Meghpara Jeel
160410116056
L41T-1

* ASSIGNMENT - 1 *

॥ नमामि देवी सरस्वति ॥

(1) Explain Security services and mechanism

→ An attack is an action that compromises the information or network security.

→ There are 2 types of attack:
(i) Passive attack (ii) Active attack

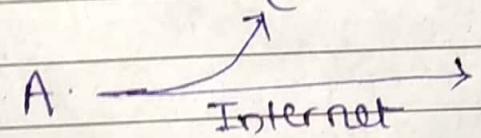
* Passive attack

The attacker only monitors the traffic attacking confidentiality of data.

(a) Release of msg content

→ It is easily understood.

→ Telephone conv, electronic mail msg, and a transferred file any contain sensitive or confidential information.



(b) Traffic Analysis

→ Suppose that we had way of masking contents of messages or other info?.

→ Even if they captured message, could not extract info from message.

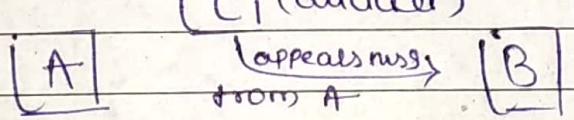
→ The common technique for making contents is encryption.

→ The opponent might determine loc & identify communication hosts and could observe

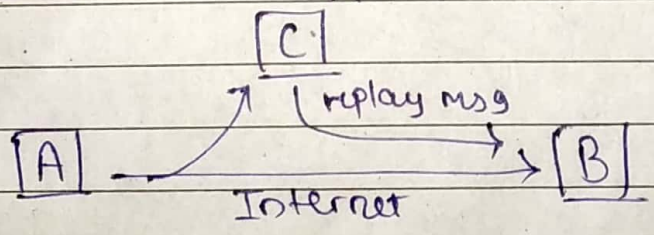
frequency and length of msg exchanged.
→ This info might be useful in guessing nature of comm^n that was taking place.
→ Passive attacks are very difficult to detect

* Active attacks.
——— Attacker tries to alter transmitted data.

(a) Masquerade.
→ It takes place when one entity pretends to be different entity.



(b) Replay
→ It involves passive capture of data unit and its subsequent retransmission to produce an authorized effect.



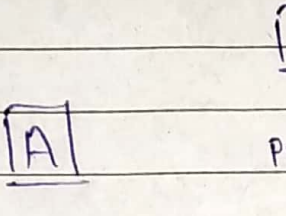
(c) Modification of message.
→ It simply means some portion of legimate message is altered, or that message are delayed or reordered, to produce unauthorized effect.

(d) Denial of services (DOS)

→ It prevents or inhibits normal use or management of communications facilities.

→ Attack may have specific target.

→ Another form of service denial is disruption of entire network, either by disabling network or by overloading it with many messages.



(2) Explain various types of cryptanalysis based on amount of info known.

→ Cryptanalysis attacks rely on nature of algo plus perhaps some knowledge of general characteristics of plaintext or even some simple-plaintext-ciphertext pairs.

* Brute-force attack
— Attacker tries every possible key on a piece of ciphertext until PT is obtained.

→ Based on amt of info known:

⇒ Cipher text only Attack: Attacker knows only cipher. It is easiest to defend.

⇒ Known plain text: Opponent has some PT-CT pairs. Or analyst may know some pattern.

⇒ Chosen plaintext: If analyst is able somehow to get source system to insert into system message chosen by analyst, then this attak is possible.

⇒ Chosen ciphertext: In this, analyst has cipher text and some PT-CT text pairs.

⇒ Chosen text: Attacker has got cipher text, chosen pt-ct pairs and chosen ct-pt pairs.

→ It is assumed that attackers know encryption & decryption algorithms.

(3) List Staganography technique & write disadv of it.

