Information Security

1) IP address
2) Static Dynamic
3) IPV4 and IPV6
4) Sub net mask
5) DNS

IP → Internet Protocol

Data < Moving data (Email, Facebook)
static data (ATM)

Netscape Navigator made SSL (Secure Socket Layer)

~~Authint~~
Confidentiality, Authentication, Integrity, ~~non repudation~~ non-repudiation.

Security Services

1) **Confidentiality:** It is the protection of transmitted data from passive attacks. With respect to release of message contains several level of protection can be identified.

2) **Authentication:** The Authentication service is concerned with assuring that a communication is Authentic. In case of single message such as a warning or alram signal, the function of authentication service is to assure the recipient that the message is from the source that it claims to be from.

Integrity: It says that the content of the message is intact i.e the content of the message is not changed in middle at the time of communication.

Non-repudiation: It ~~remains~~ prevents either sender or ~~recei~~ receiver from denying a transmitted message. Thus, when a message is sent the receiver can prove that the message was infact sent by the alleged sender. Similarly when a message is received, the sender can prove th

Rail-fence (Transposition ~~method~~ Technique)

Good Morning (Plaintext)

height [2]

G		o		~~b~~		o		n		n	
	o		d		M		r		i		g

Ritidip Sarkar height [2]

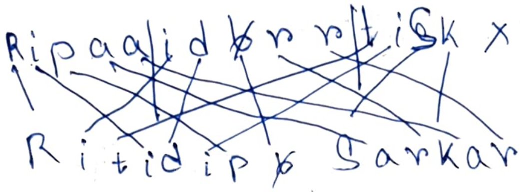
R		t		d		p		S		r		a	
	i		i		i		~~b~~		a		k		r

RtdpSraiii ~~b~~akr

Ritidip ~~b~~ Sarkar

height [3]

R			i			P			a			a		
	i			d			b			r			r	
		t			i			S			k			X



Input
E ---
D - -

Encrypt():
for (i)
else.

decrypt():

2) What is a cryptosystem?
A crypto system is a five tuple (P, C, K, E, D) where the following conditions are satisfied:
1) P is a finite set of possible plaintext.
2) C is a finite set of possible ciphertext.
3) K, the key space is finite set of possible keys.
4) For each $k \in K$ there is a encryption rule $e_k \in E$ and a coresponding decription rule $d_k \in D$
Each $e_k : P \rightarrow C$ and $d_k : C \rightarrow P$ are functions such that $d_k(e_k(x)) = x$ for every plaintext $x \in P$

Z_{26} = Any no bet 0-25

Shift Cipher (Substitution Technique)

Let $P = C = K = Z_{26}$, for $0 \leq k \leq 25$ define $e_k(x) = (x+k) \% 26$
and $d_k(y) = (y-k) \% 26$ where $x, y \in Z_{26}$

Def of Multiplicative inverse: Suppose $a \in Z_m$. The multiplicative inverse of a is an element $a^{-1} \in Z_m$ such that $a.a^{-1} \equiv a^{-1}.a \equiv 1 \mod m$

Public Key: n, e (encryption algo)
Private key: P, q, d (decryption algo)
RSA (Rivest-Shamir-Adleman)

RSA (Example)
Encrypt: (5, 14)
Text: B → 2
$2^5 \pmod{14} = 32 \pmod{14}$
$= 4$
ciphertext: 4 → D

Here $p=2$ $q=7$
$n=14$ $\phi(n) = 1 \times 6 = 6$
$e=5$ $d = 5, 11, \ldots$

Decrypt: (11, 14)
$4^{11} \pmod{14} = 4194304 \pmod{14}$
$= 2$
Text: 2 → B

① P, Q → Large semi-prime numbers (or Coprime)

② $n = P * Q$

③ $\phi(n) = (P-1) * (Q-1)$ coprime with n, $\phi(n)$
④ choose 'e' $\{1 < e < \phi(n)\}$
⑤ choose 'd' i.e. → $de \pmod{\phi(n)} = 1$ multiplicative inverse of $\phi(n)$.

This means 'd, e' is the multiplicative inverse of $\phi(n)$ such that

Let a & b are two positive int such that a is strictly less than b $(a < b)$ and a & b are relatively prime. (i.e. a & b doesn't have any common factor).
Then, a^{-1} is another integer less than b such that $a * a^{-1} = a^{-1} * a \equiv 1 \mod b$. This positive int a^{-1} is called multiplicative inverse of a in modulo b

Euclidean Algorithm

Let, $r_0 > r_1$

r_2 positive int.

then, $r_0 = q_1 r_1 + r_2$ $\quad 0 < r_2 < r_1$

$r_1 = q_2 r_2 + r_3$ $\quad 0 < r_3 < r_2$

$\vdots$

$r_{m-2} = q_{m-1} r_{m-1} + r_m$ $\quad 0 < r_m < r_{m-1}$

$r_{m-1} = q_m r_m$

Then it is not hard to show that $GCD(r_0, r_1)$

$= GCD(r_1, r_2) = \dots GCD(r_{m-1}, r_m) = r_m$

Extended

Now suppose we define a sequence of numbers $t_0, t_1 \dots t_m$ according to the following recurrence relation $t_0 = 0$

$t_1 = 1 \dots t_j = (t_{j-2} - q_{j-1} * t_{j-1}) \bmod r_0$ if $j \geq 2$

where the q_j is defined as above.

