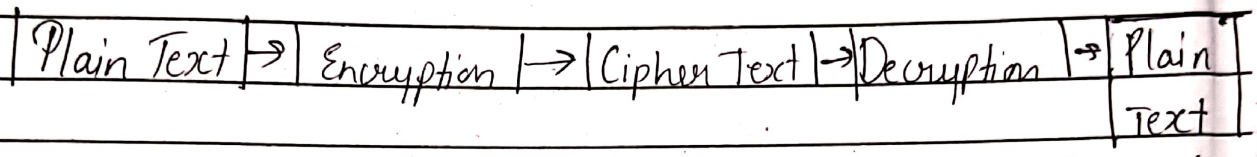
Q-1 Draw & explain cryptography system.

Cryptography is a technique of securing communication by converting plain text into cipher text. In this technique we use codes so that only those persons can access information who have actual access of it. It prevent unauthourized access. The prefix "Crypt" means "hidden" & "graphy" suffix means writing.



Readable format.

* Cryptography use by two methods

1) Symmetric key
- It is an encryption system where the senders & receivers of a message use single common key to encrypt & decrypt message.
- It is simple, faster but the problem is that the sender & receiver have to some exchange keys securly.
- The most popular symmetric key is data encryption system & advsanced encryption system.

2) Assymmetric key.
It is pair of key used to encrypt & decrypt information. A receiver public key used for encryption & private key for decryption the most popular assymmetric key algorithm in RSA algorithm.

Feature of cryptography
1) Confidentiality
2) Integrity
3) Non-repudiation
4) Authentication
5) Inter-operability
6) Adaptibility

Applications
1) Computer Password
2) Digital currencies
3) Secure web browsing
4) Electronic signature
5) End to end internet encryption.

Q-2 Find GCD of if 2740 & 1760.

i) 2740 & 1760

$a = 2740$, $b = 1760$

$a = bq + r$

$2740 = 1760(1) + 980$

again:

$a = 1760$ & $b = 980$

$1760 = 980(1) + 780$

Similarly

$980 = 780(1) + 200$

$780 = 200(3) + 180$

$200 = 180(1) + 20$

$180 = 20(9) + 0$ $\quad r = 0$.

$\therefore$ 20 is GCD of (2740, 1760)

2) 48 & 320

$A = bq + r$

$320 = 48(6) + 32$

$48 = 32(1) + 16$

$32 = 16(2) + 0 \qquad r = 0$

∴ 16 is GCD of (48 & 320

3-3 Find result of following operation

→ i) 28 mod 7

$28 \div 7 = 4$ —①

multiply the quotient (4) by the divisor 7

$4 \times 7 = 28$

Subtract the result from step 2 from orignal number.

$28 - 28 = 0$

∴ 28 mod 7 = 0

2) 140 mod 10

i) $140 \div 10 = 14$

ii) Multiply the quotient (14) by divisor.

∴ $10 * 14 = 140$

iii) Subtract the result from step 2. from orignal no.

$140 - 140 = 0$

∴ 140 mod 10 = 0.

Q.4 Explain shannon theory (diffusion & cufusion)

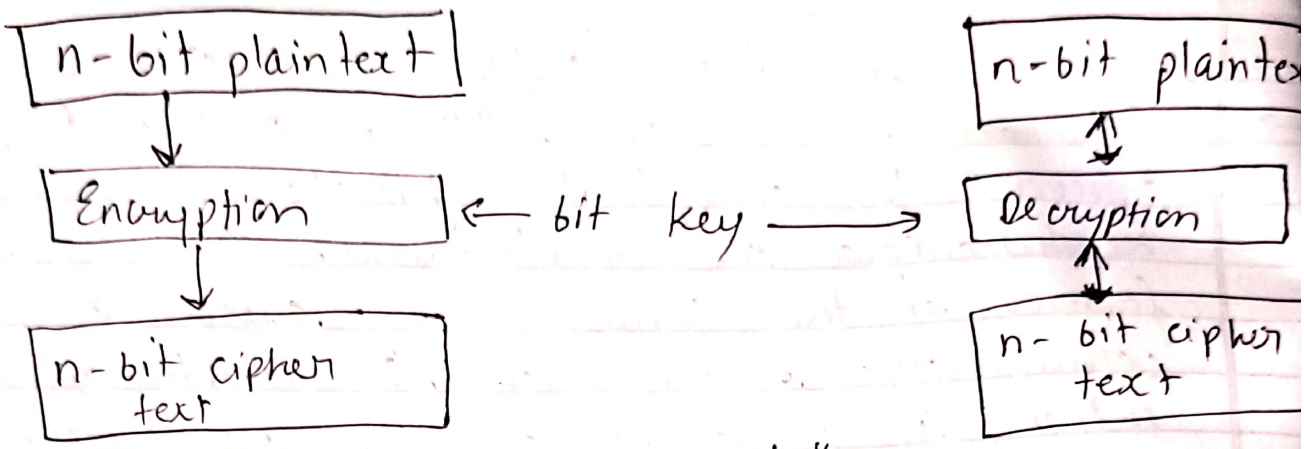
→ Shannon known as father of modern cryptography introuced the concept of information theory, which revolutionized the cryptography. Shannon theory focuses on the fundamental aspects of secure communication & encryption. In cryptography. entropy is crucial for generation secure keys & ensuring unpredictibility of encrypted data. Shannon also introduced the concepts of diffusion & confusion. which are essential principle in designing secure encryption algorithm.