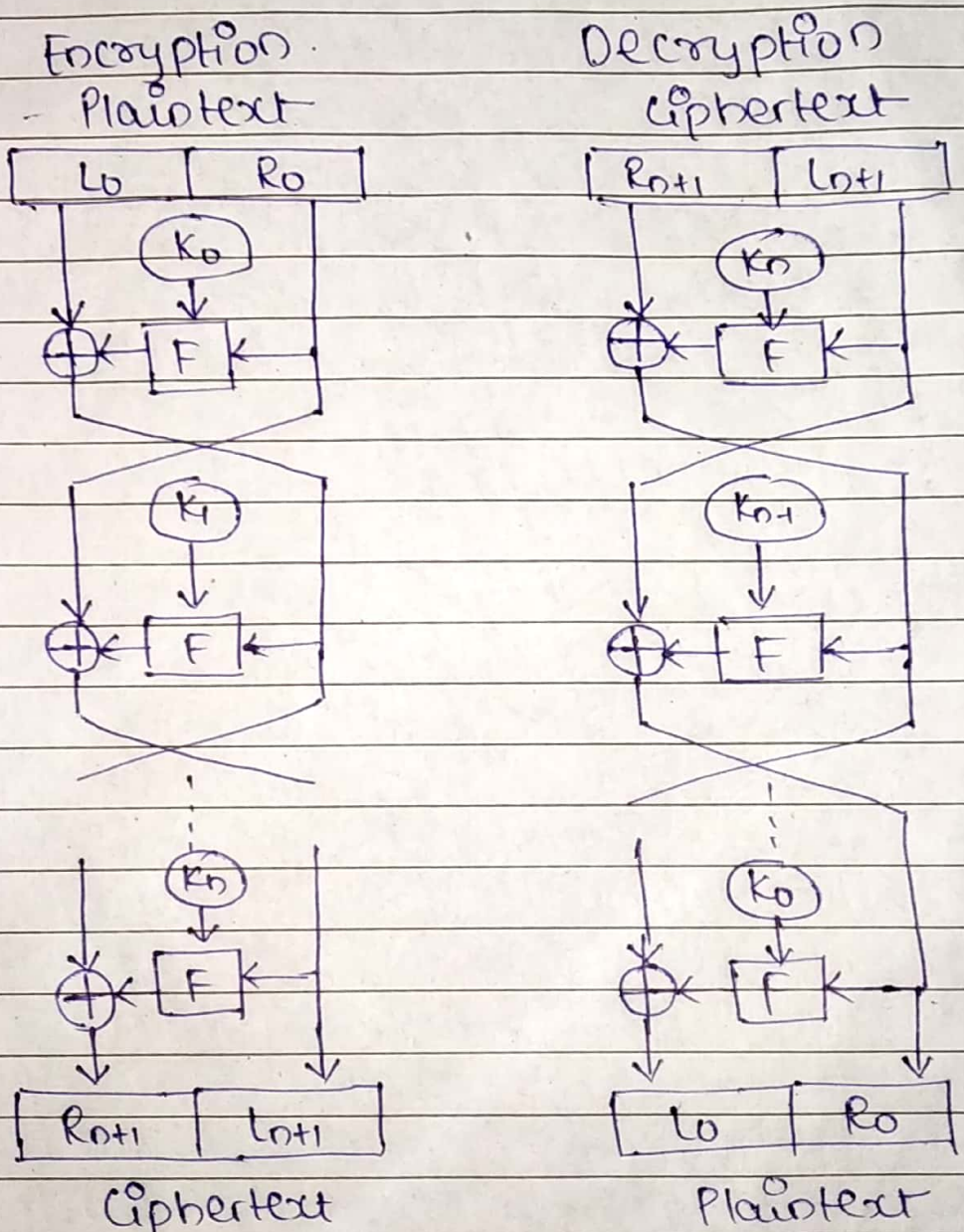
→ Some technique that have been used historically:-
(a) Character marking
(b) Invisible ink
(c) Pin punctures
(d) Typewriter correction ribbon.

→ Steganography has no of drawbacks when compared to encryption:-
⇒ It requires lot of overhead to hide relatively few bits of infon.
⇒ Once system of Steganography is discovered, it becomes virtually worthless.

(4) Draw and explain feisal structure for encryp and decryption with design parameter.

→ It is based on Idea that insted of using Ideal block

cipher which degrades performance, a "substitution permutation network" can be used.



* Encryption.

