181240116001
Vishwas Acharya

Page No.: 1
Date: / /

CNS
Assignment - 1

1) Explain Symmetric Cipher Model in detail.

Ans - A symmetric Cipher Model are ~~brod~~ broadly contain five parts.

- PlainText :- This is the original intelligible message

- Encryption algorithm :- The encryption algorith performs various substitutions and transformations on the plaintext. It takes in plaintext and key and gives the ciphertext.

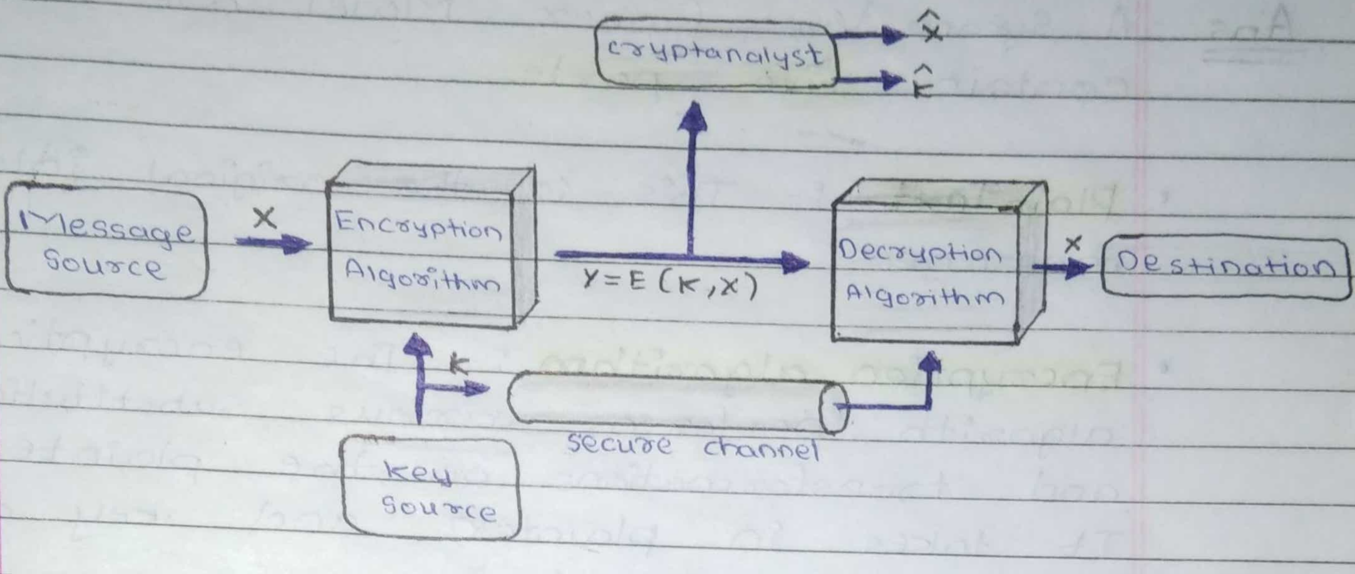
- Secret key :- The key is a value independent of the plaintext and of the algorithm. Different keys will yield different outputs

- Cipher Text :- This is the scrambled message produced as output. ~~It~~ It depends on the plaintext and the secret key.

- Decryption algorithm :- Runs on the cipher-text and the key to produce the plaintext. This is essentially the encryption algorithm run in reverse.

- Figure or diagram of symmetric cipher model is given further.

⊙ Figure →



- Two basic requirements of encryption are:

1. Encryption algorithm should be strong. An attacker knowing the algorithm and having any number of ciphertext should ~~b~~ not be able to decrypt the ciphertext or guess the key.

2. The key shared by the ~~st~~ sender and the receiver should be secret.

- let the plaintext be $X = [X_1, X_2, \dots, X_m]$, key be $K = [K_1, K_2, \dots, K_j]$ and the ciphertext produced by $Y = [Y_1, Y_2, \dots, Y_n]$. Then, we can write

$$Y = E(K, X)$$

- Here E represents the encryption algorithm and is a function of plaintext X and key K.

- The receiver at the other ends decrypts the ciphertext using the key.

$$X = D(K, Y)$$

- Here D represents the decryption algorithm and it inverts the transformations of encryption algorithm.

- An opponent not having access to X or K may attempt to recover K or X or both.

- It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms.

- If the opponent is interested in only this particular message, then the focus of the effort is to recover by generating a plaintext estimate $\hat{X}$.

