INDEX

Page No.:
Date: / /

Name :- Vishwas R. Acharya

Enrollment No. :- 181240116001

Subject :- Cryptography and Network Security

Sem :- 6

Sr.No	Name	Date
1.	Assignment - 1	5/1/2021
2.	Assignment - 2	26/2/2021
3.	Assignment - 3	12/3/2021
4.	Assignment - 4	30/3/2021
5.	Assigoment - 5	12/4/2021

CNS
Assignment - 1

1&12401160001
Vishwas Acharya
Page No.: 1
Date: 5/1/21

1) Explain Symmetric Cipher Model in detail.

Ans - A Symmetric Cipher Model are ~~broad~~ 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.

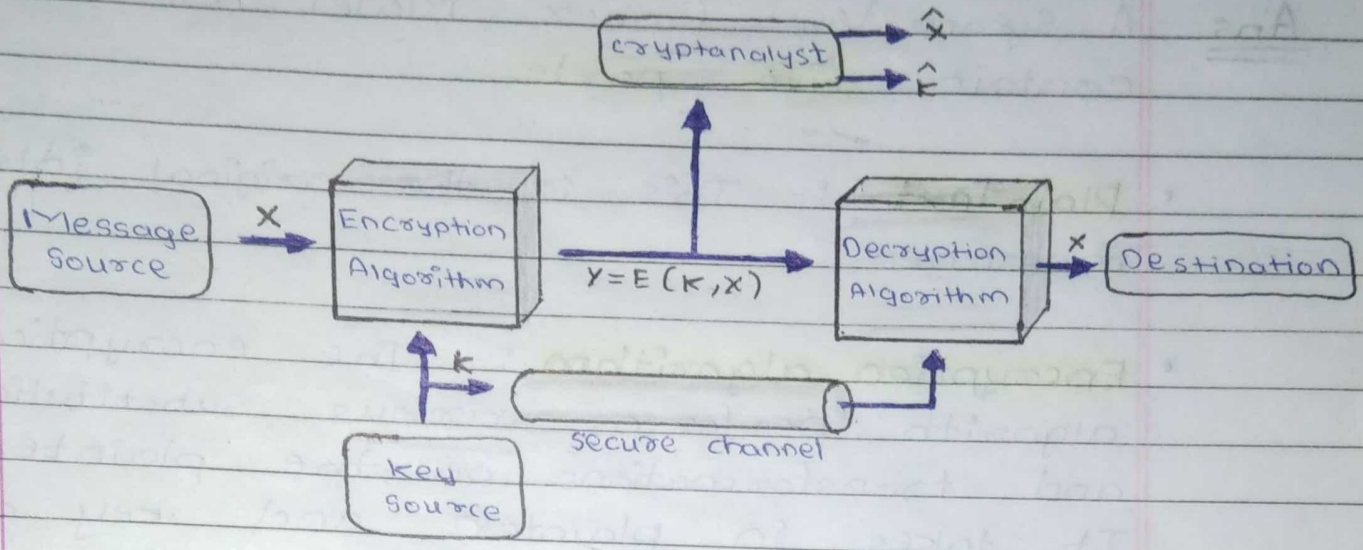
- **Secret key** :- The key is a value independent of the plaintext and of the algorithm. Different keys will yield different outputs

- **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 not be able to decrypt the ciphertext or guess the key.

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

- let the plaintext be $X = [X_1, X_2, \ldots, X_m]$, key be $K = [K_1, K_2, \ldots, K_j]$ and the ciphertext produced by $Y = [Y_1, Y_2, \ldots, Y_n]$. 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 $(F, +, \cdot)$ is called a finite field if the set F is finite.
- Ex, Z_p (p - prime) with + & * mod p is a finite field.
- It also known a Galois field (GF). $(GF)(p^n)$

• 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 " $\cdot$ ".

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

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

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

↳ Ex., $a^3 = a \cdot a \cdot a$
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 operatain has multiplicative identify & no zero divisons, it forms an integral domain.

- Field $\{F, +, \times\}$:- 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

CNS
Assignment-2

1812401160001
Vighnas Acharya

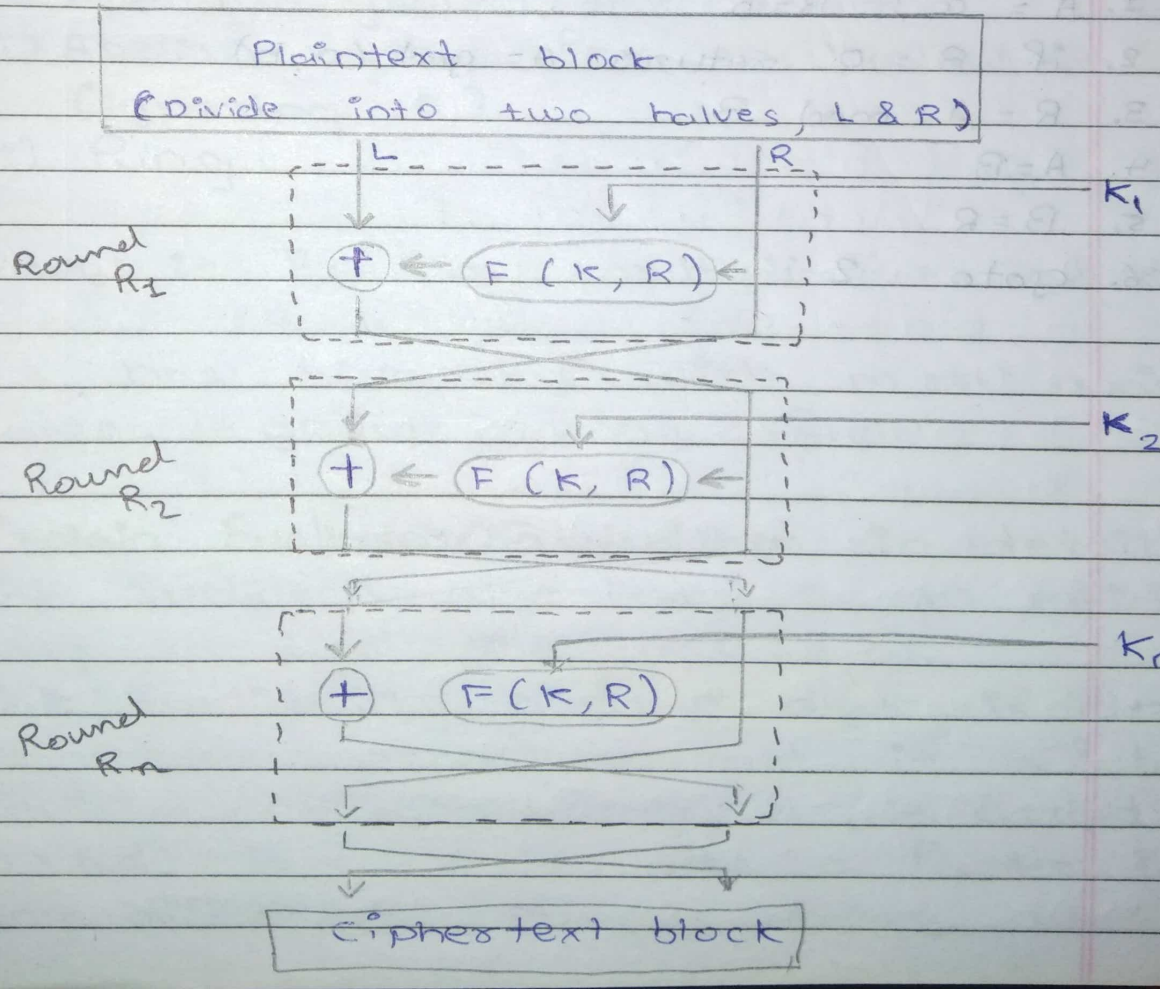
Page No.: 1
Date: 26/2/21

1) Write note on feistel cipher with figure.