- Diffusion of confusion work together to enhance the security of a cryptography system. Diffusion spread the influence of plain text across the cipher text. while confusion obsurese relationship between the key & ciphertext making it decrypt the menage. without the proper key.

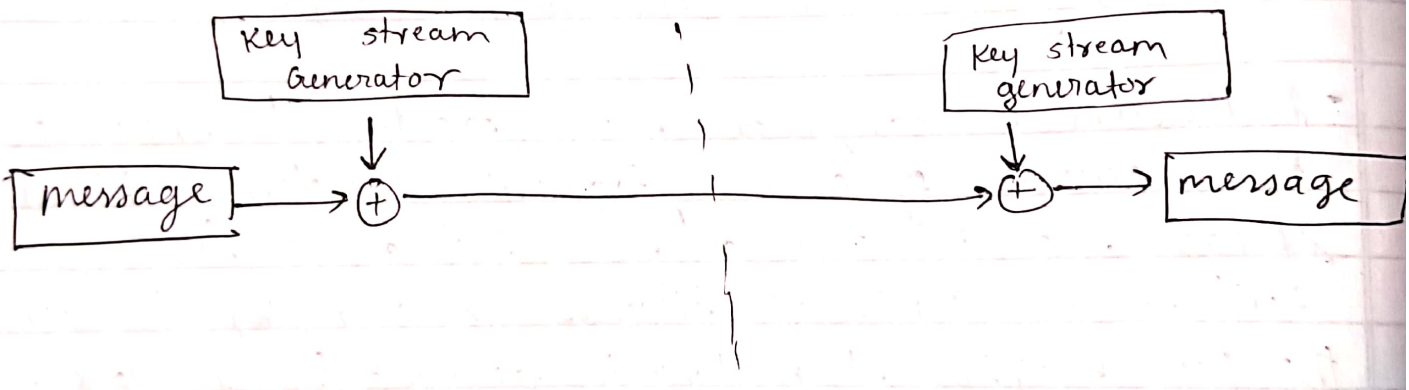
Q-5 Explain block cipher & stream cipher in details.

Block cipher :- conversion of plain text of ciphes text is done by taking its block of a time. A block cipher is an encryption algo that encrypts data in fixed size block it take a block of plain text & key as input & produces a block of cipher text size of.

- The encryption process involves multiple rounds of



A modern block cipher



Stream cipher

of substitution & permutation operation based on the key each block is processed independently.

- Block cipher are designed to be seeure against various attacks like differential & linear crypto-analysis.
- If there is some data it's ciphertext should to be similar so it's like breaking a message into blocks, putting each block through a coding machine & the combining all the coded blocks to form the encrypted message.
- A block cipher encrypt data in fixed size blocks typically 64 or 128 bits at a time.

Ex- AES DES.

In block ciphers reverse encrypted text is hard & it is slow as compared to a stream cipher.

- Operates on fixed length block of data.

Stream Cipher:

- A stream cipher encrypt data one bit or byte at a time rather than in fixed size blocks. A stream cipher is an encryption algorithm that encrypt data bit by bit or byte by byte. Often used for real time encryption or continuous data stream.
- It generates a continues stream of keying material that is combined with plaintext bit by bit to produce cipher text.

• Stream cipher are designed to be efficient for encryption large volume of data in real time but can be vulnerable to certain types of attacks if not implemented correctly.