→ Input are plaintext blk of b bites & Key.

→ Plaintext blk is divided into two halves.

→ The two halves of data pass through rounds

of processing and then combine to produce ciphertext block.

→ Each round has inp & derived from previous rounds, as well as subkey derived from overall K. & all rounds have same structure.

→ A substitution is performed on left half of data. This is done by applying round F.

→ The output of function is XORed of pre round and a subkey as input.

→ Left and right halves are then swapped.

* Decryption

Decryption is same as encryption.

→ Ciphertext is input to algo subkeys are used in reverse order.

(5) Explain security of RSA.

→ Four possible approaches to attacking RSA algo are :-

(i) Brute Force

→ This involves trying all possible PR keys

→ Defense against this attack is tause large key.

(ii) Mathematical attacks.

→ There are 3 approaches :-

(a) Factor n into two prime factors. find $\phi(n) = (p-1)(q-1)$, which in turn enables $d = e^{-1} \pmod{\phi(n)}$

(b) Determine $\phi(n)$ directly with p & q. Again, this enables $d = e^{-1} \pmod{\phi(n)}$.

(c) Determine d directly, which is at least as time-consuming as factor problem.

(iii) Timing attacks.

→ These depends on running time of decryption algo.

→ The attack proceeds as follows:

→ Suppose that first j bits are known.

→ For given ciphertext, attacker can complete first j iterations of for-loop.

→ Operations of subsequent step depends on unknown exponent bit.

→ Therefore, if observed time to execute decry-algo is always slow when this particular iteration is slow with 1 bit, then this bit is assumed as 1.

→ Counter measures to this attack are:

- Constant exponentiation time
- Random delay
- Blinding

(iv) Chosen ciphertext attacks.

→ This type attack exploits properties of RSA.

$$E(PU, M1) \times E(PU, M2) = E(PU, [M1 \times M2])$$

Compute $X = (C \times 2^e) \bmod n$

$$Y = X^d \bmod n$$

But now note that $X = (C \bmod n) * (2^e \bmod n)$

$$= (M^e \bmod n) \times (2^e \bmod n)$$

$$X = (2M)^e \bmod n.$$

Therefore $Y = (2M) \bmod n$

(6) Explain linear and differential cryptanalysis.

→ Crytpanalysis is study of cryptosystem with objective of attacking them and decrypting codes and ciphers.

→ Linear and differential are both instances of known plaintext attacks where to be effective a certain amout of pt & ct must be known.

* Linear cryptanalysis.

is an approach where we aim to find affine approx to action of a cipher.

→ It posits a linear rel^n between ele^n of plain, cipher and the key.

⇒ Steps to perform linear crypt^n

(a) Find linear appox of non-linear parts (S-box)

(b) Combine linear approx of S-box with rest of operation done in encrypt^n algo.

(c) Use linear approx as a guide for which key to try first.

* Differential cryptanalysis.

is an approach to cryptanalysis whereby differences in inputs are mapped to differences in outputs & patterns in mapping of plaintext edits to ciphertext variation are used to reverse engineer a key.

→ The input & output differences of Sbox are considered in order to determine a high probability diff° pair.

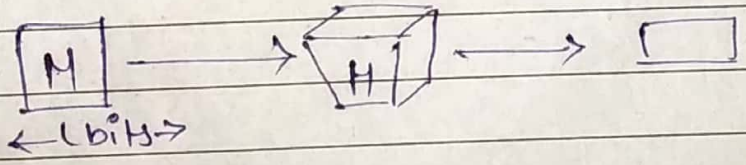
→ The subkey bits of cipher end up disappearing from difference expression because they are involved in both data point being differed.

(7) What is hash function? write application.

→ Hash function H accepts a variable length block of data as input & produce fixed-size has value.

→ A "good" has func° has property that results of applying func° to large set of inputs will produce output that are evenly distributed.

→ In general term, principal obj of hash is data integrity.



* Applications.

(1) Message authentication. → encrypt by public key & decrypt by only user having private key.
(2) Digital Signature → encrypted with user's private key & decrypted by anyone knowing user's public key.
(3) Simple hash functions.