Ans :- Feistel Cipher is not a specific of block cipher.

- It is a design model from which many different block ciphers are derived.
- DES is just one example of a Feistel Cipher.
- A cryptographic system based on Feistel Cipher structure uses the same algorithm for both encryption and decryption.

- Figure:



1. Encryption Process:

↳ The encryption process uses the fiestel structure consisting multiple rounds of processing of the plaintext, each round consisting of a substitution step followed by a permutation step.

2. Decryption Process:

↳ It's same as encryption process with the only difference is that the subkeys used in encryption are used in reverse order.

3. Numbers of Rounds:

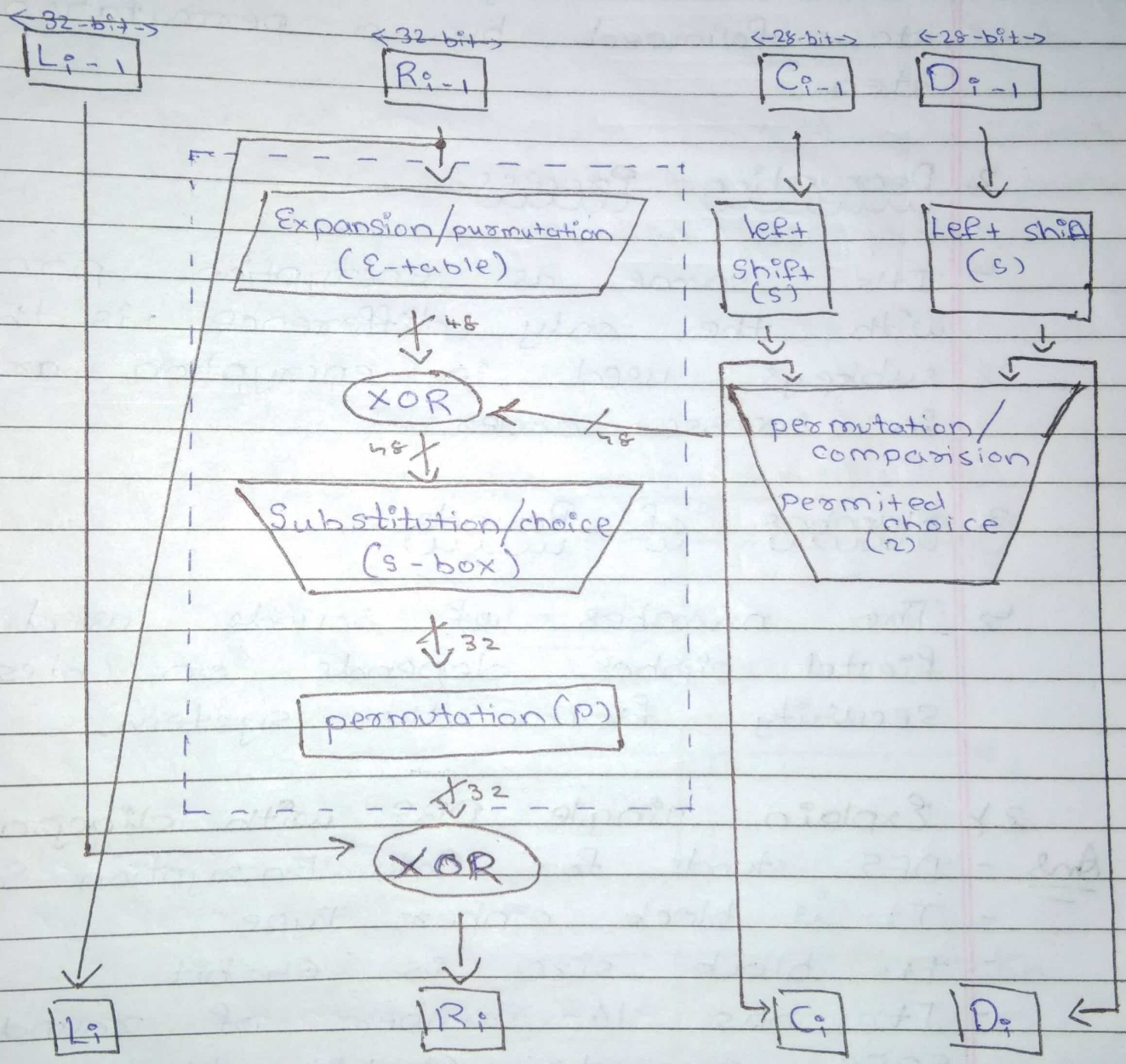
↳ The number of rounds used in fiestel cipher depends on desired security from the system.

2Y Explain single DES with diagram.

Ans
- DES stands for Data Encryption Satandard.
- It is block cipher Type.
- Its block size is 64-bit.
- It has 16 number of rounds.
- SDES encrypts 64-bit blocks using a 56-bit key and produces a 64-bit cipher text.
- DES is based on the two fundamental

attributes of cryptography
↳ substitution (aka confusion)
↳ Transposition (aka diffusion)

- Figure:



3) Write about AES with example.

Ans - AES stands for Advanced Encryption Standard.
- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the AES.
- It is found at least six time faster than triple DES.
- A replacement for DES was needed as its key size was too small.
- With increasing computing power, it was considered vulnerable against exhaustive key search attack.
- Triple DES was designed to overcome this drawback but it was found slow.

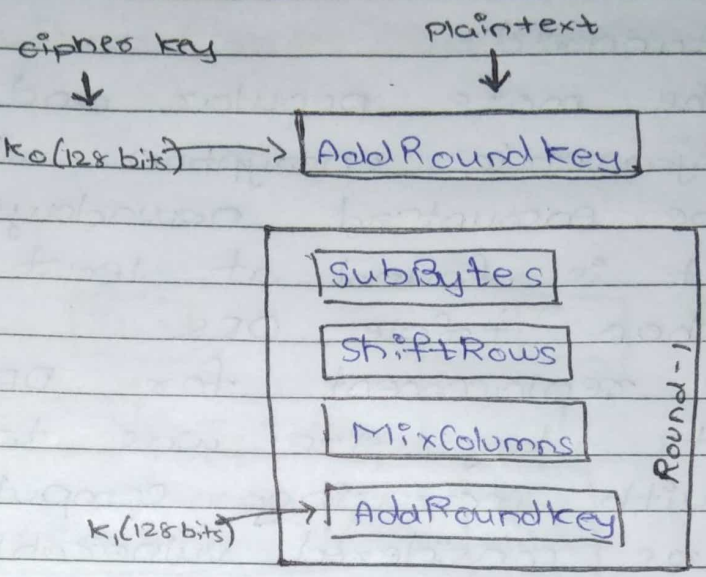
• Features:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details.
- Software implementable in C and Java

• Encryption Process

↳ Here, we ristrict to description of a typical round of AES encryption.
↳ Each round comprise of four sub-processes.