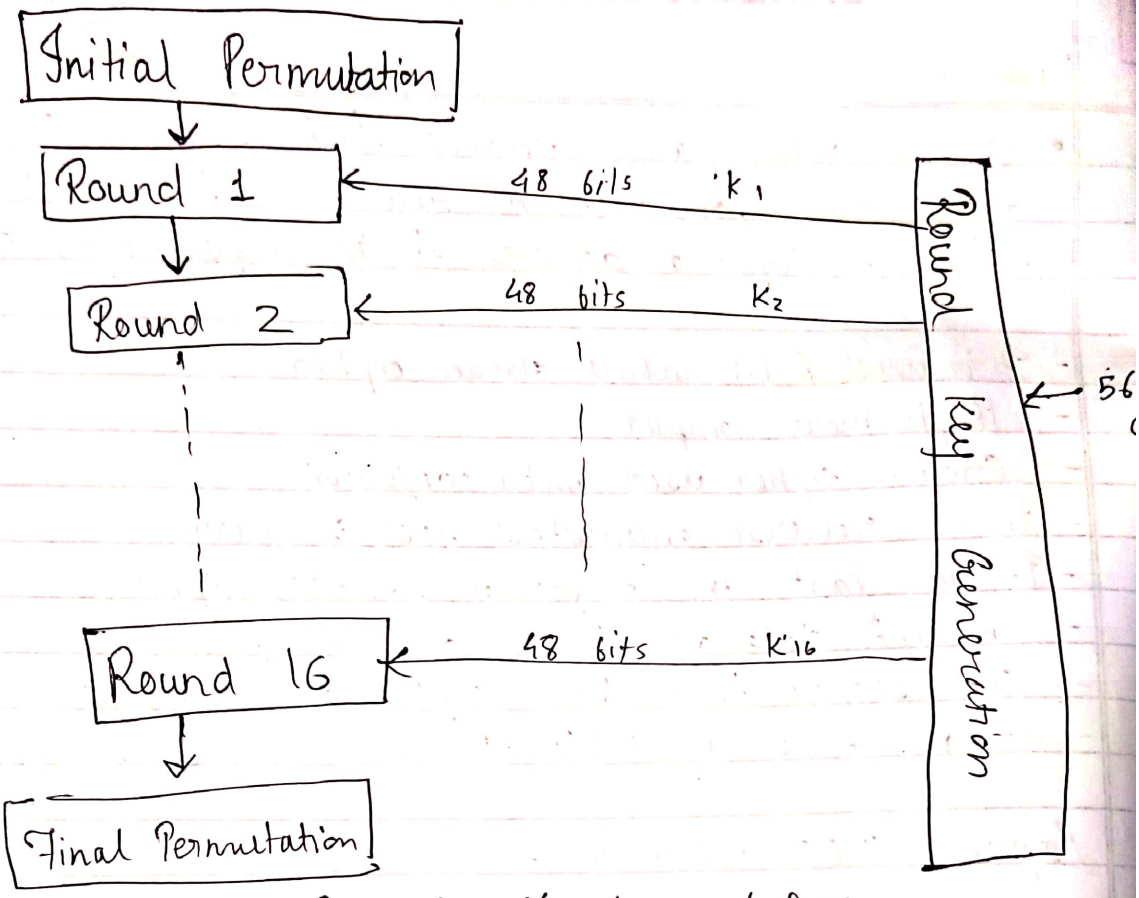
- It is used 8-bit while stream cipher
- It is more complex
- Stream cipher used only confusion
- In it reverse encrypted text is easy
- It is fast in comparsion to block cipher
- Encrypt data one bit at a time.
- less secure that block cipher when same
- key is used multiple time.

Q-6 Explain DES cipher & its reverse

⇒ DES stands for data encryption standard. It is a symmetric key block cipher. DES is an important implementation of a fiestal cipher. it uses 16 rounds. feistal structure. The block size is 64 bit. Through key length is 64 bit DES has an effective key length - 56 bit since 8 of the 64 bit of key are not used by encryption algorithm.

* General structure of DES:

① Initial Permutation: 64 bit plain text is permutated according to a fixed table to rearrange the bits. It shuffle to I/P.



General Structure of DES.

Input
↓
32 bit
↓
expansion p box
xor ⊕ ← 48 bit key, 48 bits
↓
| S | S | S | S | S |
↓
straight
↓ ← 32 bit
out.

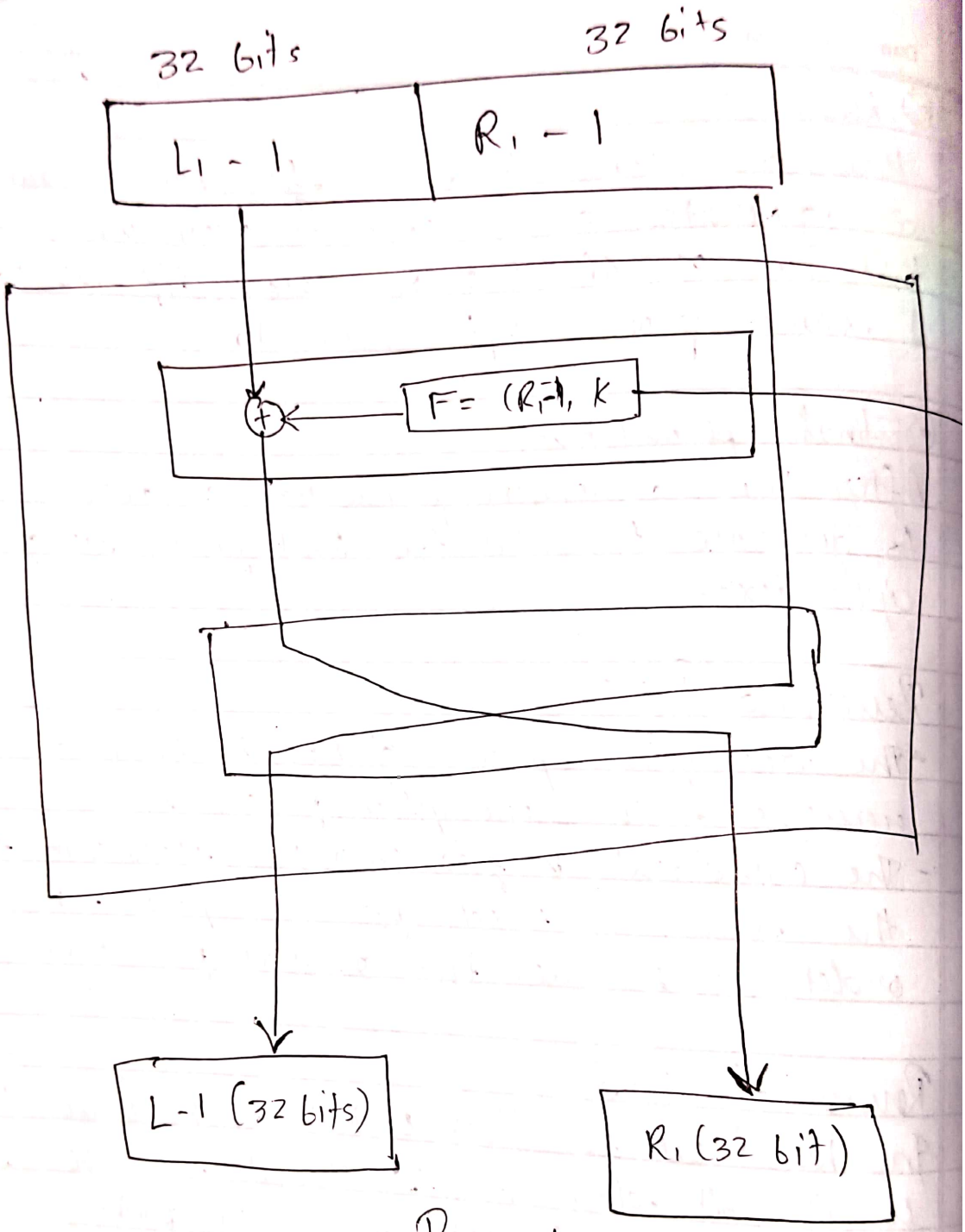
② Rounds :
Here are total 16 rounds. for each round generat - or generates one separate key which is of 48 bit that key of 48 bit & permutated i/p goes to round 1, same process upto round 16.

