The private key and the public key are unique to the subscriber and constitute a functioning key pair.

2.Electronic Governance: Legal recognition of electronic recor

- E-governance is the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizens participation in the decision making process and making government more accountable, transparent and effective.
- Where any law provides that info or any other matter shall be written , typed or printed form, than not with standing anything contained in such a law.
- The requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and accessible so as to be usable for a subsequent reference.

3.**Electronic Governance: Legal recognition of digital signature**

- A digital signature is a electronic or digital equivalent of a physical signature. A digital signature affixed to a digital document establishes the origin of that digital document.

- Digital signatures are considered to be more secure and cannot be replicated easily due to the technology behind them.

- Where any law provides that info or any other matter shall be authenticated by affixing the sign or any document shall be signed or bear the sign of any person, anything contained in such a law.

4.Use of Electronic records and Digital Signature in Government and its agencies

Because of high security associated with digital signature , govts in many countries have passed laws to encourage the use of digitally signed electronic documents.

- Where any law provides:

1. The filing of any form application or any other document with any office or body or agency owned or controlled by the appropriate government in a particular manner.
2. The issue or grant of any license , permit, sanction or approval by whatever name called in a particular manner.
3. The receipt of money in a particular manner, then not contained in any other law for the time being in force, such a requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt as the case may be is effected by means of such electronic form.

- The govt by rules can prescribe

1. The manner and format in which such electronic records shall be filed, created or issued.
2. The manner or method of payment of any fee or charges for filling, creation or issue of any electronic record.

5.Retention of electronic records

- Where any law provides that documents, records or info shall be retained for any specific period, then requirement shall be deemed to have been satisfied if such documents , records or info are retained in the electronic form , if:

1. The info contained there in remains accessible so as to be usable for a subsequent reference.
2. The electronic record is retained in the format in which it was originally generated, sent or received in a format which can be demonstrated to represent accurately the information originally generated, sent or received.
3. The details which will facilitate the identification of the origin, destination date and time of dispatch or receipt of such electronic record are available in the electronic record.

- Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

6. Publication of rules and regulations in the electronic gazett

- Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the official gazette, then, such a requirement shall be deemed to have been satisfied if such a rule, regulation, order, notification or any other matter is published in the official gazette or electronic gazette.
- Provided that where any rule, regulation, order, bye-law or any other matter is published in the official gazette, the date of publication shall be deemed to be the date of the gazette which was first published in any form.
- A person has no right to insist on accepting document in electronic form.

7. **Power to make rules by central government in respect of digital signature**

The central government may prescribe

- The type of digital signature
- The manner and format in which the digital signature shall be affixed.
- The manner or procedure which facilitates identification of the person affixing the digital signature
- Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments and
- Any other matter which is necessary to give legal effect to digital signatures.

Secure Electronic Records And Secure Digital Signature

Secure Electronic Record

- Where any security procedure has been applied to an electronic record at specific point of time, then such a record shall be deemed to be secure electronic record from such a point of time to the time of verification[14]

Secure Digital Signature

1. Unique to the subscriber affixing it
2. Capable of identifying such a subscriber
3. Create in a manner under the exclusive control of subscriber and is linked to electronic record relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such DS shall be deemed to be a secure DS.[sec 15]

Security Procedures

1. The nature of the transaction
2. The level of Sophistication of the parties with references to their technological capacity
3. The volume of similar transactions engaged in by other parties
4. The cost of alternative procedures
5. The availability of alternatives offered to but rejected by any party.

Regulation Of Certifying Authorities

1. Appointment of controller and other officers

1. The controller shall discharge his functions under this act subject to general control and direction of central government.
2. The deputy controller and assistant controllers shall perform the functions assigned to them by the controller under the general superintendence and control of the controller.
3. The qualifications, experience and terms and conditions of service of controller, deputy controllers and assistant controllers shall be such as may be prescribed by the central government.
4. The Head office and Branch office of controller shall be at such places as the central government may specify and these may be established at such places as the central government may think fit.

2. Functions Of The Controller

The Controller may perform following functions

- Exercising supervision over the activities of the certifying authorities
- Certifying public keys of the certifying authorities
- Laying down the standards to be maintained by the certifying authorities.

- Specifying the qualifications and experience that which employees of the certifying authorities should possess
- Specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of digital signature certificate and the public key;
- Specifying the form and content of a digital signature certificate and the key
- Resolving any conflict of interest between the certifying authorities and the subscribers
- Laying down the duties of the certifying authorities

3. Recognition of Foreign Certifying Authorities

- The controller may, with previous approval of the central government and by notification in the official gazette recognise any foreign certifying authority as a certifying authority for the purposes of this act.
- Where any certifying authority is recognised under subsection(1),the digital signature certificate issued by such certifying authority shall be valid for the purposes of this act.