- The first round process is depicted below-



- Decryption Process

↳ The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

↳ Each Round consists of the four processes conducted in the reverse order

  ↳ Add round key
  ↳ Mix columns
  ↳ Shift rows
  ↳ Byte substitution

↳ Since sub-processes in each round are in reverse manner, unlike for a feistel cipher, those algorithm needs to be separately implemented, although they are very close related.

4.1 Write down the difference between block cipher and stream cipher.

Ans - Both cipher difference is given below:

BLOCK Cipher	STREAM Cipher
• It converts the plain text into cipher text by taking plain text's block at a time.	• It converts the plain text into cipher text by taking 1 byte of plain text at a time.
• It uses either 64 bits or more than 64 bits	• While stream chiper uses 8 bits.
• The complexity of block cipher is simple	• While stream cipher is more complex.
• Block cipher uses confusion as well as diffusion	• While stream cipher uses only confusion
• In block cipher, reverse encrypted text is hard	• While in stream cipher, reverse encrypted text is easy
• Algo. modes are: ECB & CBC	• Algo. modes are CFB & OFB
• It works on transposition techiques like caesar, Polygram substitution cipher, etc...	• It works on substitution techniques like railfence, Columnar transposition, technique, etc..

18124011600l
Vishwas Achgrya

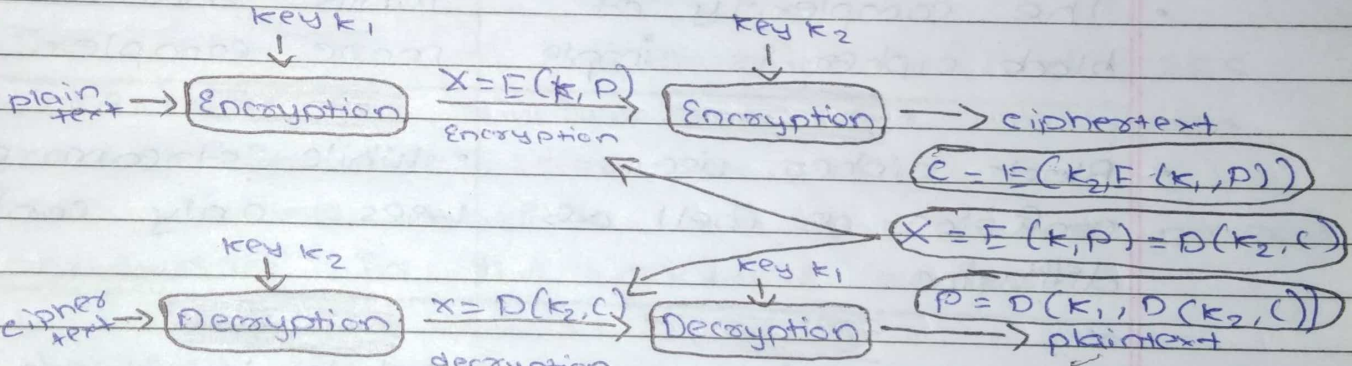
Page No.: 1
Date: 12/3/21

CNS
Assignment-3

1. Explain Multiple Encryption in detail.

Ans - Given the potential vulnerability of DES to a brute-force attack, there has been considerable interest in finding an alternative.
- For DES requires 2^{56} operations for brute force attack.
- One approach is to design a completely new algorithm, of which AES is a prime example.
- Another alternative, which would preserve the existing investment in software and equipment, is to use multiple encryption with DES and multiple keys.

- **Double DES**



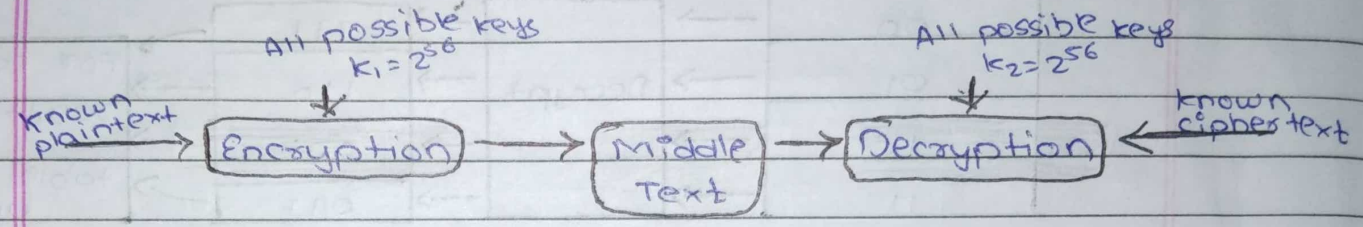
↳ For double DES, 2 x 56-bit keys, meaning 112-bit key length.
↳ Requires 2^{112} operations for brute force attack.
↳ Meet-in-the-middle attack makes it easier.

- **Meet in the Middle Attack**

↳ This attack involves encryption from one end, decryption from the other and matching the results in the middle.

↳ Suppose cryptanalyst knows P_i and corresponding C_i.

↳ Now, the aim is to obtain the values of K_1 and K_2.



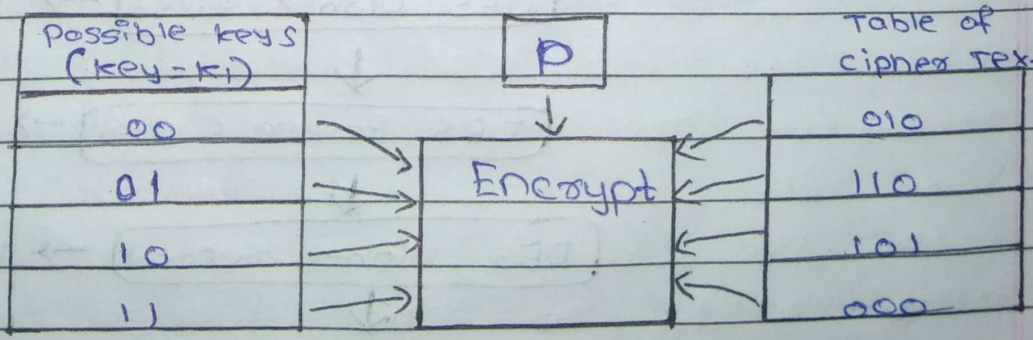
↳ No. of Encryption and Decryptions : $2^{56} + 2^{56} = 2^{57}$

↳ For Double DES requires 2^{57} operations for brute force attack.

