Test 01

(Q1) What is perfect secrecy? Describe a system that achieves it

Ans -05 marks.

- Perfect secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.
- In effect this means that, no matter how much ciphertext you have, it does not convey anything about what the plaintext and key were.
- Formally, a system has perfect secrecy if the probability of any plaintext message remains the same even after observing the ciphertext.

$$P(M|C) = P(m)$$ For all msg m and ciphertext C.

- This means that knowing the ciphertext does not help an attacker to guess the plaintext, even with unlimited computational power

* System achieving perfect secrecy: One-Time Pad (OTP)

The one time pad is the only known encryption that achieves perfect secrecy.

- Description:-
  a) Each plaintext is combined with a truly random key of the same length as the plaintext.
  b) Encryption is usually done using XOR (or modular addition)
  c) Each key is used only once and then discarded

- Why OTP achieves perfect secrecy:-
  a) Every possible plaintext is equally likely for a given ciphertext.
  b) Without the key, the ciphertext provides no statistical info about the msg.

c) Even an attacker with infinite computational power cannot break it.

- **Conditions required for perfect secrecy in OTP**

1. The key must be truly random
2. The length must be equal to msg length
3. Key must be used only once
4. Key must be kept completely secret.

- **Limitations :-**

Although OTP is theoretically secure, it is impractical in real systems due to difficulties in secure key generation, storage and distribution.

Que 2) Explain briefly the concepts : One-way function, One-way hash function, trapdoor one-way fn

One way function :- It is, by definition, a mathematical function that is easy to compute in forward direction but computationally infeasible to invert.

Forward computation : $y = f(x)$ is easy

Inversion : $x = f(y)$ is infeasible.

- One-way fns are the foundation of modern assymmetric (or public key) cryptography. In fact, all asymm-cryptographic algo used to protect data and communicat^{n} base their security on the difficulty of ~~inverting~~ inverting these objects.

Eg :- (1) Diffie-Hellman key exchange $\Rightarrow f(x) = g^x \bmod p$.
* calculating power x-th of g modulo p is easy but given a +ve integer h less than p, finding element x for which $g^x = h \bmod p$ is hard.

(2) multiplying 2 large primes is easy but factoring is hard.

One way hash function:- one way hash function maps data of arbitrary length to a fixed-length hash value and is infeasible to reverse.

- Furthermore, a one-way hash fn is designed in such a way that is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way).
- A document's hash can serve as a cryptographic equivalent of the document since it is infeasible to produce a document that would hash to a given value or find two document that hash to same value.
- This makes a one-way hash fn a central notion in public key cryptography. When producing a digital signature for a document, we no longer need to encrypt the entire document with a senders private key (which can be extremely slow). It is sufficient to encrypt the documents hash value instead.
- Properties:- (1) Pre-image resistance :- given h, it is hard to find x such that $H(x) = h$
  (2) Second preimage resistance :- hard to find another $x' \neq x$ with same hash.
  (3) Collision resistence :- hard to find any two different inputs with the same hash.

Trapdoor one-way function:- A trapdoor one-way function is a special type of one-way function that is easy to invert only if a secret trapdoor is known.

- without trapdoor :- Inversion is infeasible
- with trapdoor :- Inversion becomes easy.

These have particularity of being easy to reverse as long as some secret information is known (trapdoor), while, otherwise, they act like a normal one-way f^n

Eg :- RSA is a trapdoor one-way f^n because computing $f(m) = m^e \bmod N$ is easy but reversing it is hard unless the private key d is known which acts as a trapdoor.

Why is it hard to reverse?

Given $c = m^e \bmod N$

Finding m from c means :

- Taking an e-th root modulo N
- This is extremely hard without knowing p & q