③ Final permutation
After the 16 rounds permutation is applied of data to generate the cipher text. And finally we get 64 bit cipher text.

Reversing DES
→ The decryption proces of DES is essentially the reverse of the encryption process.
- The cipher text is feed into DES algorithm along with the same key used for encryption. in reverse order to recover the orignal plaintext.

Round of DES
In DES we use block cipher so here we have divided by 64 bit data into 32-32 bit per block.
① left block (L-1) & ② Right block (R-1)

In right block there has an DES function in which comes with 48 bit key. these DES function convert 48 bit key into 32 bit key generated by function XOR with each other then that o/p goes to right hand block i.e (32 bit) & right hand ~~in DES~~ goes to left (.



Round in DES.

Q-7 Explain Key generation in DES.

⟹ In DES initial key always of 64 bit. It passes to the parity drop. In priority drop remove some bit which is in sequence of 8, 16, 32, 24, 48, 56, 64 - total 8 bit remove from initial key & get 56 bits.

- 56 bits divided into 28 bit in these both shift left operation perform on both side if round - 1, 2, 9, & 16 is going then 1 bit shift to left. Otherwise 2 bit will shift at left. so we get o/p of 28 bit total 56.

- Compression p box :-
56 bit o/p which get from shifting in get compress some process as we have done in parity drop each 8 bit will remove from 56 bit i.e 8, 16, 24, 32, 40, 48, 56, 64 so we get o/p of 48 bits. that 48 bits is nothing but our key - 1 same process happen for each key generati

- Original input convert into 48 bit by expanding or repeating data in I/p so expansion p box has of 48 bits. now 48 bit key & expansion p box 48 bits data get XOR. so it o/p will 48 bit. these 48 bit data gets to 'S' box.

Page No.:

Q.8 Draw & explain structure of each round in AES & encryption side.

⇒ It is a symmetric key block cipher & fixed block size is 128 bits. i.e 16 bytes = 4 words As in DES was 16 round same