=> **STEP - I**

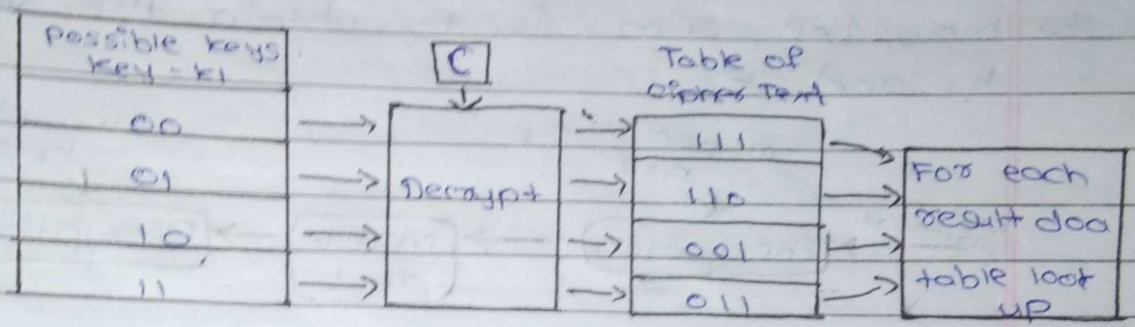
↳ For all possible values (2^{56}) of key, K_1, the cryptanalyst would encrypte the known plaintext by performing $E(K_1, P)$

↳ The cryptanalyst would store output in a table.



⇒ STEP - 2

↳ Cryptanalyst decrypt the known ciphertext with all possible values of K2.
↳ In each case cryptanalyst will compare the resulting value with the all values in the table of ciphertext



• TRIPLE DES

↳ It is an encryption technique which uses three instance of DES on same plain text.
↳ It uses there different type of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

64-bit Plain Text
↓
DES cipher first → KEY 1 (56 bit)
↓
DES Reverse Cipher → KEY 2 (56 bit)
↓
DES cipher second → key 3 (56 bit)
↓
64-bit Cipher Text

↳ Triple DES is also vulnerable to meet-in-the middle attack because of which it give ~~tab~~ total security level of 2^112 instead of using 168 bit of key.
↳ The block collision attack can also be done because of short block size and using same key to encrypt large size of text.
↳ It is also vulnerable to sweet 32 attack.

2) Write note on Cipher Block Chaining Mode.

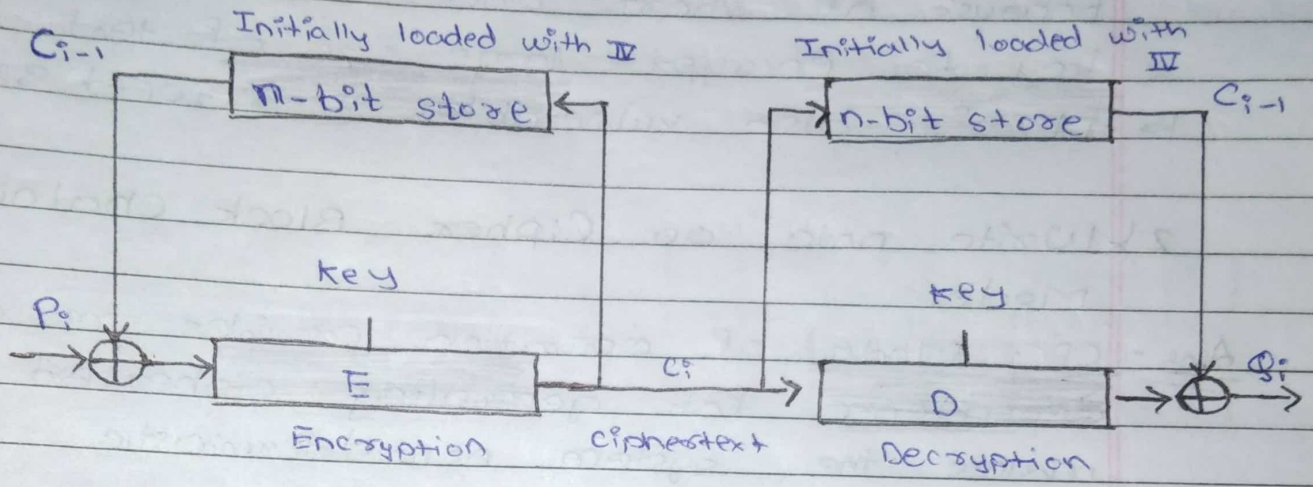
Ans - CBC Mode of operation provides message dependence for generating ciphertext and makes the system non-deterministic.

- **Operation**

↳ The operation of CBC mode is depicted in the following illustration.
↳ The steps are as follows -

- Load the n-bit Initialization Vector (IV) in the top register.
- XOR the n-bit plaintext block with data value in top register
- Encrypt the result of XOR operation with underlying block cipher with key K.
- Feed ciphertext block into top register and continue the operation till all plaintext blocks are processed.
- For decryption, IV data is XORed with first

ciphertext block decrypted. The first ciphertext block is also fed into to register replacing IV for decrypting next ciphertext block.



- Analysis of CBC Mode

↳ In CBC Mode, the current plaintext block is added to the previous ciphertext block, and then the result is encrypted with the key.

↳ Decryption is thus the reverse process, which involves decrypting the current cipher text and then adding the previous cipher text block to the result.

↳ Advantage of CBC over ECB is that changing IV results in different ciphertext for identical message. On the drawback side, the error in transmission gets propagated to few further block during

decryption due to changing effect.

↳ It is worth mentioning that CBC mode forms the basis for a well-known data origin authentication mechanism. Thus, it has an advantage for those applications that require both symmetric encryption and data origin authentication.

3) Write note on Electronic Code Book.

Ans → This mode is a most straightforward way of processing a series of sequentially listed message blocks.

