Network Security

Cryptography
→ Sym – DES & modes, AES
→ Asym

Same key
Symmetric key

*) For a group of n individuals num of keys req'd in
Private key cryptography – $\frac{n(n-1)}{2}$
public key cryptography – $2n$

DES :

DES – 56 bit key
2-DES – 112 bits
3-DES – 168 bits

Plaintext, Cipher text } 64 bit

AES: 10 Rounds – 128 bits
12 Rounds – 192 bits
14 Rounds – 256 bits

Proof : Feistal → Based on XOR property.
Attack : leslie.
Monoalphabetic substitution.
↓ sol
Modes of DES
→ Electronic code book.
→ cipher block chaining
→ cipher block feedback
→ output feedback
→ stream mode
→ Counter mode

Stages : 19
- 16 – key dependant and iterative
- 3 – key independent

*) 3 DES can be implemented with two keys
$\boxed{K_1\ K_2\ K_1}$ E $\boxed{K_1\ K_2\ K_1}$ D

*) Property of Good Candidate key is N and $\frac{N-1}{2}$ should be primes

RSA Algorithm :

$p, q > 10^{100}$
$n = p * q$
$\phi(n) = (p-1) * (q-1)$
$GCD(d, \phi(n)) = 1$
$ed \equiv 1 \bmod \phi(n)$

d → private key
(e, n) → public key

$C \equiv M^e \bmod n$ → Encryption
$M \equiv C^d \bmod n$ → decryption

Digital signature :

$K_r A$ — $K_u B$ $K_r B$ — $K_u A$

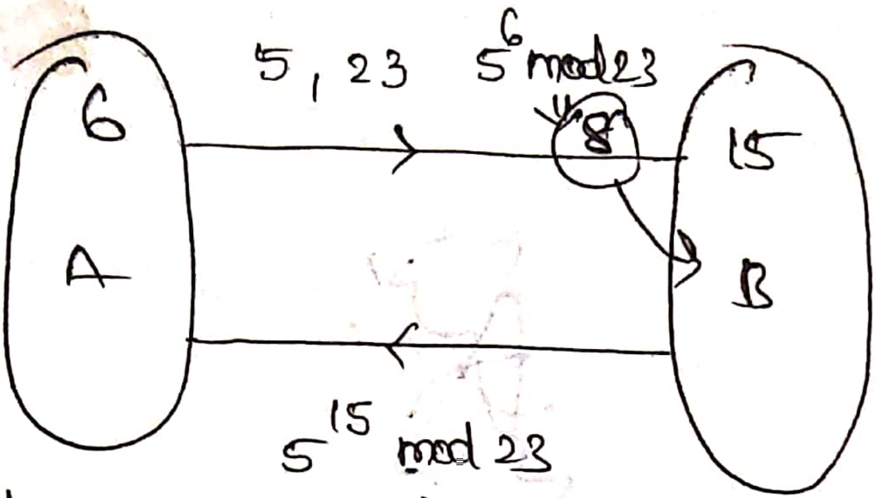
∴ sign is big
↓ sol
Message digest

Msg → Hash Algo → $E_{K_{rA}}(\ )$ → sign

	i/p	o/p
MD5	128 bits	Arbitrary len
SHA-1	160 bits	
SHA-512	512 bits	
SHA-1024	1024 bits	

11

DH Key Exchange $g:5$ mod 23



$\Rightarrow$

19^6 mod 23

$\Rightarrow 2$ ✓

8^{15} mod 23

$\Rightarrow 2$ ✓

Modular Arithmetic :

*) $a \equiv b \bmod n$: a and b leave same remainder when you divide them by 'n'.

*) $a \equiv b \bmod n$: if n divides $a-b$.

*) If $a \equiv b \bmod n$ and $c \equiv d \bmod n$ then $a+c \equiv (b+d) \bmod n$

$a-c \equiv (b-d) \bmod n$

$a*c \equiv (b*d) \bmod n$

Imp
*) If $a \equiv (b*c) \bmod n$ then $a \equiv (b \bmod n * c \bmod n) \bmod n$.