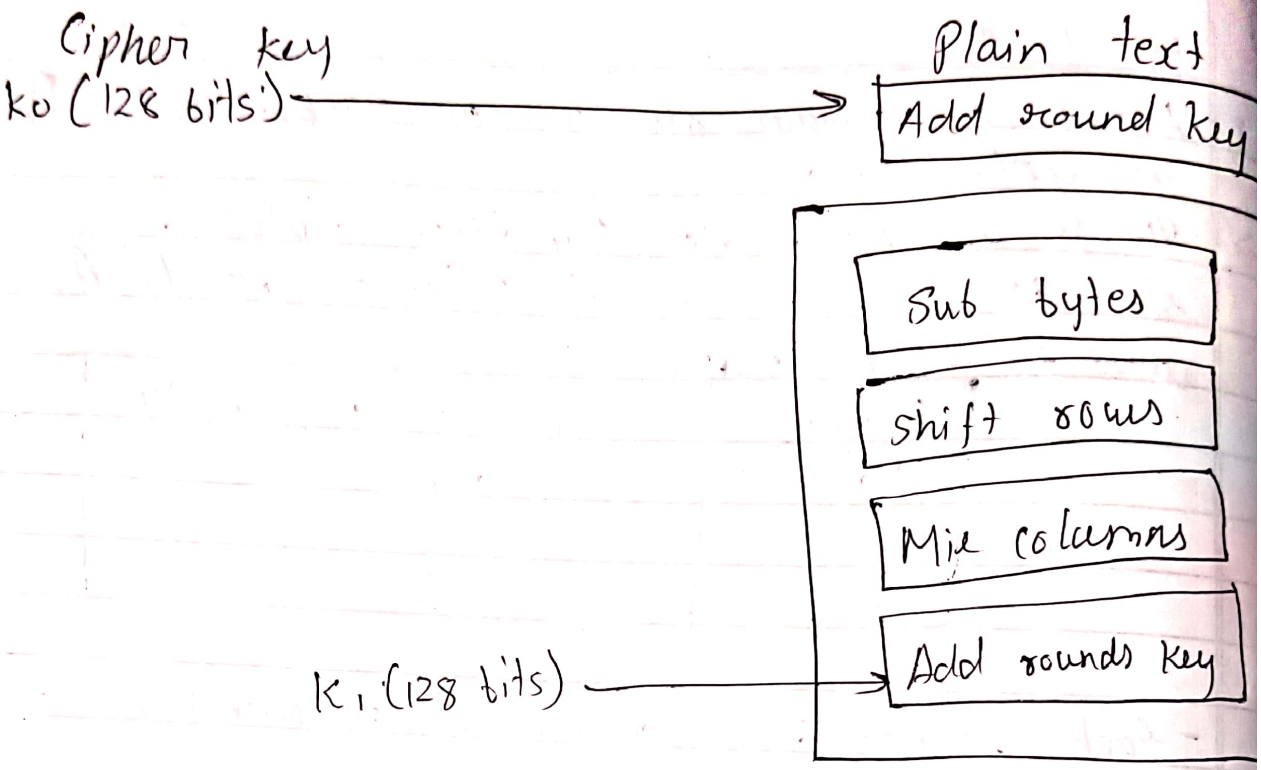
Round	No. of bits in key
10	128
12	192
14	256

- Each round consists of multiple operation that transform the data.
- AES is widely used today as it is much stronger than DES.
- AES is efficient & flexible support different key sizes.

Encryption:
AES consider each block as a 16 byte. Gradient column major arrangenent

b0	b4	b8	b12
b1	b5	b9	b13
b2	b6	b10	b14
b3	b7	b11	b15

* Each round comprises of 4 steps
1. Sub bytes
2. Shift rows
3. Mix column
4. Add round key


Cipher key
k0 (128 bits)
Plain text
Add round key
Sub bytes
shift rows
Mix columns
Add rounds key
k1 (128 bits)

① Sub bytes:
The 16 i/p bytes are substituded by looking up a fixed table given in design the result is in a matrix of four rows & four columns.

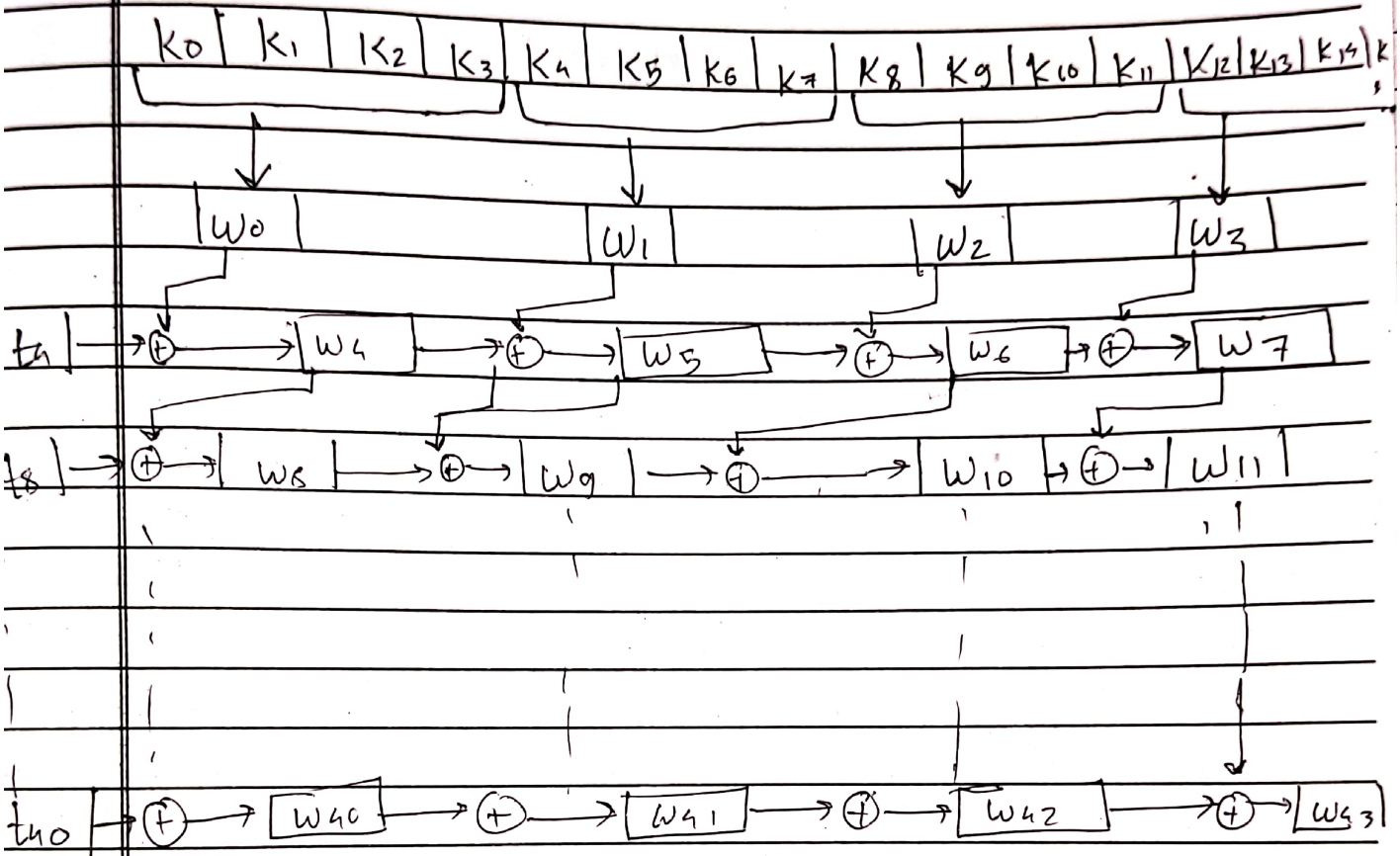
② Shift rows
Each of 4 rows of matrix is shift to left any entities fall off are rein serted on right side of row. shifted row is carried out as follow.
- first row is not shifted
- Second row is shifted one position to left
- Third row is shifted two position to left
- Fourth row is shifted 3 position to left.