- **Operation**

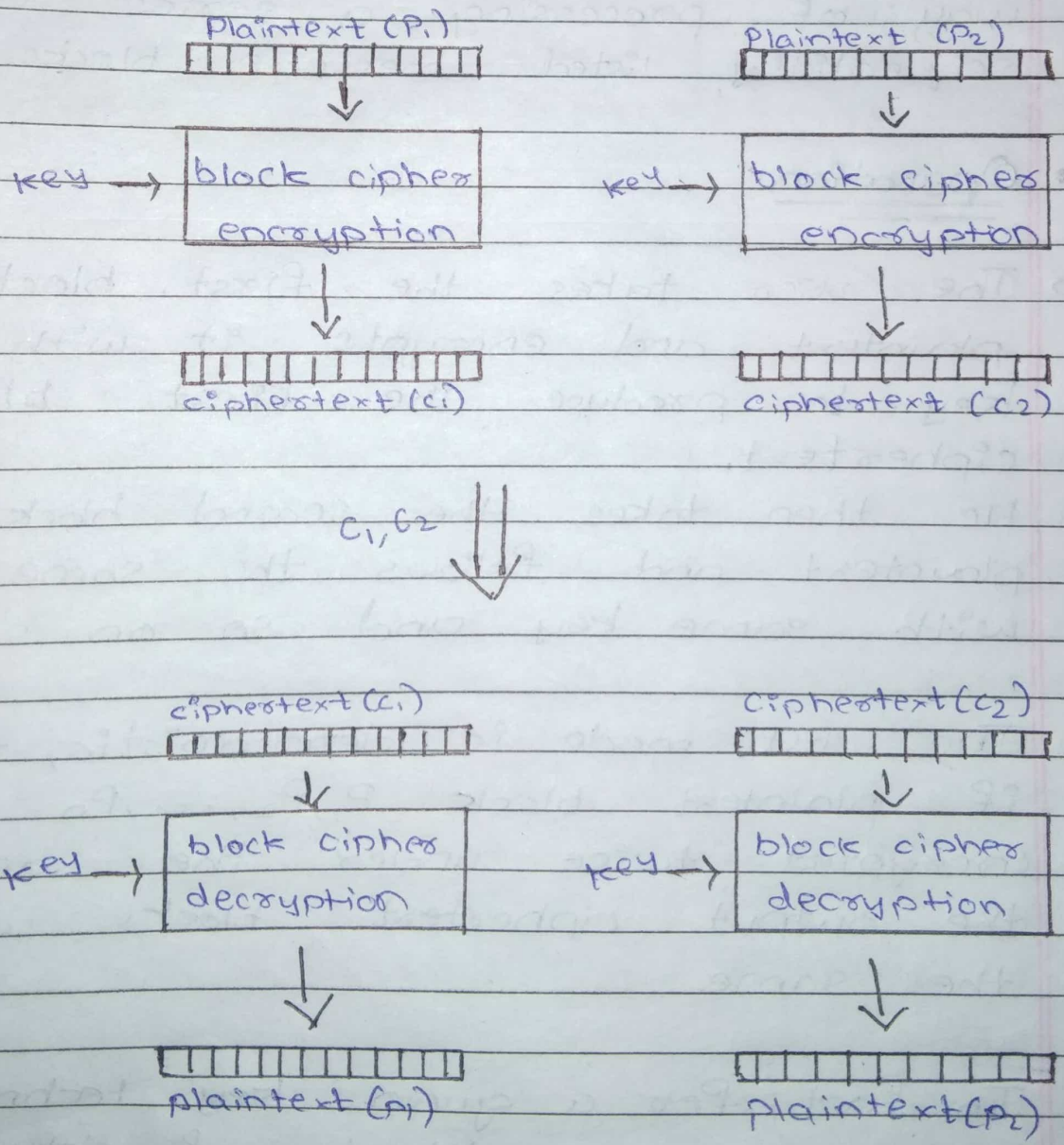
↳ The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.

↳ He then takes the second block of plaintext and follows the same process with same key and so on so forth.

- The ECB mode is deterministic, that is, if plaintext block $P_1, P_2, \ldots, P_n$ are encrypted twice under the same key, the output ciphertext blocks will be the same.

- In fact, for a given key technically we can create a codebook of ciphertexts for

all possible plaintext blocks.
- Encryption would then entail only looking up for required plaintext and select the corresponding ciphertext.
- Thus, the operation is analogous to the assignment of code words, in a codebook, and hence get an official name - Electronic Codebook mode of operation (ECB).
- It is illustrated as follows -



- **Analysis of ECB Mode**

↳ In reality, any application data usually have partial information which can be guessed.

↳ For example, the range of salary can be guessed.

↳ A ciphertext from ECB can allow an attacker to guess the plaintext by trial-and-error if the plaintext message is within predictable.

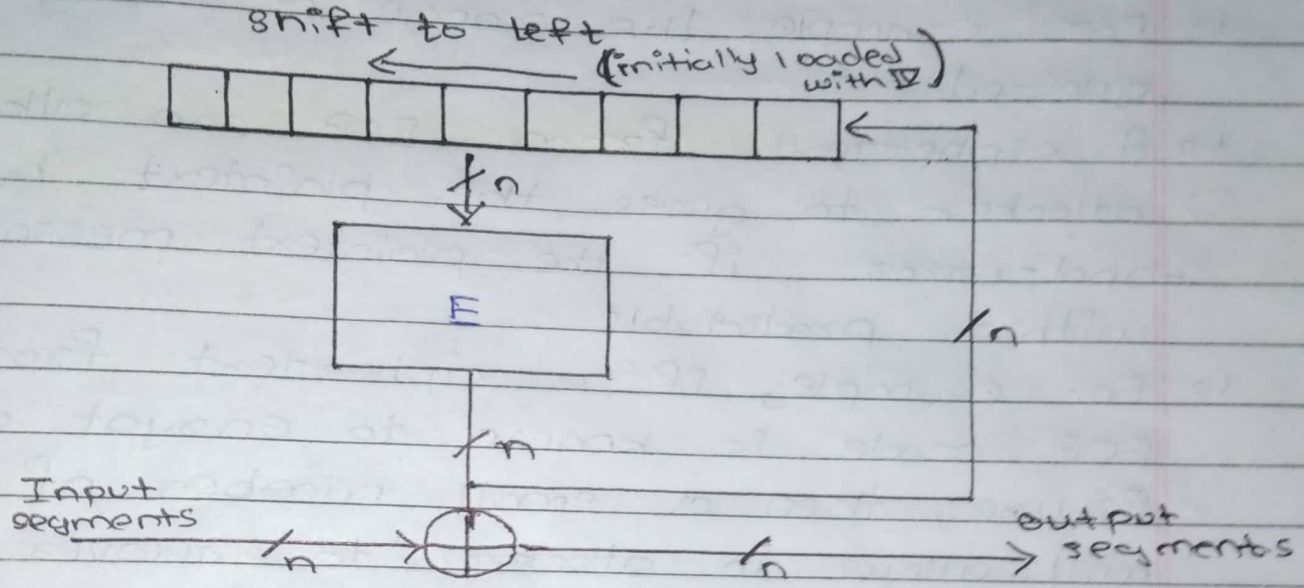
↳ For example, if a ciphertext from the ECB mode is known to encrypt a Salary figure, then a small number of trials will allow an attacker to recover the figure.

↳ In general, we do not wish to use a deterministic cipher, and hence the ECB mode should not be used in most applications.

4b Write note on Output Feedback mode.

Ans
- It involves feeding the successive output blocks from the underlying block cipher back to it.
- These feedback blocks provide string of bits to feed the encryption algorithm which act as the key-stream generator as in case of CFB mode.
- The key stream generated is XOR-ed with the plaintext blocks.