- If the opponent is interested is being able to read future messages as well then he will attempt to recover the key by making an estimate $\hat{K}$.

2) What is cryptography? Explain substitution techniques in detail.

Ans - The area of study containing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

- Cryptographic systems are characterized along three independent dimensions.

- Type of encryption operations used
  - ↳ substitution
  - ↳ Transposition
  - ↳ Product

- Number of keys used
  - ↳ Single-key / private
  - ↳ Two-key / public

- Way in which plaintext is processed
  - ↳ block
  - ↳ Stream

◉ Substitution Techniques

- Various conventional encryption schemes or substitution techniques are given further:

1. **Caesar Cipher** : In this techniques, to encrypt the plain text, each alphabet of the plain text is replaced by the alphabet three places. further.

2. **Monoalphabetic Cipher** : In this techniques, the cipher alphabet for each plain text alphabet is fixed for entire encryption.

3. **Playfair Cipher** : In this technique, multiple letters are encrypted at a time and it uses 5x5 matrix which is also known as key matrix.

4. **Hill Cipher** : This cipher is based on linear algebra and each letter is represented by numbers from 0 to 25 and calculations are done module 26.

5. **Vigenère Cipher** : This is a type of polyalphabetic cipher and in this cipher, the key determines which particular substitution is to be used.

- Hence, this are techniques of substitution in cryptography.

3) Write a note on finite fields.

Ans - A finite fields is simply a field with a finite number of elements.

- It can be shown that the order of a finite field (number of elements in the field) must be a power of a prime p^n where → n is a positive integer.
- A order p can be defined using arithmetic mod p.
- A field (F, +, ·) is called a finite field if the set F is finite.
- Ex, Zp (p - prime) with + & * mod p is a finite field.
- It also known a Galois field (GF). (GF)(p^k)

- Properties

↳ It can be shown that finite field have order p^n where p is a prime.

↳ It can be shown that for each prime p & each positive integer n, there is, up to isomorphism, a unique finite field of order p^n.

↳ Let GF(p^n) represent a finite field of order p^n.

- **Group : $\{G, \cdot\}$** :- A set of elements or number with a binary operator "·".

- Obeys:
  ↳ Closure : $a \in G, b \in G \Rightarrow a.b \in G$
  ↳ Associative: $(a.b).c \Rightarrow a.(b.c)$
  ↳ Identify:(e) $e.a \Rightarrow a.e = a$
  ↳ Inverse a^{-1} : $a.a^{-1} = e$

- If commutative $a.b = b.a$ then is called an abelian group.

- **Cyclic Group** :- It define exponentiation as repeated application of operator.

↳ Ex., $a^3 = a.a-a$
Identify be $e = a^0$

↳ A group is cyclic if every element is a power of some fixed element $a \in G$

↳ $b = a^k$; for some a & every b in group.

↳ Here, a is said to be a generator of the group.

- **Ring $\{R, +, \times\}$** :- A set of "numbers" with two operations (addition & multiplication) where are:

↳ An abelian group with addition operation

& multiplication (has closure, is associative, distributive over addition).
$a(b+c) = ab + ac$

↳ If multiplication operation is commutative, it forms a commutative ring ($ab=ba$) $a, b \in R$

↳ If multiplication opertain has multiplicative identify & no zero divisons, it forms an integral domain.

- **Field {F, +, x}** :- A set of numbers with two operations

(i) Abelian group for addition
(ii) Abelian group for multiplication (ignoring 0)
(iii) Ring

↳ Obeys :- It has multiplicative inverse a^{-1}:
$a \cdot a^{-1} = e$

↳ It has hierarchy with more axioms/laws, group > ring > field

4) Explain Euclidean algorithm in detail.

Ans - The Euclidean algorithm is an efficient way to find the GCD (a, b).

- The Euclidean algorithm ~~algo~~ is derived from the observation that if a & b have a common factor d (ie. $a=m.d$ & $b=n.d$) then d is also a factor in any difference between them, vis: $a - p.b = (m.d) - p.(n.d) = d.(m - p.n)$.

- Euclid's Algorithm keeps computing successive differences until it vanishes, at which point the greatest common divisor has been reached.

- Theorem :

  - $GCD(a, b) = GCD(b, a \bmod b)$

- Algorithm :

```
EUCLID (a,b)
1. A = a ;  B = b
2. if B = 0 return A = gcd (a,b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```