4. Controller to act repository

- The controller shall be the repository of all digital signature certificate issued under this act.

- Make use of hardware, software, and procedures that are secure of intrusion and misuse
- Observe other such standards as may be prescribed by the central government to ensure that the security of the digital signature is assured.
- The controller shall maintain a computerised data base of all pubic keys in such a manner that such a data base and the public keys are available of nay member of the public

5. Licence to issue Digital Signature Certificates

- The process of obtaining a DSC essentially involves submission of paperwork that establishes applicants to the issuer.
- Any person may make an application, to the controller, for a licence to issue digital signature certificates.
- No licence shall be issued under sub section(1),unless the applicant full fills such requirement's with respect to qualification, manpower, financial resources which are necessary to issue digital signature certificates as may be prescribed by the central government
- A licence granted under this section shall
- Be valid for such period as may be prescribed by the central government
- Not be transferable.

6. Application for licence

Every application for issue of a licence shall be accompanied by

1. A certification practice statement
2. A statement including the procedure with respect to the identification of the applicant
3. Such other documents as may be prescribed by the central government

7. Renewal of Licence

An application for renewal of a licence in the required form.

8. Procedure for grant or rejection of licence

The controller may, on receipt of an application under subsection(1) of section 21,after considering the documents accompanying the application.

9. Suspension of licence

The controller may, if he is satisfied after making such inquries as he thinks fit that a certifying authority has

- Made a statement in, or in relation to, the application for the issue or renewal of licence which is incorrect or false in material particular
- Failed to maintain the standards specified under clause(b)of subsection (2)of section 20
- The controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under subsection(1).by order, suspend such a licence pending the completion of any inquiry ordered by him
- No certifying authority whose licence has been suspended shall issue any digital signature certificate during such suspension

10. Notice of suspension or revocation of licence

- Where the licence of the certifying authority is suspended or revoked the controller shall publish notice of such suspension or revocation as the case may be in the database maintained by him
- Where one or more repositories are specified the controller shall publish notices of such suspensions or revocations as the case may be in all such repositories

11. Power to delegate

- The controller may in writing, authorise the deputy controller, assistant controller, or any officers to exercise any of the power of the controller .

12. Power to investigate contraventions

- The controller, or any officer authorised by him in this behalf, shall take up for investigation any contravention of the provision of this act rules or regulations made under.

13. Access to computers and data

- The controller, or any person authorised by him shall if he has reasonable cause to suspect that any contravention of the provisions of this act, rules or regulations made under has been committed have access to any computer system.

14. Certifying authority to follow certain procedures

- Make use of hardware, software and procedures that are secure from intrusion and misuse
- Observe such other standards as may be specified by regulations.

15. Certifying authority to ensure compliance of the act

- Every certifying authority shall ensure that every person employed or otherwise engaged by it complies in the course of his employment.

16. Display of Licence

- Every certifying authority shall display its Licence at a place of the permises in which it carries on its business

17. Surrender of Licence

- Every certifying authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to controller.
- Where any certifying authority fails to surrender a licence under subsection(1)the person in whose favour a licence is issued shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or fine up to 100000 or both.

18. Disclosure

- The digital certificate which contains the public key corresponding to the private key used by that Certifying authority to digitally sign digital signature certificate.
- Notice of the revocation of its certifying authority certificate

Digital signature certificates

- DSC is a certificate issued by a CA necessary for an undertaking to be able to digitally sign a document.

1. Certifying authority to issue digital signature certificate.

- Any person may make an application to the CA for issue of a DSC in such form as may be prescribed by the central Government.
- Every such application shall be accompanied by fee not exceeding 25000 as may be prescribed by the central government to be paid to the CA.
- Each such application shall be accompanied by a certification practice
- Provided that no digital certificate shall be granted unless the CA is satisfied that the applicant holds the pair keys, private key which is capable of creating a digital signature, public key used to verify a DS.

Source : diginotes.in

2. Representations upon issuance of digital signature certificate.

A CA while issuing a DSC shall certify that

- It has complied with the provisions of this act and the rules and regulations made .
- It has published the DSC.
- The subscriber holds the private key corresponding to the public key.
- The information contained in the DSC is accurate.

3. Suspension of digital signature certificate

May suspend such a DSC

- On receipt of a request to that effect from the subscriber or any person.
- A DSC shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity to be heard in the matter.