- The OFB mode requires an IV as the initial random n-bit input block.
- The IV need not be secret.
- The operation is depicted in the following illustration:-



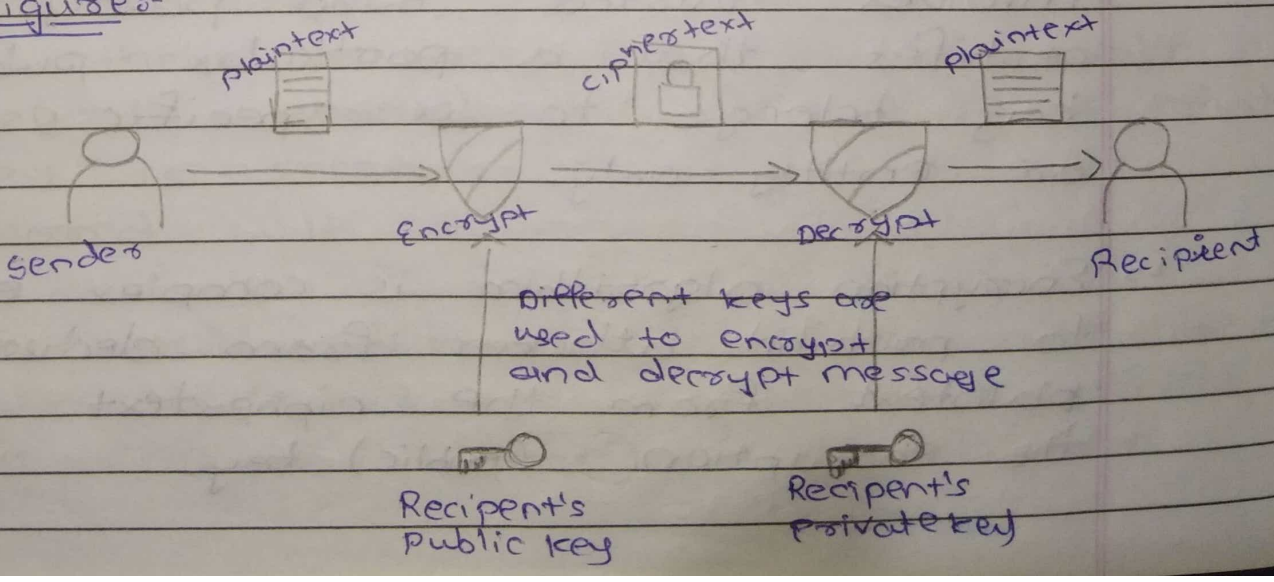
CNS
Assignment-4

18124011600 1
Assign. Vishwas Acharya
Page No.: 1
Date: 30/3/21

1) Explain Public key Cryptosystems with applications.

Ans - Unlike symmetric key cryptography, we do not find historical use of public-key cryptography.
- It is a relatively new concept.
- Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.
- With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale.
- The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosytems.

- Figure:-



- Public key encryption scheme

↳ Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.

↳ Each receiver possesses a unique decryption key, generally referred to as his private key.

↳ Receiver needs to publish an encryption key, ~~or~~ referred to as his public key.

↳ Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receivers.

↳ Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.

↳ Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.

↳ Though private and public keys are related mathematically, it is not be fasible to calculate the private key from the public key.

↳ In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

- There are three types of Public key Encryption schemes

  ↳ RSA Cryptosystem.
  ↳ ElGamal Cryptosystem
  ↳ Elliptic Curve Cryptography (ECC)

2) Explain RSA algorithm with example.

Ans - The RSA algorithm is an asymmetric cryptography algorithm; this means that it uses a public key and a private key. (i.e. two different, mathematically linked keys).

- As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

- The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.

The following illustration highlights how asymmetric cryptography works:

- How it works

↳ The RSA algorithm ensures that the keys, in the above illustration, are as secure as possible.

↳ The following steps highlight how it works:

1. Generating the keys

↳ Selecting two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out.

↳ Calculate $n = x * y$

↳ Calculate the totient function; $\phi(n) = (x-1)(y-1)$

↳ ~~To~~ Select an integer e, such that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) makes up the public key.

NOTE: Two integers are co-prime if the only positive integer that divides them is 1.

↳ Calculate d such that $ed \equiv 1 \pmod{\phi(n)}$. d can be found using the extended euclidean algorithm. The pair (n,d) makes up the private key.

2. ENCRYPTION

↳ Given a plaintext P, represented as a number, the ciphertext C is calculated as:

$C = P^e \bmod n$

3. DECRYPTION

↳ Using the private key (n,d) the plaintext can be found using:

$P = C^d \bmod n$.

3) Explain Diffie-Hellman key exchange algorithm with example.

Ans :- The purpose of diffie-Hellman algorithm is to enable two users to securely exchange a key that can be used for subsequent encryption of message.

- This algorithm depends for its effectivness on the difficulty of computing discrete ~~algorithms~~. logarithm.

- **Primitive root**

- Let p be a prime number
- Then a is a primitive root for p, if the powers of a modulo p generates all integers from 1 to p-1 in some permutation

$$a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$$

- **Discrete Logarithm**

- For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$$b = a^i \pmod p \quad \text{where } 0 \le i \le (p-1)$$

- The exponent i is referred as the discrete logarithm of b for the base a, mod p. It expressed as below.

$$\text{bollog}_{a,p}(b)$$

- User A and user B agree on two large prime numbers q and α
- User A and User B can use insecure channel to agree on them.
- User A selects a random integer $X_A < q$ and calculates Y_A

- Global Public Elements

↳ q = prime number
↳ α = $\alpha < q$ and α is primitive root of q

- User A key Generation

↳ Select private X_A $X_A < q$
↳ Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

- User B key generation

↳ Select private X_B $X_B < q$
↳ Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

⊙ Example

- Alice and bob agrees on a prime number $q = 23$
- $\alpha = 5$ as primitive root of q
- Alice selects a private integer $X_A = 6$
- Alice computes $Y_A = \alpha^{X_A} \bmod q \Rightarrow Y_A = 5^6 \bmod 23 = 8$
- Bob selects a private integer $X_B = 15$
- Bob computes $Y_B = \alpha^{X_B} \bmod q \Rightarrow Y_B = 5^{15} \bmod 23 = 19$
- Alice sends Y_A to Bob and Bob sends Y_B to Alice
- Alice compute key $k = (Y_B)^{X_A} \bmod q \Rightarrow k = (19)^6 \bmod 23$
  $k = 2$
- Bob computes key $k = (Y_A)^{X_B} \bmod q \Rightarrow k = (8)^{15} \bmod 23$
  $k = 2$

4) Explain Man-in-Middle attack in detail.

- When there is an unwanted proxy in the network intercepting and modifying the requests/response, this proxy is called as Man-in-the middle.
- The network then is said to be under a Man in the middle attack.
- The interesting point lies in the fact that this rouge proxy is often misunderstood as a legitimate endpoint in a communication by the other endpoint.

- Example:-

- Suppose you ar connected to a WiFi network and doing a transaction with your bank.
- An attacker is also connected to the same WiFi.
- The attacker does the following:

1. Attacker sends the rogue ARP packets in the network the map the IP address of the access point to the MAC address of attacker's device.