③ Mix columns
- Each columns of 4 bytes is how transformed using a special mathematics function. This function takes as i/p the 4 bytes of one column & o/p 4 completely new bytes, which replace the orignal columns

④ Add round key
They 16 bytes of matrix are now considered as 28 bits & are XOR to 128 bit of round key. If this is the last round then o/p is cipher text. Otherwise, the resulting 128 bit are interpreted as 16 bytes & use begin on other similar round.

-9 Draw expansion of key in AES-128.

Cipher key



Assignment 2

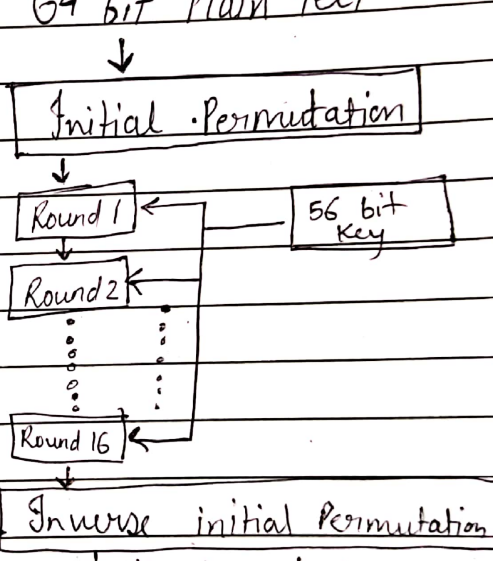
1 DES draw & explain single round procedure.

DES - Data encryption standard is a block cipher with a 56-bit key length that has played a significant role in data security. And data in blocks of size of 64 bits each.

- It is symmetric cipher. 64 bit plaintext block, In encrypt the data in block of size 64 bit each.
- 16 round each round is feister round.

*Steps for DES :-

① Initial permutation
② Swapping / left-right swap
③ Final permutation



- Input : 64-bit data
- Feistal function applied to the right half (R), involving expansion, XOR with round subkey, S-box substitution & permutation.
- XOR the result with left half (L).
- Swap the left & right halves for the next round.
- This process is repeated for 16 rounds, each with a different subkey, to create the final encrypted output.

Explain key generation of DES.

- Initial 64-bit key :- The 64 bit key is reduced to a 56-bit key by ignoring the parity bits.

- PC-1 (permutation choice 1) :-

The 56-bit key is divided into two 28-bit halves C_0 and D_0 using a specific permutation.

- Shifting :- Each round involves shifting the two halves C_i & D_i left by 1 or 2 bits.

- PC-2 (permutation choice 2) :-

After each shift, a 48-bit subkey is generated by applying a second permutation to the concatenated halves.

- This process repeats for 16 rounds, producing 16 subkeys of 48 bits each; used in the corresponding rounds of DES encryption.

- Example :- Assuming we start with 56 bit key, the process look like :-

Initial 56 bit key, for each round :-

- Perform a left circular shift
- Apply PC-2 to create a 48 bit subkey
- Repeat for all 16 rounds.

1.3 AES encryption cipher. Draw & explain.

- It is symmetric key. block cipher. & fixed block size is 128 bits.
  i.e. 16 bytes = 4 words.