4. Revocation of digital signature certificate

- A CA may revoke a DSC issued by it where the subscriber or any other person authorised by him, upon the death of the subscriber, winding up of the company.
- A DSC shall not be revoked unless the subscriber has been given an opportunity to be heard in the matter.
- On revocation of a DSC under this section, the CA shall communicate the same to the subscriber.

5.Notice of suspension or revocation

- Where a DSC is suspended or revoked under sec 37 or 38, the CA shall publish a notice of such a suspension or revocation in the repository specified in the DSC for publication of such a notice.

Duties of subscribers

1. Generating key pair.

2. Acceptance of digital signature certificate:

- A subscriber shall be deemed to have accepted a DSC if he publishes the publication of a DSC to one or more persons, in a repository.
- By accepting a DSC, the subscriber certifies to all who reasonably rely on the information contained in the DSC that the subscriber holds the pair or all representations made by the subscriber to the CA.

3. Control of private key

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his DSC and take all steps to prevent its disclosure to a person not authorised to affix the DS of the subscriber.
- If the private key corresponding to the public key listed in the DSC has been compromised, the subscriber shall communicate this without any delay to the CA in such manner as may be specified by the regulations.

Penalties and adjudication

1. Penalty for damage to computer, computer system.

- If any person without the permission of the owner accesses or secures access to such computer, downloads any data, introduces any computer contaminant or computer virus into any computer, damages any computer, disrupts any computer network, denies access or causes the denial of access to any person authorised to access any computer, provides any assistance to any person to facilitate access to a computer charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, he shall be liable to pay damages by way of compensation not exceeding 1 crore to the person.

2. Compensation for failure to protect data

- If a body corporate handling any sensitive personal data or information in a computer resource which owns is negligent in implementing and maintaining reasonable security practices such body shall be liable to pay damages to the aggrieved party.

3. Penalty for failure to furnish information return

- If any person who is required under this act should furnish any document , return to the controller or the CA fails to furnish the same , he shall be liable to a penalty not exceeding 150000 for each such failure.

4. Residuary penalty

- Whoever contravenes any rules or regulations made under this act, shall be liable to pay a compensation not exceeding 25000 to the person affected by such contravention.

5. Power to adjudicate

6. Factors to be taken into account by the adjudicating officer

- The amount of gain of unfair advantage, wherever quantifiable made as a result of the default.
- The amount of loss caused to any person as a result of the default.
- The repetitive nature of the default.

The cyber regulations appellate tribunal

- Establishment of cyber appellate tribunal.
- Composition of cyber appellate tribunal.
- Qualification for appointment as presiding officer of cyber appellate tribunal.
- Term of office.
- Salary, allowances, and other terms and conditions of service of presiding officer.
- Filling up of vacancies.
- Resignation and removal.
- Orders constituting appellate tribunal to be final.
- Staff of the cyber appellate tribunal.
- Appeal to cyber appellate tribunal.
- Procedure and powers of the cyber appellate tribunal.

- Right to legal representation.
- Limitation.
- Civil court not to have jurisdiction.
- Appeal to high court.
- Compounding of contraventions.
- Recovery of penalty.

Offences

1. Tampering with computer source documents

- Whoever knowingly or intentionally conceals, destroy or alters or intentionally or knowingly causes another to conceal, destroy any computer source code used for a computer or computer network, shall be punishable with imprisonment up to three years or with a fine up to 2 lakh or with both.

2. **Hacking with computer system**

- if any person dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine up to 5 lakh or both.

3. Punishment for receiving stolen computer resources or communication device

- Whoever dishonestly received or retains any stolen computer resource of communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment for a term which may extend up to 3 years or with fine up to 1 lakh or both.

4. Punishment for identity theft

- Whoever fraudulently or dishonestly make use of electronic signature ,password or unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

5. Punishment for cheating by personation by using computer resource

- Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to 1 lakh rupees.

6. Punishment for violation of privacy

- Whoever, intentionally publishes or transmits the image of a private area of any person without his or her consent, shall be punished with imprisonment which may extend to 3 years or fine not exceeding 2 lakh rupees or both.

7. Punishment for cyber terrorism

- Whoever with intent to threaten the unity, integrity, security of sovereignty of India or any section of the people by- denying or cause the denial of access to any person authorized to access computer resource or attempting to penetrate or access a computer resource without authorization or exceeding authorized access.
- Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted.
- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

8. Publishing of information which is obscene in electronic form

- Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest, shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 1 lakh.