2. Each device connected in the network caches the entry contained in the rogue packets.

3. Your device uses ARP to send the packets destined for your bank's web server to the access point (which is the default gateway for the network).

4. The packets get sent to the attacker's machine.

5. Attacker can now read and modify the requests contained in the packets before forwarding them.

- This way the attacker is suitably situated between you and your bank's server. Ever bit of sensitive data that you send to your server including your login password, is visible to the attacker. ARP cache poisoning is one of the many ways to perform an MITM attack; other ways are:-

1. DNS spoofing
2. IP spoofing
3. Setting up a rogue WiFi AP
4. SSL spoofing etc.

CNS
Assignment-5

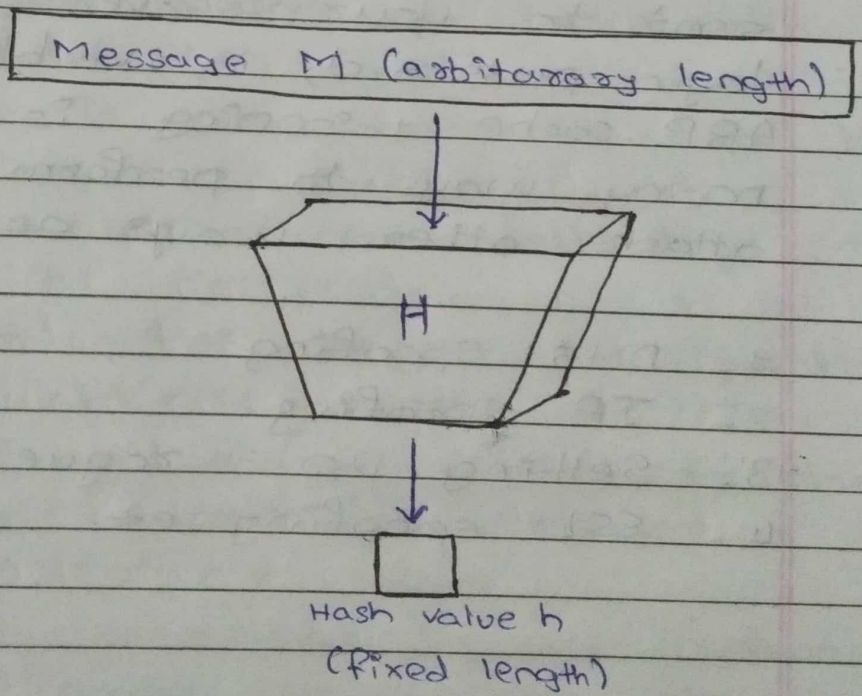
1812401160001
Vishwas Acharya

Page No.: 1
Date: 12/5/21

Q1 Write about Cryptographic Hash Functions in detail.

Ans - Hash functions are extremely useful and appear in almost all information security applications.
- A hash functions is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of arbitary length but output is always of fixed length.
- Values returend by a hash function are called message digest or simply hash values.

- Figure :-



- **Features :-**

↳ **Fixed Length Output (Hash Value)**
- Hash function converts data of arbitrary length to a fixed length. This process is often referred to as hasing the data.
- In general, the hash is much smaller than the input data, hence hash functions are sometimes called compression functions
- Since a hash is a smaller representation of a larger data, it is also referred to as a digest.

↳ **Efficiency of Operation**
- Generally for any hash function h with input x, computation of h(x) is a fast operation.
- Computation hash functions are much faster than a symmetric encryption.

- **Properties :-**

↳ Pre-Image Resistance
↳ Second Pre-Image Resistance
↳ Collision Resistance

- **Applications :-**

- There are two direct applications of hash function based on its cryptographic properties

↳ Password Storage
  ↳ Hash functions provide protection to password storage

↳ Data Integrity Check
  ↳ It checks the most common application of the hash functions.

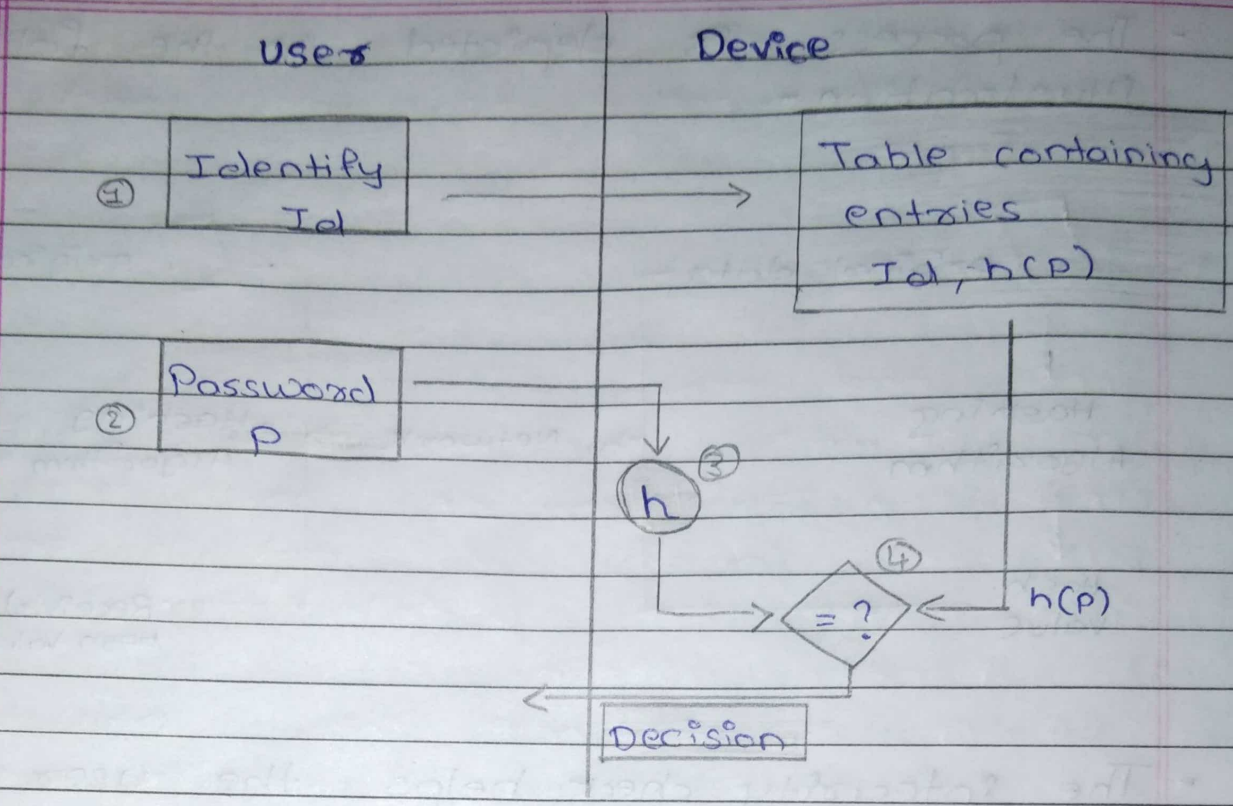
2) Explain Hash functions applications in detail.