- As in DES was 16 round same may:

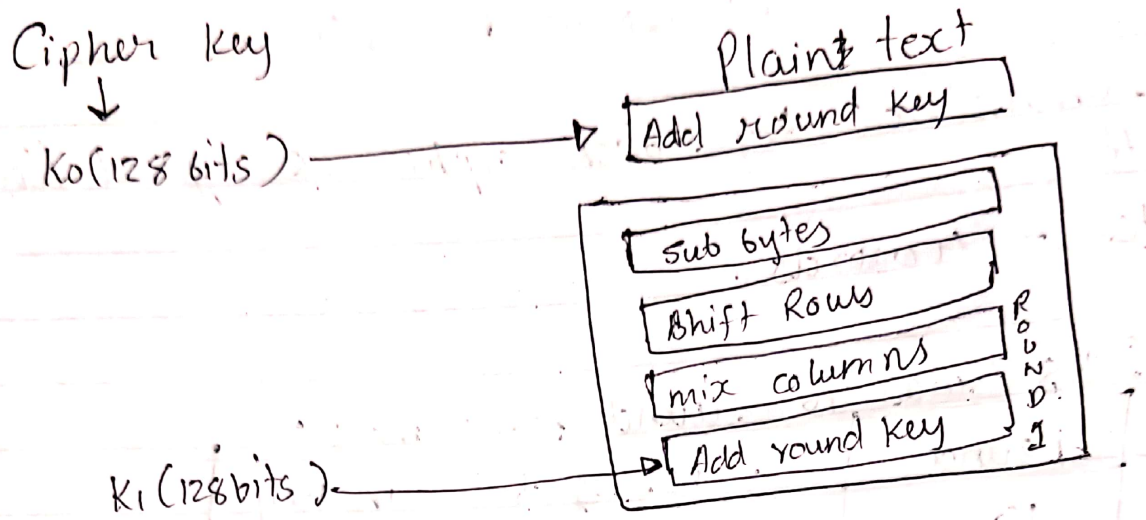
Round	no. of bits in key
10	128
12	192
14	256

- AES is widely used today as it is much stronger than DES.

- Encryption :-
  AES considers each block as a 16 byte. grid in a column-major arrangement each round comprises of 4 steps
  ① Subbytes ② Shiftrows
  ③ mixcolumns ④ Add Round key

- Subbytes :- The 16 i/p bytes are substituted by looking up a fixed table given in design. The result is in a matrix of four rows & four columns.

- Shiftrows:
  Each of 4 rows of matrix is shifted to left. Any entries "fall off" are re-inserted on right side


Cipher key
K0 (128 bits)
Plain text
Add round key
Sub bytes
Shift Rows
mix columns
Add round key
ROUND 1
K1 (128 bits)

of row. Shift is carried out as follows.

- First row is shifted one position to left.
- Second row is shifted one position to left.
- Third row is shifted two position to left.
- Four row is shifted 3 position to left.
- The result is a new matrix consisting of same 16 bytes but shifted with respect to each other.

Mix column:

Each columns of 4 bytes is now transformed using a special math function. This function takes as i/p the 4 bytes of one column & o/p 4 completely new bytes which replace the orignal columns.

SHREEYASH PRATISHTHAN'S

Shreeyash Technical Campus

SHREEYASH COLLEGE OF ENGINEERING & TECHNOLOGY, AURANGABAD

Department of Electronics and Computer Engineering

(202 -202)

Class:

Subject Name:

Subject Code:

Assignment No.	
Title	
Date of Performance	
Date of Submission	
Roll No.	
Name of Student	

Evaluation:

Sr.No.	Rubric	Maximum Marks	Marks Obtained
1	On time Submission & Completion	08	
2	Content & Organization	02	
	Total	10	

Signature of Teacher:

-1 Explain MAC (message authentication code).

→ The transfer of message between two people also faces other external problems like noise, which may alter the orignal message constructed by the sender.

To ensure that the message is not altered. there is a method MAC. Here MAC sender & receiver share some key where sender generate a fixed size output called cryptonic graphic checksum or message authentication code & appends it to orignal message. On receiver side, receiver also generate the code & compares it with what he/she received thus ensuring the orginality of the menage.

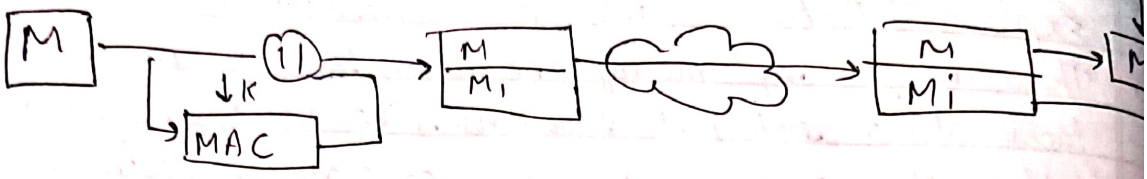
- There are different types of model of MAC

① MAC without encryption:
The model can provide authentication number confidentiality as anyone can see menage.

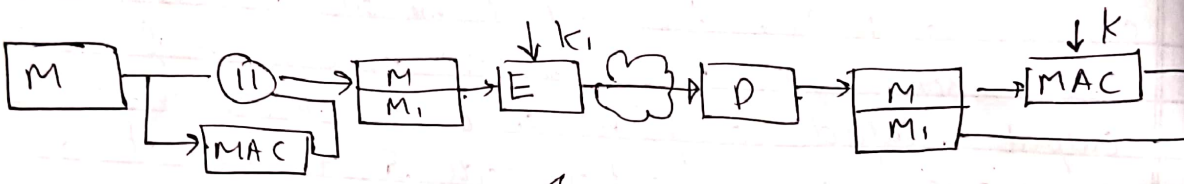
② Internal Error code - Sender encrypts the content before sending it through network for confidentiality. Thus this model provides confidentiality as well as authentication.