$a \equiv (b+c) \bmod n$ then $a \equiv (b \bmod n + c \bmod n) \bmod n$

Euler's totient function :

Num of +ve integers which are less than 'n', Coprime to n.
$\boxed{GCD = 1}$

*) when n is prime num $\phi(n) = n-1$

*) when m and n are Coprime then $\phi(m*n) = \phi(m) * \phi(n)$
$= (m-1)*(n-1)$

*) If the prime factorization of n is given by

$$n = P_1^{e_1} * P_2^{e_2} * \dots * P_n^{e_n} \quad \text{then}$$

$$\phi(n) = n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right) \dots \left(1-\frac{1}{P_n}\right)$$

Multiplicative Inverse :

For each $a \not\equiv 0 \bmod p$ [p is a prime num] there is 'b' such that $ab \equiv 1 \bmod p$ then b is multiplicative inverse of a.

ie $ab \equiv 1 \bmod p$

$$b \equiv a^{-1} \bmod p$$

→ GCD = 1

If p is not prime.

If a and n have no common factors then a has a multiplicative inverse mod n.

$\boxed{GCD(a,n) = 1}$

Ex:- ① $2 \not\equiv 0 \bmod 7$ prime.

$2 * \underline{x} \equiv 1 \bmod 7$

4

$4 \equiv 2^{-1} \bmod 7$ — 4 is multiplicative Invene of 2 mod 7

Ex:- $23^{-1} \bmod 100$

$ab \equiv 1 \bmod n \Rightarrow 23 \cdot b \equiv 1 \bmod 100.$

97 77 87 46

87

② $5 \not\equiv 0 \bmod 9$

$5 * \underline{x} \equiv 1 \bmod 9$ not prime but $\underline{GCD(5,9) = 1}$

2 Coprime.

$2 \equiv 5^{-1} \bmod \underline{9}$

Eulers theorem :

If n is a +ve Integer and a, n are Coprime then

$$\boxed{a^{\phi(n)} \equiv 1 \bmod n}$$

Ex:- $a = 8$ $n = 165$

$GCD(8, 165) = 1$ ✓

Now,

$\phi(165) = 3 * 55 \Rightarrow 3 * 5 * 11$

$\Rightarrow 165\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{11}\right)$

$\Rightarrow 165 * \frac{2}{3} * \frac{4}{5} * \frac{10}{11} \Rightarrow 80$

$$\therefore \boxed{8^{80} \equiv 1 \bmod 165}$$

Fermat's theorem :

Special case of Eulers theorem

For any prime number n and $a \not\equiv 0 \bmod n$ then

$$\boxed{a^{n-1} \equiv 1 \bmod n}$$

*) If n is a +ve Integer and a, n are Co-prime then

$$\boxed{\begin{array}{c} a^{\phi(n)+1} \equiv a \bmod n \\ \text{(or)} \\ a^{\phi(n).t+1} \equiv a \bmod n \end{array}}$$

Ex:- $a=9$ $n=13$ $\phi(n)=12$.

$9^{12} \equiv 1 \bmod 13$

$9^{13} \equiv 9 \bmod 13$

$9^{25} \equiv 9 \bmod 13.$

*) If n is a +ve Integer, (a,n) are Coprimes and $b \equiv 1 \bmod \phi(n)$ then

$$\boxed{a^b \equiv a \bmod n}$$

Primitive root:

The number b in $a \equiv b \bmod n$ is called residue of $a \bmod n$.

Residue:

Ex:- $7 \equiv 85 \bmod 13$

85 is residue of 7 mod 13

Residue class:

Residue classes of $f(x) \bmod n$ are all possible values of $f(x) \bmod n$

Ex:- RC of $x^2 \bmod 6$ are $\{0, 1, 3, 4\}$

$0^2 \bmod 6 \Rightarrow 0$

$1^2 \bmod 6 \Rightarrow 1$

$2^2 \bmod 6 \Rightarrow 4$

$3^2 \bmod 6 \Rightarrow 3$

$4^2 \bmod 6 \Rightarrow 4$

$5^2 \bmod 6 \Rightarrow 1$

$\vdots \qquad \vdots$

Ex:- $a = 2$ $p = 11$ $b = 9$

$a^x \equiv b \mod p$

Primitive root :

let p be a prime then b is a primitive root for p if power of b

$b^0, b^1, b^2 \ldots$ includes all residue classes of mod p.

