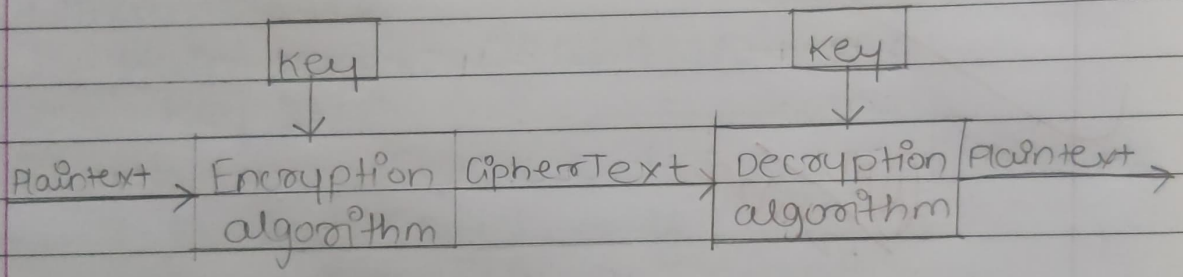
M T W T F S S
Page No.: YOUVA
Date: 10/11/22

Assignment no.3

Q.1) Explain Symmetric key encryption & assymetric key encryption with diagram.

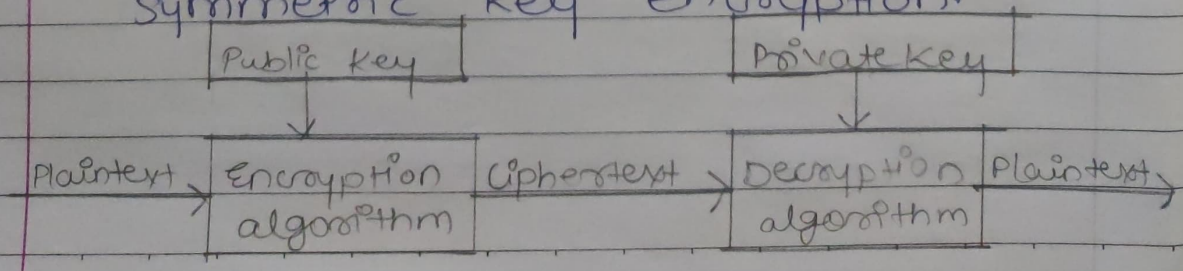
→ a) Symmetric key encryption :-

- It involves usage of one secret key which helps in securing the contents of the message.
- When user uses same key as an encryption and decryption process is called as symmetric key encryption.
- The strength of symmetric key encryption depends upon number of key bits.
- It is relatively faster than assymetric key encryption.



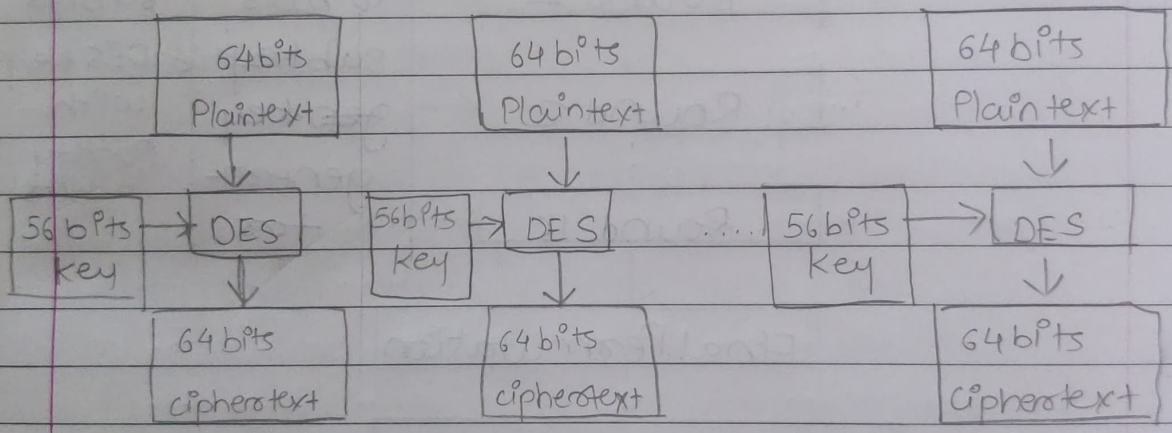
b) ~~Assymetric~~ Assymetric Key encryption :-

