Alan Palayil
A20447935

ECE 543

Homework #2

Due Date: 2/19/23

Chapter 3

2) All that is required internally is a clock and a cryptographic algorithm that includes the key. Every time the clock ticks, a new number is produced to display. This number can either be a result of result of encrypting the time using the secret key, or it can be the subsequent output of a cryptographic pseudorandom number generator, such as RC4. It's important that the device's clock operates accurately and consisently, so the computer system can make necessary adjustments. A small, unexpected deviation in the clock's accuracy can be addressed by allowing the system to accept multiple values.

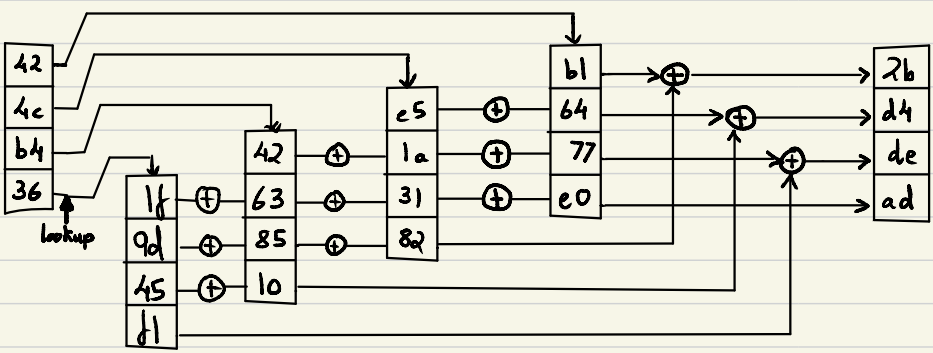
4) Revise the DES algorithm to eliminate the initial permutation of the key. Any message encrypted using standard DES and key 'K' can be encrypted using the modified version of the algorithm, using a key 'K' that is derived from K by performing the initial key permutation in DES. If we are able to successfully penetrate the modified version, we can then decrypt the message.

8) Weak keys are characterized by having C_0 and D_0 as either all ones or all zeroes. As each C_i is a permutation of C_0 and each D_i is a permutation of D_0, all the C_is are equal to C_0 and all the D_is are equal to D_0. Since K_i depends only on C_i and D_i, all K_is will be the same. This results in the K_is being identical both forwards and backwards, making the encryption and decryption process identical.

11) It is sufficient to demonstrate that by performing two DES encryption in sequence, with the order of the 48-bit keys reversed, we end up with the original information. Let's call these two encryptions E and D, respectively. We will attempt to collapse pieces of E and D until there is nothing left. Firstly, we observe that the final permutation in E is undone by the

initial permutation in D. At this point, we have Round 16 of E followed by a swap of halves and then Round 1 of D. Based on the observation, a round followed by a swap of halves is equivalent to a reverse of that round followed by a swap of halves. Thus, Round 16 of E followed by a swap of halves and then Round 1 of D collapses into just a swap of halves. As we continue with lower rounds of E and higher rounds of D, all the rounds eventually collapse, leaving only the swap of halves from E. This then collapses with the swap of halves from D, leaving only initial permutation from E and the final permutation from D.

12)



Chapter 4

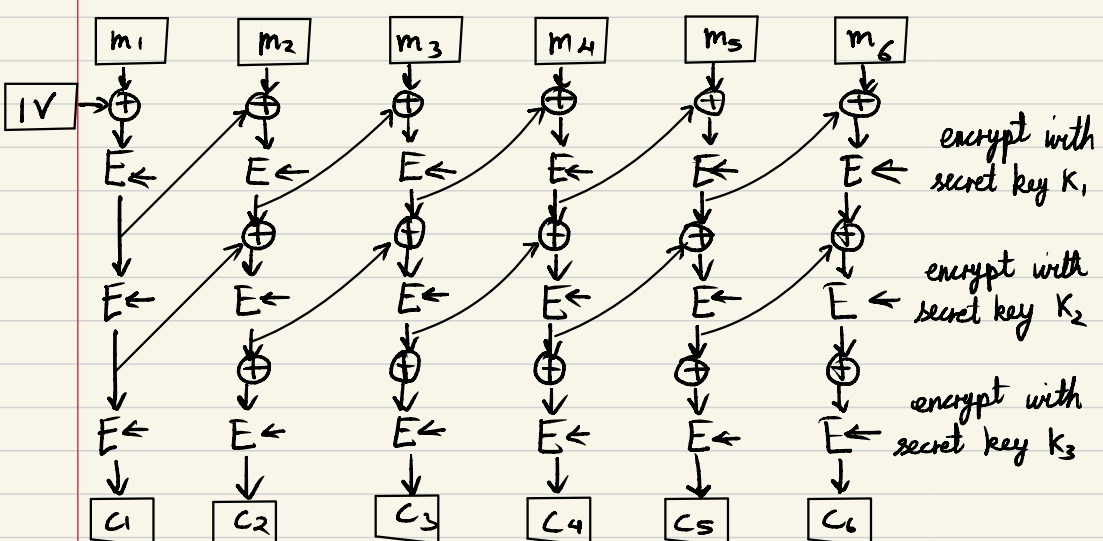
1) 64-bit OFB generates the stream $K(IV)$, $K(K(IV))$, $K(K(K(IV)))$, if K is a weak DES key, $K(K(IV)) = IV$ and the stream is just $K(IV)$, IV, $K(IV)$, IV, ...

