HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

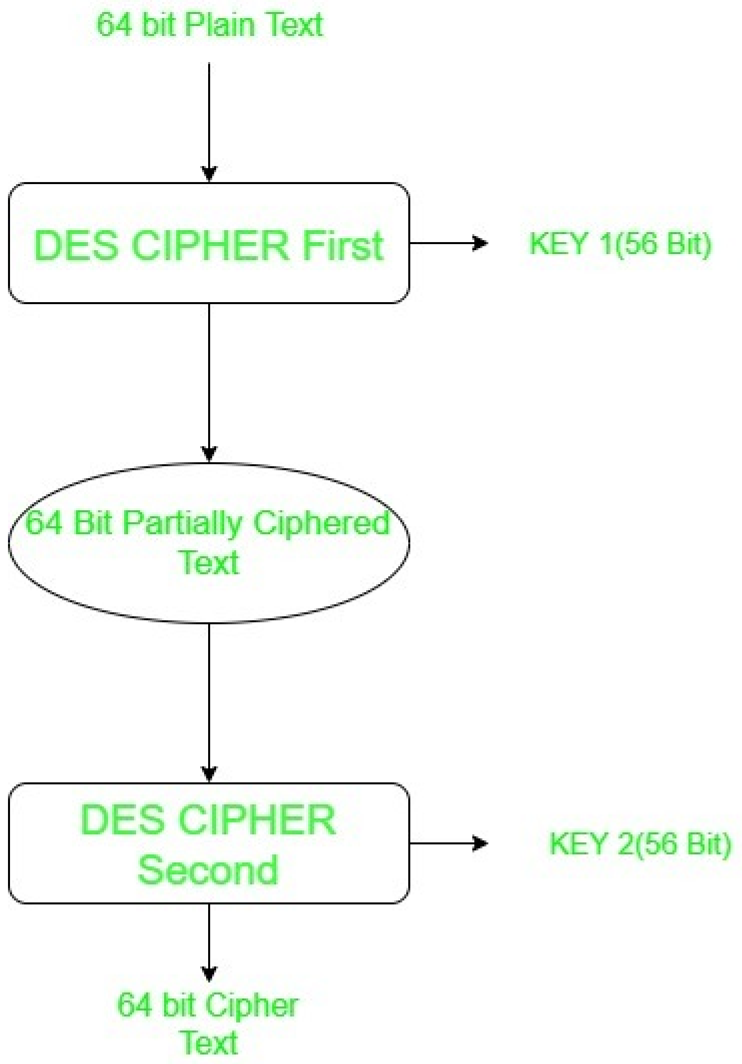
BBM 456 HOMEWORK 1

Mehmet Taha USTA – 21527472

Subject: Why Not Double Des? Explain

1) Double Des

Double DES is a encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which than converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.



However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

2) Meet in the middle Attack

The meet-in-the-middle attack is one of the types of known plaintext attacks. The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 2DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

A cipher, which is to be broken using meet-in-the-middle attack, can be defined as two algorithms, one for encryption and one for decryption. Each of them contains two simpler algorithms:

C = Eb(kb, Ea(ka, P))

P = Da(ka, Db(kb, C))

where:

- C is a ciphertext,
- P is a plaintext,
- E is an algorithm for encryption,
- D is an algorithm for decryption,
- ka and kb are two secret keys

A following equation can be written for the cipher defined above:

Db(kb, C) = Ea(ka, P)

Where C is the ciphertext, known to the intruder, which corresponds to the message P, also known to the intruder.

The first step of the attack is to create a table with all possible values for one side of the equation. One should calculate all possible ciphertexts of the known plaintext P created using the first secret key, so Ea(ka,P). A number of rows in the table is equal to a number of possible secret keys. It is good idea to sort the received table based on received ciphertexts Ea(ka,P), in order to simplify its further searching.

The second step of the attack is to calculate values of Db(kb,C) for the second side of the equation. One should compare them with the values of the first side of the equation, computed earlier and stored in the table. The intruder searches a pair of secret keys ka and kb, for which the value Ea(ka,P) found in the table and the just calculated value Db(kb,C) are the same.