- It is also known as public key encryption because it involves usage of a public key along with secret key.
- When a user uses different keys as encryption and decryption process is called as assymetric key encryption.
- It is very slow compared to symmetric key encryption.



Q.2) Describe DES algorithm with diagram.

→ • DES stands for Data Encryption Standard Algorithm.
• DES is a block cipher and encrypts data in blocks of size of 64 bits each.
• 64 bits of plain text goes as the input to DES which produces 64 bits of cipher text.
• The same algorithms and keys are used for encryption and decryption with minor differences.
• The key length is 56 bits.



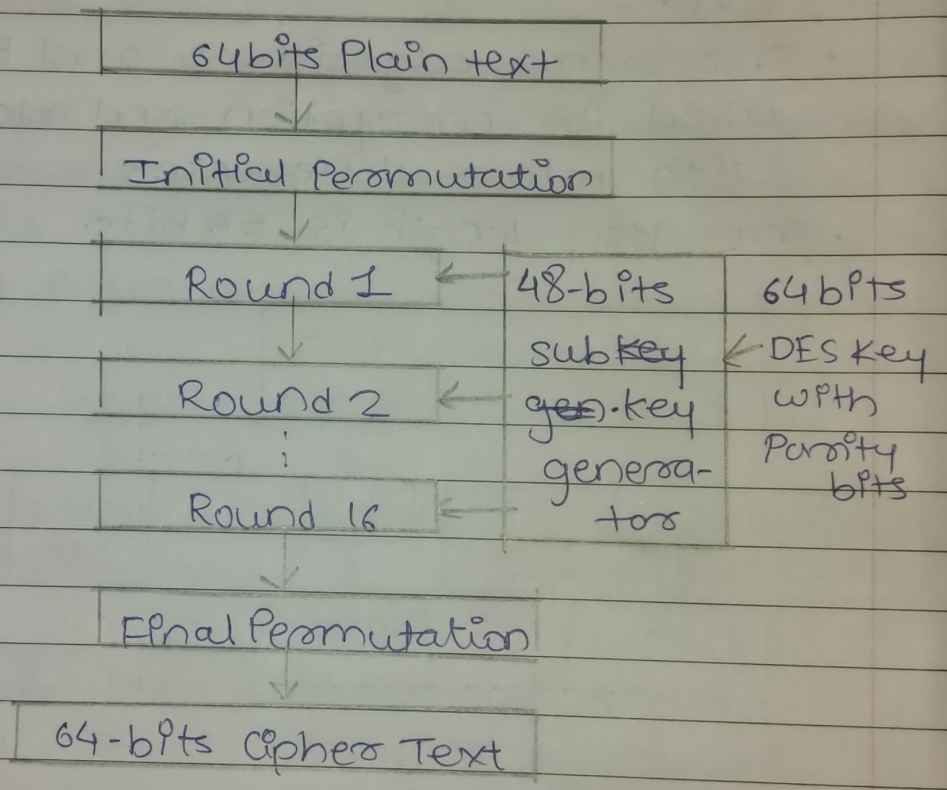
• Steps of DES algorithm:-

a) In the first step, the 64-bits plain text is handed over to an initial permutation function.

b) Initial permutation is performed on plain text.

c) The initial permutation produces two resultant permuted block say left plain text (LPT) and right plain text (RPT).