Ans - There are two direct applications of hash fuction based on its cryptographic properties.

- Password Storage

↳ Hash functions provide protection to password storage.

- Instead of storing password in clear, mostly all logon processes store the hash values of passwords in the file.
- The Password file consists of a table of pairs which are in the form (user id, h(p)).
- The process of logon is depicted in the following illustration -

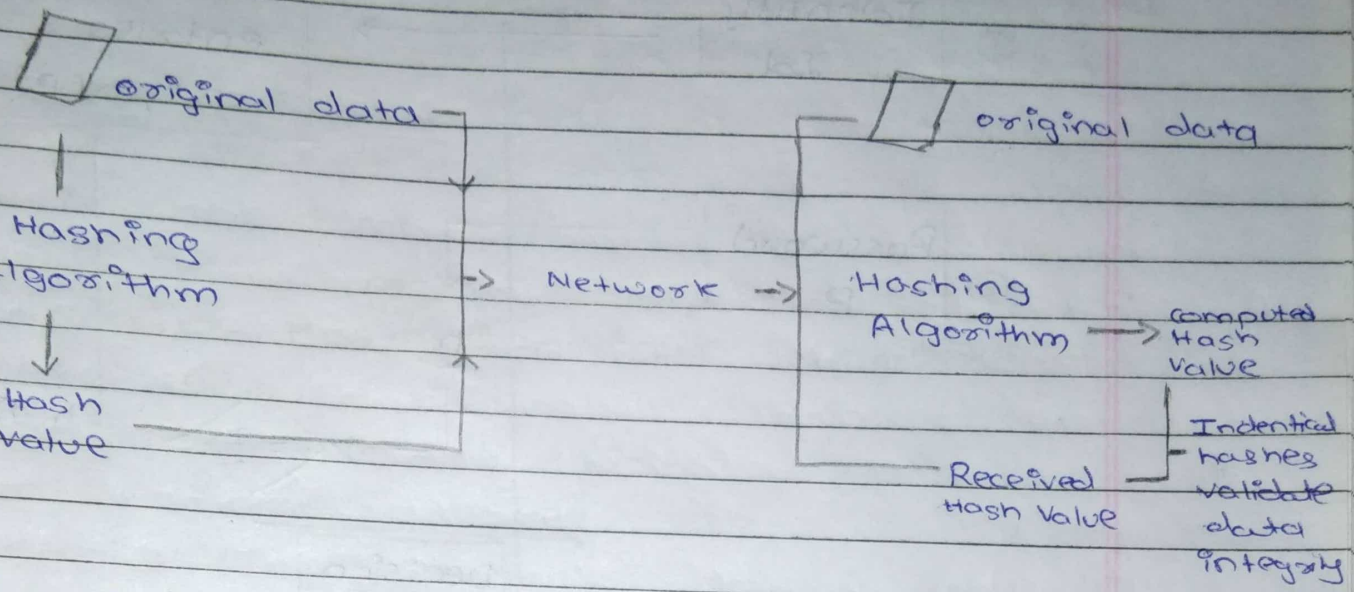


- An intruder can only see the hashes of passwords, even if he accessed the password.
- He can neither logon using hash nor can he derive the password from hash value since a hash function possesses the property of pre-image resistance.

- **Data Integrity Check**

↳ Data Integrity check is a most common application of the hash functions.
↳ It is used to generate the checksums on data files.
↳ This application provides assurance to the user about correctness of the data.

- The process is depicted in the following illustration -

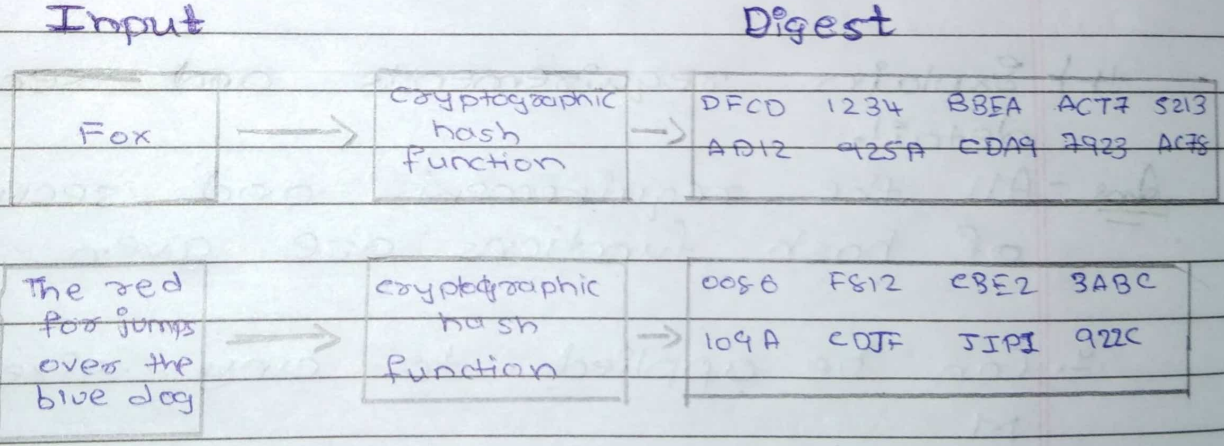


- The integrity check helps the user to detect any changes made ~~th~~ to original file.
- It however, does not provide any assurance about originality.
- The attacker, instead of modifying file data, can change the entire file and compute all together new hash and send to the receiver.
- This integrity check application is useful only if the user is sure about the originality of file.

3) Explain SHA algorithm in detail.

Ans - A Secure Hash Algorithm is actually a set of algorithms developed by the National Institutes of standars and Technology (NIST) and other government and private parties. These secure encryption or "file check" functions have arisen have arisen to meet some of the top cybersecurity challengs of the 21st century, as a number of public servic groups work with federal government agencies to provide better online security standards for organizations and the pubic

- Figure:



- Characteristics :

- Cryptographic hash functions are utilized in order to keep data secured by providing three fundamental of characteristes which

is consist of : pre-image resistance, second pre-image resistance, and collision resistance.

- **Types of SHA**

- There are many types of SHA, some of those family are SHA-0, SHA-1, SHA-2, SHA-3 and SHA-256, each of which was succeded increasingly stronger encryption and still being updated in response to hacker attack.
- SHA-0, for example, this is now obsolete due to widely exposed to the world.
- Because there are too many types of SHA algorithms, in this article I will just point out few of those types

4) Explain requirements and security in detail.

Ans - All the requirements and security of hash functions are given further.

1. Can be applied to any sized message M
2. Produces fixed-length output h
3. It is easy to compute $h = H(M)$ for any message M.
4. Given hash value h is infeasible to find y such that $(H(y) = h)$
   - one way property.

5. For given block x, it is computational infeasible to find $y \neq x$ with $H(y) = H(x)$
   - weak collision resistance
6. It is computationally infeasible to find meessages m1 and m2 with $H(m1) = H(m2)$
   - strong collision resistance.