~~Ex:- p=7~~

Note : If p is a prime,

The powers of b form a repeating cycle and the cycle can't be larger than (p-1) then b is primitive root of p.

Ex:- $p = 7$ $b = 3$

$3^0 \equiv 1 \mod 7$
$3^1 \equiv 3 \mod 7$
$3^2 \equiv 2 \mod 7$
$3^3 \equiv 6 \mod 7$
$3^4 \equiv 4 \mod 7$
$3^5 \equiv 5 \mod 7$
$3^6 \equiv 1 \mod 7$

✓ ∴ 3 is primitive root

*) Excluding 1, 2, 4 the numbers with primitive roots are of shape p^k, $2p^k$ where p is odd prime number

Ex:- 3, 5, 6, 7, 10, 14, $2*7^2$ - - -

*) 'm' is primitive root modulo n iff multiplicative order of m is $\phi(n)$

ie $m^{\phi(n)} \equiv 1 \mod n$.

Discrete logarithm :

The problem of finding x such that $a^x \equiv b \mod p$ [p is prime, a, b are non zero Integers] is called Discrete logarithm problem

→ It is a Np hard problem

→ It is one way function

If f(x) is Easy to Compute, but y is computationally Infeasible to find x such that $y = f(x)$.

Ex:- $a = 2$ $p = 11$ $b = 9$

$$a^x \equiv b \bmod p$$

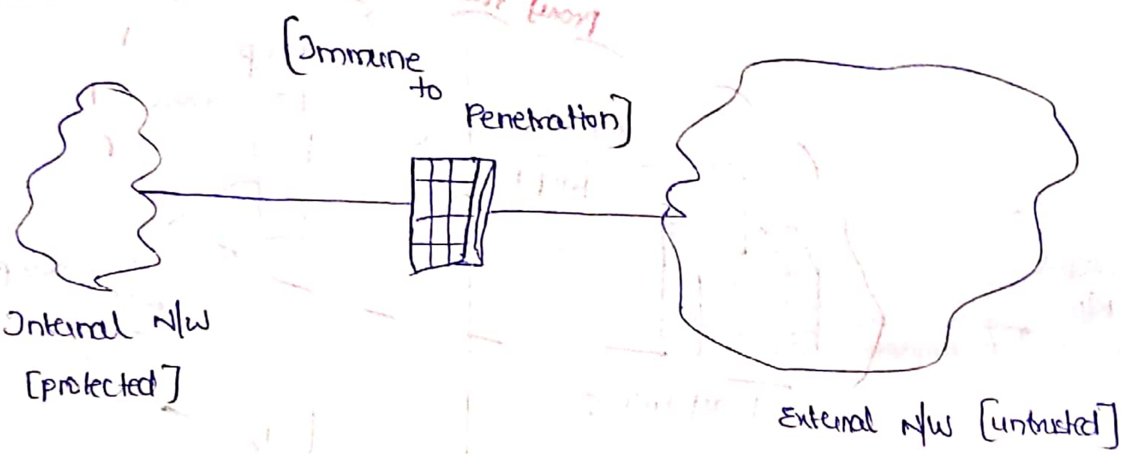
$$2^x \equiv 9 \bmod p$$

At $x = 6$ $\longrightarrow$ Hard to find

Fire walls : (software)

→ A Firewall forms a barrier through which the traffic going in each direction must pass through it

→ A Firewall security policy dictates which traffic is authorized to pass in each direction



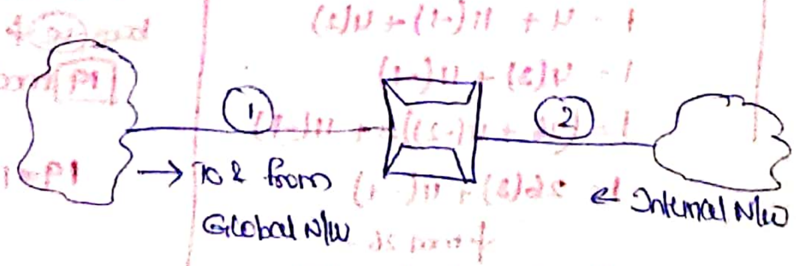
=> A Firewall may be designed to operate as a filter at the level of Ip packets or may operate at higher layer protocols.