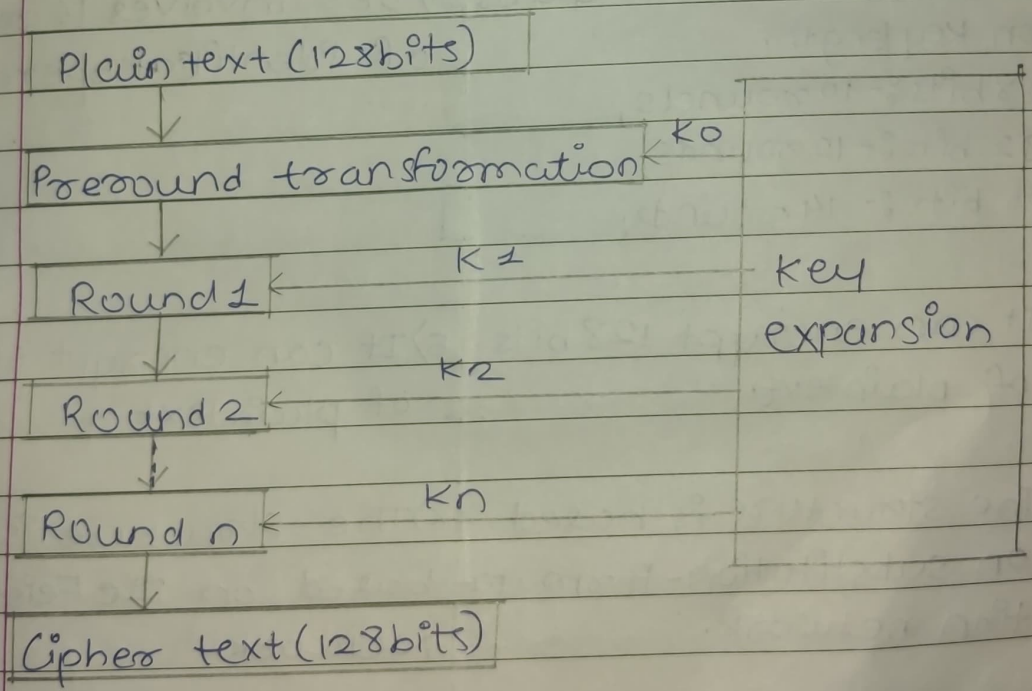
d) Each LPT and RPT goes through 16 rounds of encryption process.
e) In the end, LPT and RPT are rejoint and a final permutation is performed on the combined block.
f) The result of this process produced 64-bit cipher text.



Q.4) Describe AES algorithm with diagram
→ • AES stands for Advanced Encryption Standard.
• It is a specification for the encryption of electronic data established by US National Institute of standard and technology (NIST) in 2001.
• AES is widely used today as it is a much stronger than DES. DES being

harder to implement.

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- In DES, encrypts data in block of 128 bits each. It means it takes 128 bits as input and output 128 bits of encrypted cipher text as a output.
- The number of rounds depend on the key length as follows:-
  a) 128 bit key:- 10 rounds.
  b) 192 bit key:- 12 rounds.
  c) 256 bits key:- 14 rounds.



Q.5) Differentiate between DES and AES.

→

AES	DES
1) AES stands for Advanced Encryption Standard	1) DES stands for Data Encryption Standard.
2) It is byte oriented.	2) It is bit oriented.
3) Key length can be 128-bits, 192-bits and 256-bits.	3) Key length is 56 bits.
4) Number of rounds depends on key length. 128 bits :- 10 rounds, 192 bits :- 12 rounds, 256 bits :- 14 rounds.	4) DES involves 16 rounds of identical operation.
3) It can encrypt 128 bits of plaintext.	5) It can encrypt 64 bits of plaintext.
6) The structure is based on substitution-Permutation network.	6) The structure is based on Feistel Network.

Q.6) Explain RSA algorithm in details?