3) The attack remains essentially the same. The only difference is that Table B is created using its keys for encryption instead of decryption.

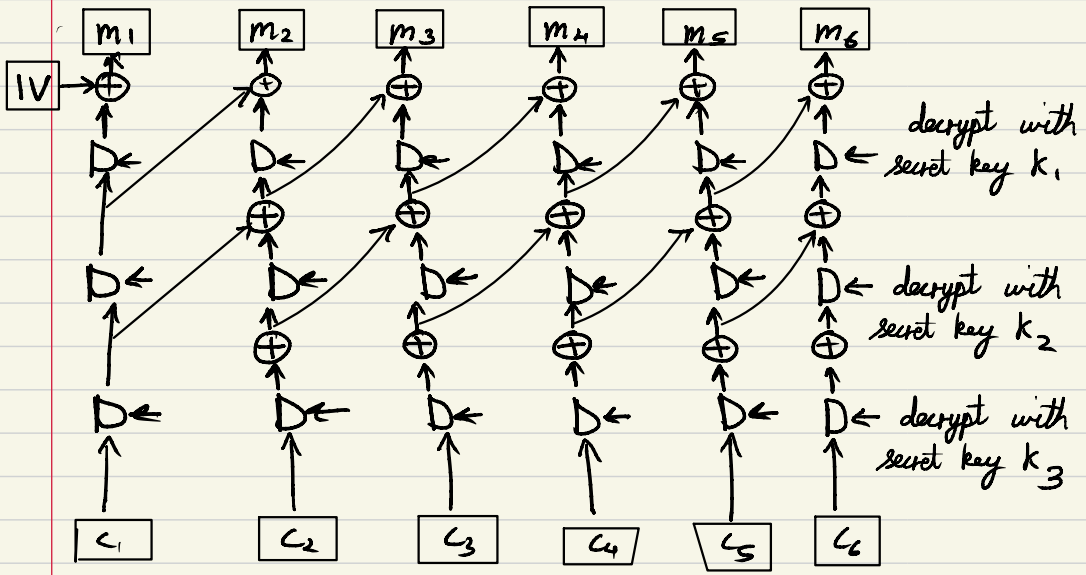
4) This question pertains to a specific 64-bit block of plaintext, denoted as 'p', and a specific 64-bit block of ciphertext, denoted as 'c'. To create a table with 'n' entries, the following process is performed:

a key is chosen at random, the plaintext 'p' is encrypted with the chosen key, and if the result is not already in the table, it is stored along with the key. If the table is not yet full, the process is repeated. To find a triple of keys, two keys are picked randomly, the ciphertext 'c' is decrypted using the second key, the result is encrypted using the first key, and if the result is found in the table, a triple of keys has been discovered. If not, the process is repeated. The expected no. of picks to find a successful combination $2^{64}/n$, where the probability of a randomly chosen pair of keys producing a result in the table is $n/2^{64}$. By choosing 'n' to be 2^{32}, the process of generating the table and searching for a successful combination can each be completed in approximately 2^{32} steps, which is manageable.

5) Triple encryption using EEE with CBC on the inside is 3 successive CBC encryptions:



Decryption is the inverse operation:



It can be observed that a change to the ciphertext block n will impact the plaintext blocks from n to $n+3$, but no other plaintext blocks are altered.