9. Punishment for publishing or transmitting of material containing sexually explicit act in electronic form

- Whoever publishes or transmits or causes to be published in the electronic form any material which contains sexually explicit act or conduct shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 10 lakh rupees.

10. Power of controller to give directions

- The controller may, by order, direct a CA or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, if those are necessary to ensure compliance with the provisions of this act, rules made thereunder.
- Any person who fails to comply with any order under sub-section 1 shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding 3 years or to a fine not exceeding 2 lakh or to both.

11. Government agency power to intercept information

- The act empowers the central/ state government authorised agency to intercept, monitor or decrypt any information generated, transmitted or stored in any computer resource if it is deemed fit in the interest of the sovereignty .
- The agency can also secure all the facilities and technical assistance from the subscriber or computer personnel to decrypt the information.
- The subscriber or any person who fails to assist the agency shall be punishable with an imprisonment for a term to 7 years.

12. Protected system

- The appropriate government may, by notification in the official gazette, declare any computer, computer system or computer network to be a protected system.
- The appropriate government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section 1.
- Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished up to 10 years and shall be liable to fine.

13. Penalty for misrepresentation.

- Whoever makes any misrepresentation to, or suppresses any material fact from, the controller or the CA for obtaining any licence or digital signature certificate, as the case may be, shall be punished up to 2 years or with fine which may extend to 1 lakh or both.

14. Penalty for breach of confidentiality and privacy

- Any person who, in pursuance of any of the powers conferred under this act, rules or regulation made thereunder, has secured access to any electronic record, book, register or other material without the consent of the person concerned, discloses such electronic record or other material to any other person shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

15. Penalty for publishing digital signature certificate false in certain particulars

- No person shall publish a DSC with the knowledge that the CA listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it.
- Any person who contravenes the provisions of sub section 1 shall be punished up to 2 years imprisonment or fine with 1 lakh or both.

16. Publication for fraudulent purpose

- Whoever knowingly creates, publishes or otherwise makes available a DSC for any fraudulent shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

17. Act to apply for offence or contravention committed outside India

- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.
- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer located in india.

18. Confiscation

- Any computer, computer system, floppies, CD, tape drives or any other accessories related thereto, in respect of which any provision of this act or rules, orders or regulations made thereunder has been or is being contravened shall be liable to confiscation.

19. Penalties or confiscation not to interfere with other punishments

- No penalty imposed or confiscation made under this act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

20. Power to investigate offences

- Notwithstanding anything contained in the code of criminal procedure 1973, a police officer not below the rank of deputy superintendent of police shall investigate any offence under this act.

Miscellaneous provisions

1.Power of police officer and other officers to enter search

- Notwithstanding anything contained in the code of criminal procedure 1973, a police officer not below the rank of deputy superintendent of police, or any other officer authorised by the central government, may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this act.

- Where any person is arrested by an officer other than a police officer, such an officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in –charge of a police station.

2. Act to have overriding effect

3. Controller, deputy controller, and assistant controllers to be public servants

4. Power to give directions: The central government may give directions to any state government as to the carrying into execution in the state of any of the provisions of this act or of any rule, regulation or order made thereunder.

5. Protection of action taken in good faith

6. Offences by companies

- Where a person committing a contravention of any of the provisions of this act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished.

7. Removal of difficulties

- If any difficulty arises in giving effect to the provisions of this act, the central government may, by order published in the official gazette, make such provisions not inconsistent with the provisions of this act as appear to it to be necessary for removing the difficulty provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this act.
- Every order made under this section shall be laid, as soon as possible after it is made, before each house of parliament.

8. Constitution of advisory committee

- The central government shall, as soon as possible after the commencement of this act, constitute a committee called the cyber regulations advisory committee.
- The cyber regulation advisory committee shall consist of a chairperson and such a number of other official and non-official members representing the interests principally affected or having special knowledge of the subject- matter as the central govt.

9. Special provisions for evidence relating to electronic record

10. Admissibility of electronic records

11. Presumption as to electronic records and digital signatures

- In any proceeding involving a secure electronic record, the court shall presume, unless the contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.
- In any proceeding, involving a secure DS, the court shall presume, unless contrary is proved, that the secure DS is affixed by subscriber with the intention of signing or approving the electronic record.

12. Presumption as to digital signature certificates

13. Presumption as to electronic messages

- The court may presume that an electronic msg forwarded by the originator through an electronic mail server to the addressee to whom the msg purports to be addresses corresponds with the msg as fed into his computer for transmission but the court shall not make any presumption as to the person by whom such msg was sent.

THANK YOU