→ • RSA stands for RIvest - Shamir - Adelman.
• RSA is an ~~assymm~~ assymetric cryptographic algorithm.
• Assymetric means it works on two different keys i.e. public key and private key.
• As the name describes that the public key is given to everyone and private key is kept private.
• Example of Assymetric cryptography:-

1) A client sends its public key to the server and requests for some data.
2) The server encrypts the data using client's public key and sends the encrypted data.
3) Client receives this data and decrypts it.

Q.7) Define the following terms:-

1) Digital Signature:-
It is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

2) Digital Certificate:-
Digital certificate is issued by a trusted thirdparty which proves sender's identity to the receiver and receiver's

identity to the sender.

It contains name of certificate holder, serial number which is used to uniquely identify certificate, Expiration Dates, copy of certificate holder's public key, Digital signature of certificate issuing authority.

3) Cryptographic Hash function :-

It is a special class of Hash function that has certain properties which make it suitable for use in cryptography.

It is a mathematical algorithm that maps data of ~~arbitrary size~~ arbitrary size to a bit string of a fix size (a hash function) which is designed to be a oneway function that is a function which is infeasible to invert.

Q.8) Explain Diffie Helman Scheme Key Exchange algorithm.

→ • It is a method of securely exchanging cryptographic key over a public channel and was one of the first public key protocol as originally conceptualized named Diffie-Helman Scheme.

• It is a public key exchange implemented within the field of cryptography.

• This algorithm is used to establish a shared secret key that can be used for secure communication while exchanging data over

public network.

Alice	Bob
Public key available = P, G	Public key available = P, G
private key selected = a	private key selected = b.
Key generated = $x = G^a \bmod P$	Key generated = $Y = G^b \bmod P$
Exchange of generated keys takes place	
Key received = Y.	Key received = x
Generated secret key $K_a = Y^a \bmod P$.	Generated secret key $K_b = X^b \bmod P$.

Algebrically it can be shown that,

$$K_a = K_b$$

Users now has symmetric key to encrypt :-

Step 1 :- Alice and Bob get public numbers,
P = 23, G = 9.

Step 2 :- Alice ~~and~~ selected private key, a = 4.
Bob selected private key, b = 3.

Step 3:- Alice and Bob compute public values.

Alice:-	Bob:-
$X = G^a \bmod P$	~~Bob:~~ $Y = G^b \bmod P$
$X = 9^4 \% 23$	$Y = 9^3 \% 23$
$X = 6561 \% 23$	$Y = 729 \% 23$
$X = 6$ [Remainder]	$Y = 16$

Step 4:- Alice and Bob exchange public numbers.
Step 5:- Alice receives public key, $y = 16$ & Bob receives public key, $x = 6$.

Step 6:- Alice & Bob compute symmetric keys

Alice:- $K_a = Y^a \bmod P$	Bob:- $K_b = X^b \bmod P$
$= 16^4 \% 23$	$= 6^3 \% 23$
$= 65536 \% 23$	$= 216 \% 23$
$K_a = 9$	$K_b = 9$.

$$K_a = K_b$$

Step 7:- 9 is the secret key.

Q.9) What are the advantages of Data Encryption process?

→ Advantages of Data Encryption process are as follows:-

a) Supports Compliance:- Encryption is explicitly needed by some regulations and market standards. It is having strong encryption in place can provide

demonstrate to auditors that sensitive information is well secured by organization.

b) Provides Privacy:-

Data Encryption is not only beneficial for organization or military, but normal computer users can also use it to save sensitive data like Bank details, Account details, etc. without proper Encryption, anyone who can access device will be capable to view and copy it.

c) Provides security at All Times:- There are several tools to password protect folder / information that someone it can choose, but it is only way to secure information. This is possible because without proper decryption of information, noone can use it.

d) Protects data in Cloud storage:- When data is stored in the public cloud, it can be exposed to a much broader range of threats. Encrypting information in cloud storage by default supported a layer of security against all threats.