Corollary → if $GCD(r_0, r_1) = 1$ then $t_m = r_1^{-1} \bmod r_0$

Extended Algorithm

$n_0 = n$

$b_0 = b$

$t_0 = 0$

$t = 1$

$q = \left\lfloor \frac{n_0}{b_0} \right\rfloor$

$r = (n_0 - q) * b_0$

```
while (r > 0)
{
  temp = (t0 - q) * t
  if (temp >= 0)
    temp = temp mod n
  if (temp < 0)
    temp = n - {(-temp) mod n}
  t0 = t
  t = temp
}
```

$n_0 = b_0$

$b_0 = r$

$q = \lfloor n_0 / b_0 \rfloor$

$r = n_0 - q * b_0$

}

if $(b \neq 1)$

b has no inverse of modulo n

else

$b^{-1} = b \bmod n$

Multiplicative inverse using Extended EA

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	-1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
X	1	0	X	2	-5	X

multiplicative inverse of 3 mod 5.

$T = 0 - 1 \times 1$

$= -1$

$T = 1 - (-1) \times 1$

$= 1 + 1$

$= 2$

$T = -1 - (2) \times 2$

$= -1 - 4$

$= -5$

The value of T_1 in last row is 2.

∴ 2 is MI of 3 mod 5.

Points to note (A, B must be coprime)

$A > B$

$$B \overline{) A} (Q$$
$$\frac{B}{R}$$

$T_1 = 0$ & $T_2 = 1$ [For first row]

$T = T_1 - T_2 \times Q$

T_1 is Multiplicative inverse

KNAPSACK Algorithm (Martin Hellman, Ralph Merkle)
[This is first General Public-key algo)

Key → Public key (Encrypt) [Hard Knapsack]

Key → Private key (Decrypt) [Easy Knapsack] → weights are in superincreasing seq.

$\{1, 2, 4, 9, 20, 38\}$

$a_0, a_1, \ldots a_n$

$a_n > a_1 + a_2 + \ldots + a_{n-2} + a_{n-1}$

Solved problem

Superincreasing seq(D) = (1, 2, 4, 10, 20, 40) [private key]

n and m should be greater than sum of all no in seq.

Let m → 110

n → multiplier [No factor in common with modulus]

(1×31) mod 110 ⇒ 31

(2×31) mod 110 ⇒ 62

(4×31) mod 110 ⇒ 14

(10×31) mod 110 ⇒ 90

(20×31) mod 110 ⇒ 70

(40×31) mod 110 ⇒ 30

Plain text = [100100, 111100, 101110]

E = (31, 62, 14, 90, 70, 30) Public key.

100100 ⇒ 31 + 90 = 121

111100 ⇒ 31 + 62 + 14 + 90 = 197

101110 ⇒ 31 + 14 + 90 + 70 = 205

Cipher text = [121 197 205]

Decription

$n^{-1} \Rightarrow 31^{-1}$] 71

31 × x mod 110 = 1

(121 × 71) mod 110 = 11 → 100100

how to make 11 using private key (1, 10) so

(197 × 71) mod 110 = 17 → 111100

(205 × 71) mod 110 = 35 → 101110

Plaintext is achieved by receiver's side

15/11/22

Q) What is Cryptosystem?

- Subset sum
- Superincreasing seq.
- Extended euclidean algo.

Security for static data is access control. DB (DBMS) ATM

Q) <u>Congruency</u>: Suppose a and b are integers and m is a positive integers then we write $a \equiv b \pmod{m}$ if m devied by (b-a). The integer m is called modulus.

(code) ciser, affine

Q) <u>Shift cipher</u>: Let $P = C$

Q) M.I of $a \in Z_m$ is an element $a^{-1} \in Z_m$

i.e. $a.a^{-1} \equiv a.a^{-1} \equiv 1 \pmod{m}$

<u>Corollary</u>: The multiplicative inverse of a in mod m exists if a & m are relatively prime i.e. a & m doesn't have any common

Stream Cipher: In the crypto system we have studied to this point successive plaintext element are encripted using same key i.e. the cipher ~~text~~ string y are obtained as follows. $y = y_1 y_2 \ldots = e_K(x_1) e_K(x_2) \ldots$

Crypto system of this type are often called block ~~cypher~~ ciphers. An alternative approach is to use what are called stream ciphers. The basic idea is to generate a key stream $z = z_1 z_2 \ldots$ and use it to encript a plan text string $x = x_1 x_2 \ldots$ according to the rule of stream cipher $y = y_1 y_2 \ldots = e_{z_1}(x_1)\ e_{z_2}(x_2)$

Public key ~~crypt~~ & Private key Cryptosystem

In the classical model of cryptography we have been studying so far, we use same key k for encryption & decryption or the decryption key can be easily derived from encription key. For example, DES cryptosystem. The cryptosystem of this type are known as private key cryptosystem. Since, the encryption of e_K renders the system insecure.

The Idea behind the public key system that it might be possible to find a cryptosystem where it is computationaly infeasiable to determine d_K given e_K. Then the encryption rule could be made public by publishing it in a directory. The decription rule d_K will be kept private.

What is a crypto system
What is plaintext, cipher text, shift cipher, substitution cipher, ceaser cipher, affine cipher, Private key crypto system, Public key crypto system.
What is multiplicative inverse, EEA for finding MI, RSA crypto system, Knapsack crypto system, Digital signature, Hash function.
Firewall, SSL, S/MIME, PGP, Access Control
(Pretty Good Privacy)