③ External error code
We apply MAC on the encrypted message 'c' & come it with received MAC value on receiver end.
④ Decrypt 'c' if they both are same, else we simply discard the content received.

Page No.:



MAC without encrypt



Internal Error code.

Q-2 Explain any two attacks on RSA.

Ans Two common attacks on RSA are the "Factorization attack" where an attacker tries to directly factor the public modules to derive the private key & the "old channel attack". which exploits information leaked during the encryption / decryption process, like timing variations, to gradually reveal the private key details.

- Factorization Details.

The security of RSA relies on the difficulty of factoring large ~~& randomly~~ numbers, particularly when "p" & "q" are large & randomly chosen prime numbers.

- Breaking RSA:

Successfully factoring "D" effectively breaks the RSA encryption scheme as it allows the attacker to calculate the private key "d".

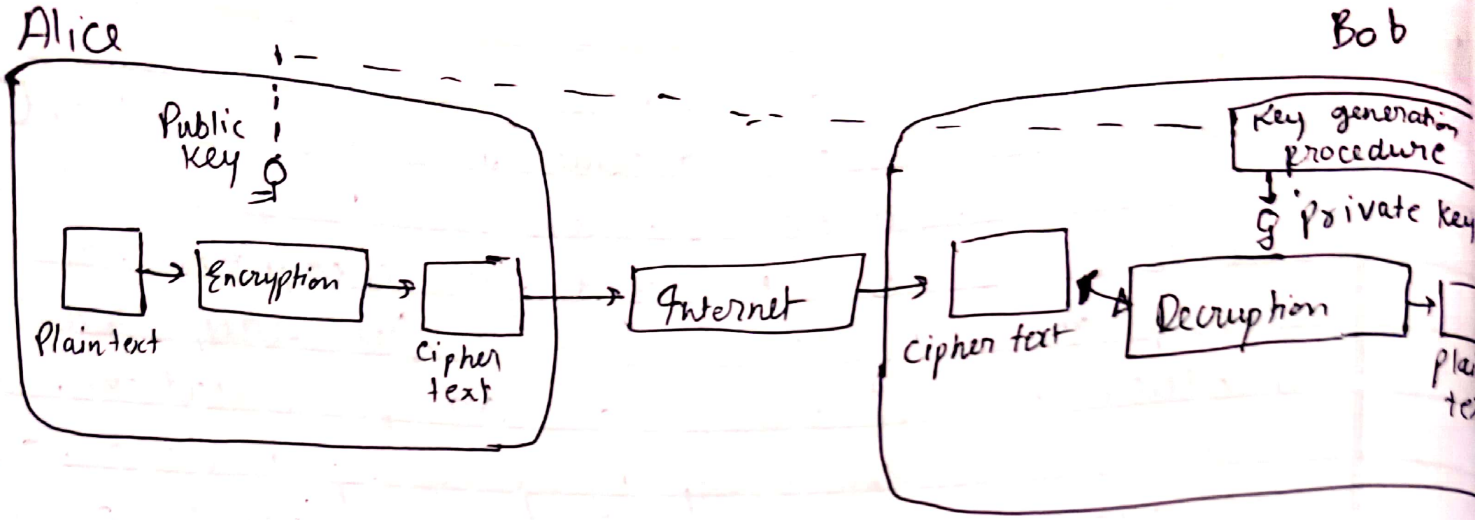
- While factorization attack ~~the~~ one considered the most significant threat, other attacks like "low exponent attacks" or timing attacks! can also exploit vulnerabilities in RSA implementation.

Q-3 Draw & explain assymetric key cipher

Assymetric key cryptography uses mathematical functions to transform plaintext & ciphertext represented as numbers for encryption & decryption, while symmetric key cryptography involves symbol substitution or permutation. In assymmetric-key cryptography, plaintext & ciphertext are treated as integers, regularity encoding & decoding processes for encryption & decrypti

- Characteristics of assymmetric key cryptography:-
- Security responsibility:-
- In assymmetric cryptography, the burden or security primarily falls on the receiver. like Bob. Bob must generate both a private & public key. with the public key distributed to community.
- Key Management.
- Bob needs only one private key to receive message from anyone in the community.
- Alice on the other hand, needs multiple public keys one for each entity one-communicate with. This means alice requires a collection of public key for effective communication.

- Key Components
- Plaintext • Encryption algorithm • Public & private key
- ciphertext • Decryption algorithm.



Assymmetric - key cryptosystem:

SHREEYASH PRATISHTHAN'S

Shreeyash Technical Campus

SHREEYASH COLLEGE OF ENGINEERING & TECHNOLOGY, AURANGABAD

Department of Electronics and Computer Engineering

(202 -202)

Class:

Subject Name:

Subject Code:

Assignment No.	
Title	
Date of Performance	
Date of Submission	
Roll No.	
Name of Student	

Evaluation:

Sr.No.	Rubric	Maximum Marks	Marks Obtained
1	On time Submission & Completion	08	
2	Content & Organization	02	
	Total	10	

Signature of Teacher: