161240116001
Vishwas Acharya

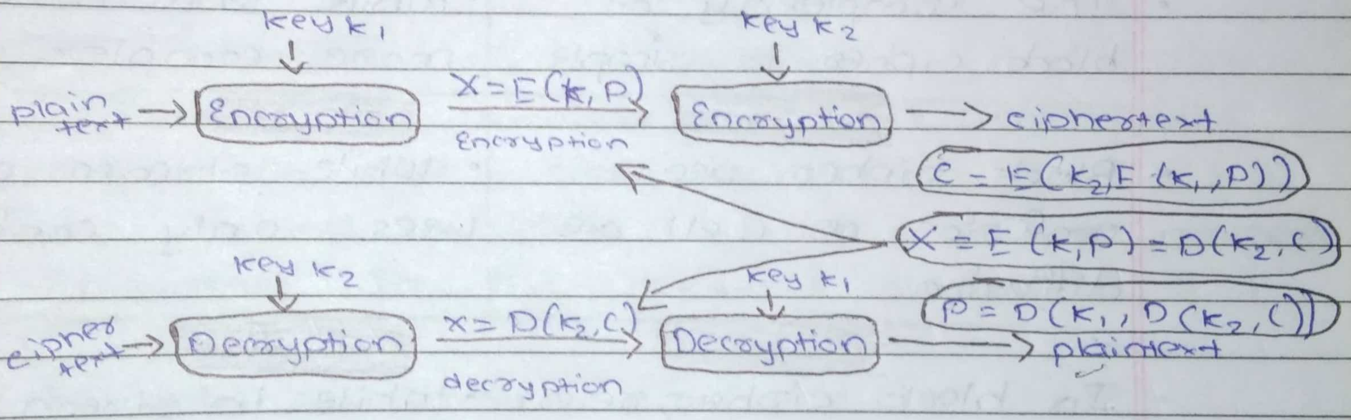
CNS
Assignment-3

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 × 56-bit keys, meaning 112-bit key length.

↳ Requires 2^{112} operations for brute force attack.

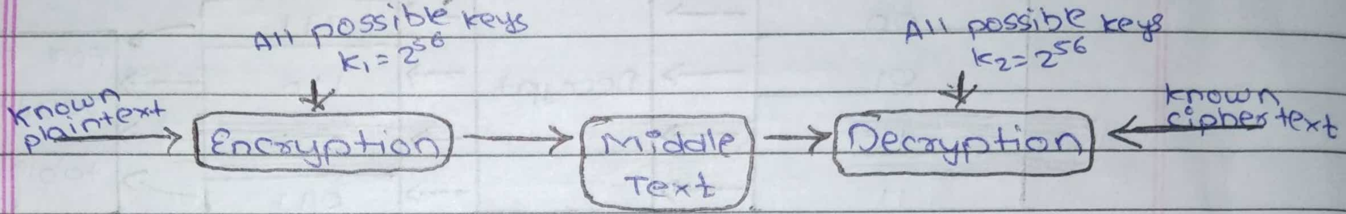
↳ Meet - in - the - middle attack makes it easier

- **Meet in the Middle Attack**

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

↳ Suppose cryptanalyst knowns P_i and corresponding C_i.

↳ Now, the aim is to obtain the values of k_1 and k_2.



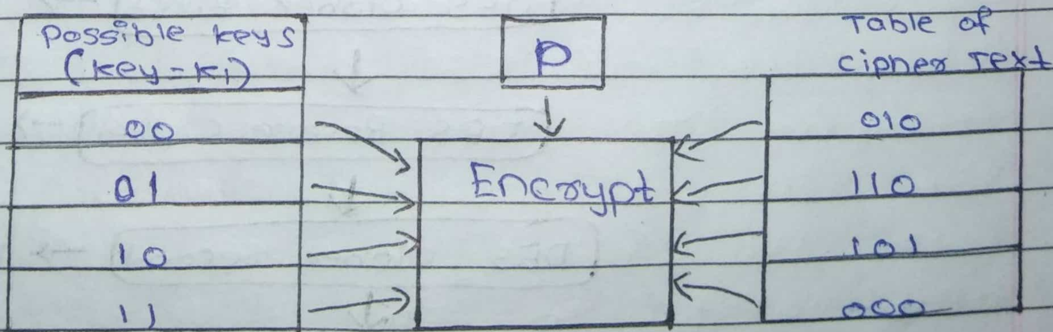
↳ No. of Encryption and Decryptions : $2^{56} + 2^{56} = 2^{57}$

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

⇒ STEP - I

↳ For all possible values (2^{56}) of key, k1, the cryptanalyst would encrypte the known plaintext by performing $E(k_1, P)$

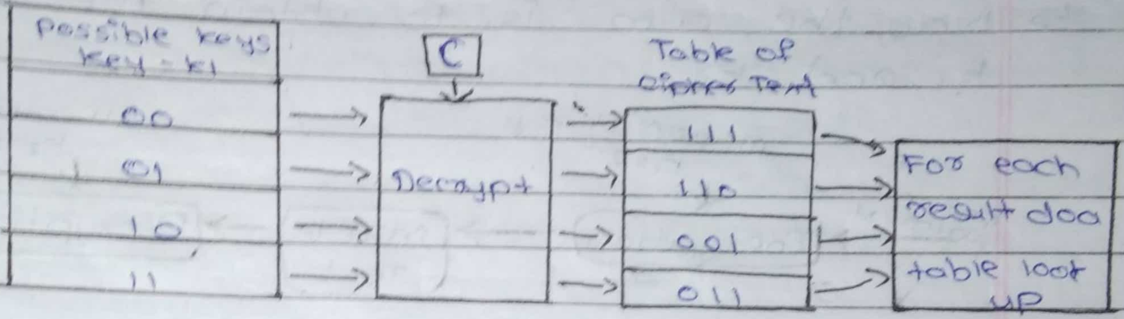
↳ The cryptanalyst would store output in a table.



⇒ **STEP-2**

↳ Cryptanalyst decrypt the known ciphertext with all possible values of k2.

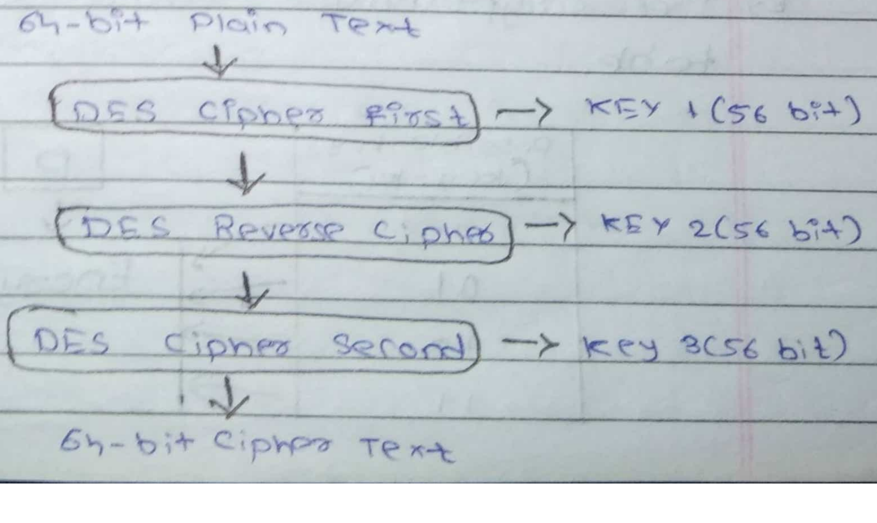
↳ In each case cryptanalyst will compare the resulting value with the all values in the table of ciphertext



- **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.



↳ Triple DES is also vulnerable to meet-in-the middle attack because of which it give ~~tota~~ 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.

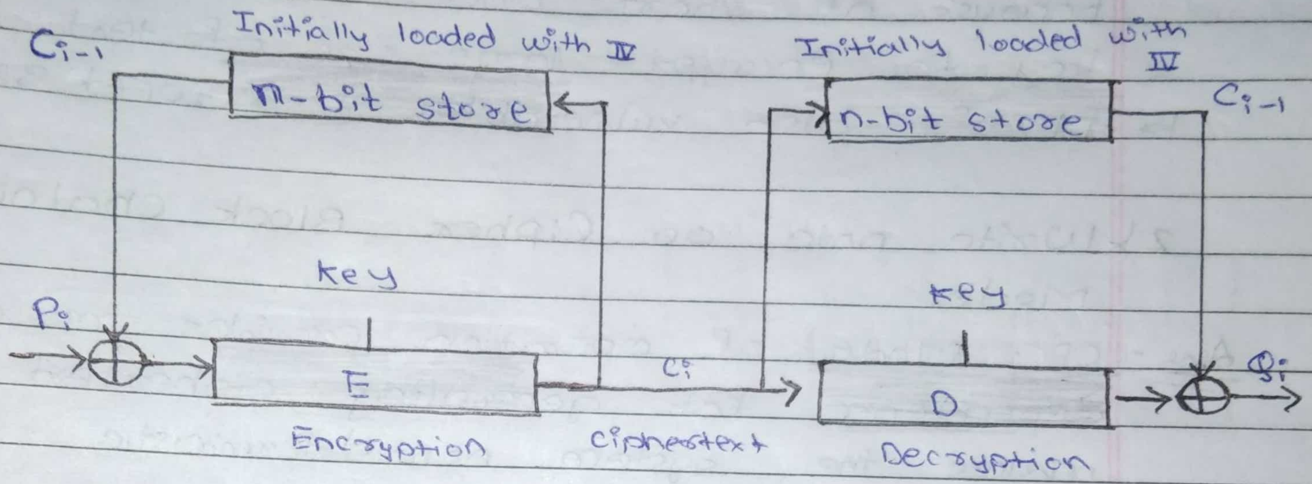
- Operation

↳ 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**

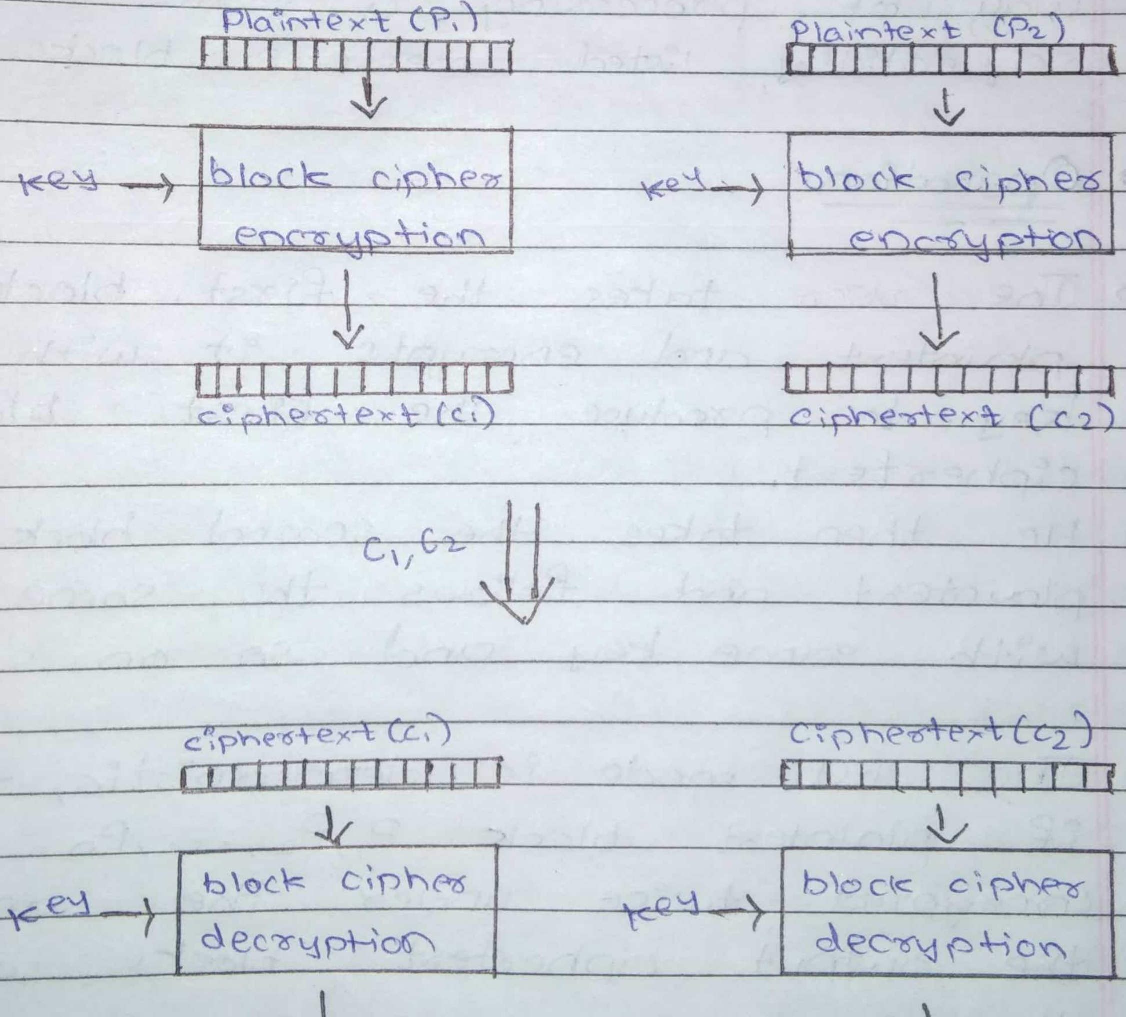
↳ The user takes the first block of plaintext and encrypts it with the key to produce the first block of ciphertext.

↳ 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 analogoue 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.

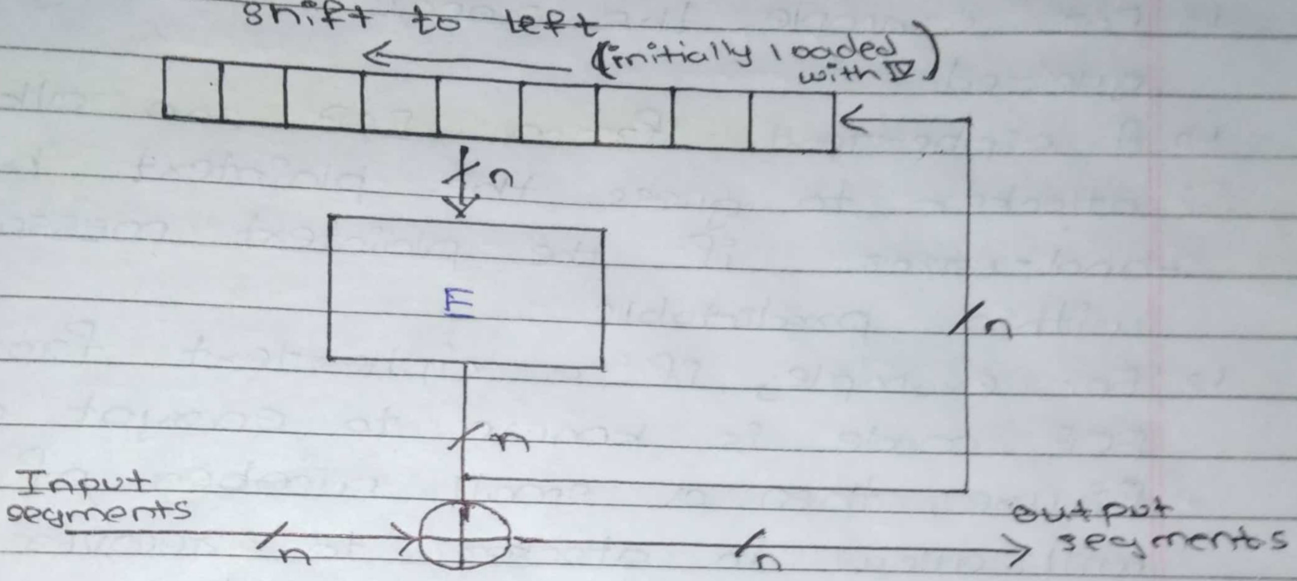
4) Write note on Output Feedback mode.

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-


shift to left
(initially loaded with IV)
n
E
n
n
Input segments
n
n
output segments