→ ~~A Firewall defines a single choke point~~

Types of Firewalls :

① packet filtering Firewall :

A packet filtering firewall applies a set of rules to each incoming and outgoing Ip packet and then forwards or discards the packet based on Information present in Tcp and Ip headers.



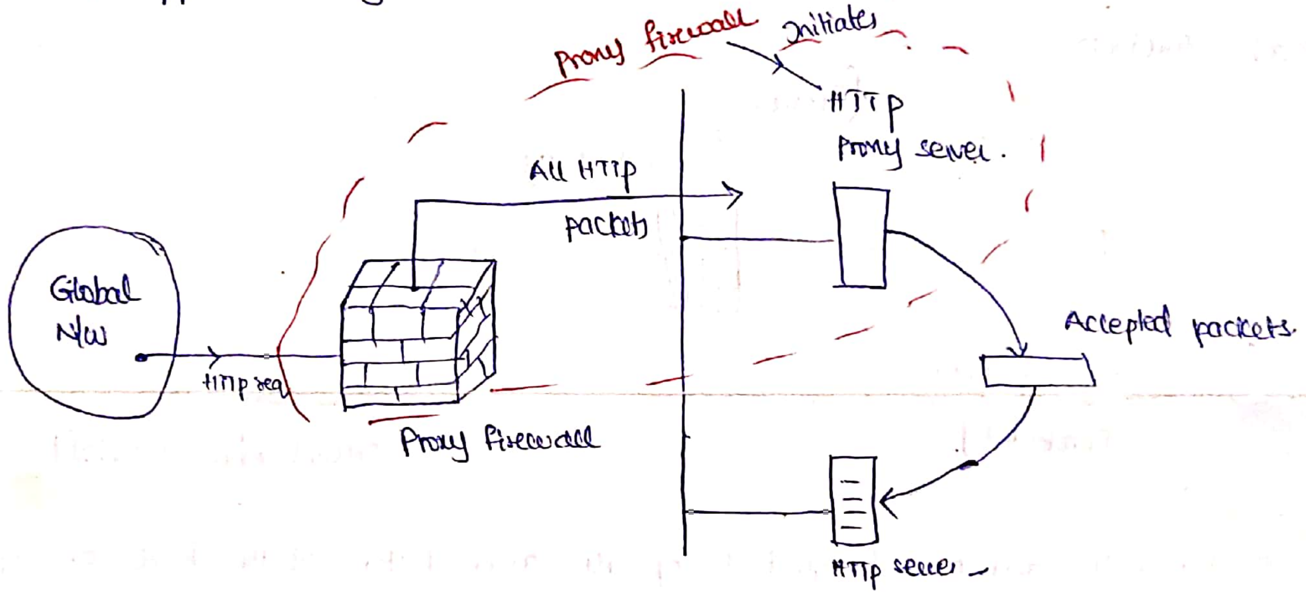
then)

Interface	Source Ip	Source port	Destination Ip	Destination port	
1	131.34.0.0	*	*	*	Block a N/w entering into Internal N/w
*	*	*	*	23	Blocks Telnet Service from both sides
1	*	*	194.78.20.8	*	Blocks accessing particular Ip addr
2	*	80	*	*	HTTP is accessed within Internal N/w

② **proxy firewall :**

→ Filters the message based on contents of the message

→ works at application layer



→ When user client process sends a message, the proxy firewall runs a server Process to recieve the request

→ The server opens the packet at the application level and finds out if the request is legitimate.

Finding modulo Inverse. (11^{-1} mod 26)

Using Extended Euclidian Algo

$26 = 11(2) + 4$

$11 = 4(2) + 3$

$4 = 3(1) + 1$ → can be applied

$3 = 1(3) + 0.$

$\therefore$

$1 = 4 + 3(-1)$

$1 = 4 + (11 + 4(-2))(-1)$

$1 = 4 + 11(-1) + 4(2)$

$1 = 4(3) + 11(-1)$

$1 = (26 + 11(-2))3 + 11(-1)$

$1 = 26(3) + 11(-7)$

mod 26.

$1 = 0 + 11(-7)$ mod 26

$1 = 11(-7)$ mod 26

-7 mod 26 =

keep (+ve)

$\boxed{19}$ mod 26.

$19 * 11 = 1$ mod 26