Experiment 2

Chinmay Parikh A059

Questions

1. What are the various modes of operation of DES?
2. Explain linear cryptanalysis attack on DES?
3. List Advantages and Disadvantages of DES
4. A single bit error occurs in exactly one block of CT during transmission. How will this affect the recovery of PT in the following modes?

Answers

1. The types of modes included are:

   - Electronic Codebook (ECB) modeThe Electronic Codebook (ECB) mode is a basic, block, cryptographic method which transforms 64 bits of input to 64 bits of output as specified in FIPS PUB 46. The analogy to a codebook arises because the same plaintext block always produces the same cipher text block for a given cryptographic ey. Thus a list (or codebook) of plaintext blocks and corresponding ciphertext blocks theoretically could be constructed for any given key. In electronic implementation the codebook entries are calculated each time for the plain text to be encrypted and, inversely, for the ciphertext to be decrypted.
   - CipherBlock Chaining (CBC) mode CBC is a block cipher system in which the first plain text data block is exclusive-ORed with a block of pseudo-random data prior o being processed through the DES. The resulting ciphertext block is then exclusive-ORed with the next plain text data block to form the next input block to the DES, thus chaining together blocks of ciphertext. The chaining of ciphertext blocks provides an error extension characteristic which is valuable in protecting against fraudulent data alteration.
   - Cipher Feedback (CFB) mode. The CFB mode is a stream method of encryption in which the DES is used to generate pseudo random bits which are exclusive-ORed with binary plain text to form ciphertext. The cipher text is fed back to form the next DES input block. Identical messages that are encrypted using the CFB mode and different IVs will have different cipher texts. IVs that are shorter than 64 bits should be put in the least significant bits of the first DES input block and the unused, most significant, bits initialized to “0’s.”

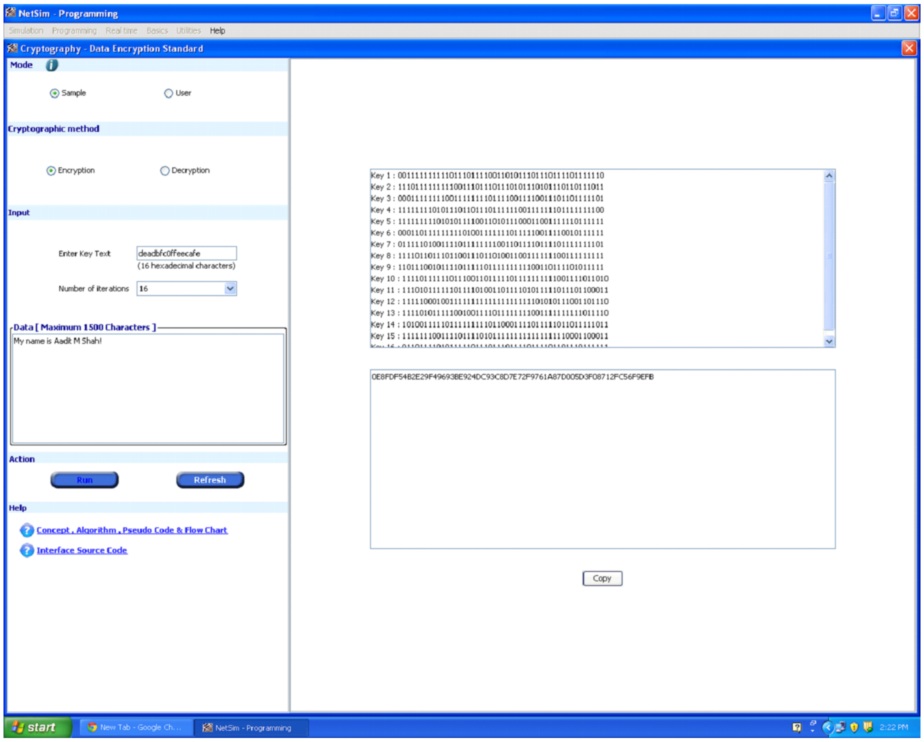
- Output Feedback (OFB) mode. The Output Feedback (OFB) mode is an additive stream cipher in which errors in the ciphertext are not extended to cause additional errors in the decrypted plaintext. One bit in error in the ciphertext causes only one bit to be in error in the decrypted plaintext. Therefore, this mode cannot be used for data authentication but is useful in applications where a few errors in the decrypted plaintext are acceptable. In the OFB mode, the same K bits of the DES output block that are used to encrypt a K-bit unit of plain text are fed back for the next input block. This feedback is completely independent of all plain text and all ciphertext. As a result, there is no error extension in OFB mode. If cryptographic synchronization is lost in the OFB mode, then cryptographic initialization must be performed. The OFB mode is not a self-synchronizing cryptographic mode.

2. In cryptography, linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers.There are two parts to linear cryptanalysis.The first is to construct linear equations relating plaintext, cipher text and key bits that have a high bias; that is, whose probabilities of holding (over the space of all possible values of their variables) are as close as possible to 0 or 1. The second is to use these linear equations in conjunction with known plaintext-cipher text pairs to derive key bits.

3. - DES has been around a long time, even now no real weaknesses have been found: the most efficient attack is still brute force.
   - DES is also an ANSI and ISO standard – it is easy to learn and implement.
   - Since DES was designed to run on 1977 hardware, it is fast in hardware and relatively fast in software.
   - The 56-bit key size is the biggest defect of DES. Chips to perform one million of DES encrypt or decrypt operations a second are available. A $1 million DES cracking machine can search the entire key space in about 7 hours.
   - Hardware implementations of DES are very fast; DES was not designed for software and hence runs relatively slowly.
   - As the technology is improving lot more day by day so there is a possibility to break the encrypted code, so AES is preferred than DES.
   - In DES only one private key is used for encryption as well as decryption because of its symmetric encryption key so if the key to decrypt is lost then the data will not be readable at the receiving end.

4.
- ECB: one bit error in a ciphertext block affects only the corresponding plaintext block (results in garbage) it is not recommended for messages longer than one block, or if keys are reused for more than one block.
- CBC: one bit error in a ciphertext block Yj has an effect on the j-th and (j+1)-st plaintext block Xj' is complete garbage and Xj+1' has bit errors where Yj had an attacker may cause predictable bit changes in the (j+1)-st plaintext block it automatically recovers from loss of a ciphertext block.

Output



Mode: ● Sample ○ User

Cryptographic method: ● Encryption ○ Decryption

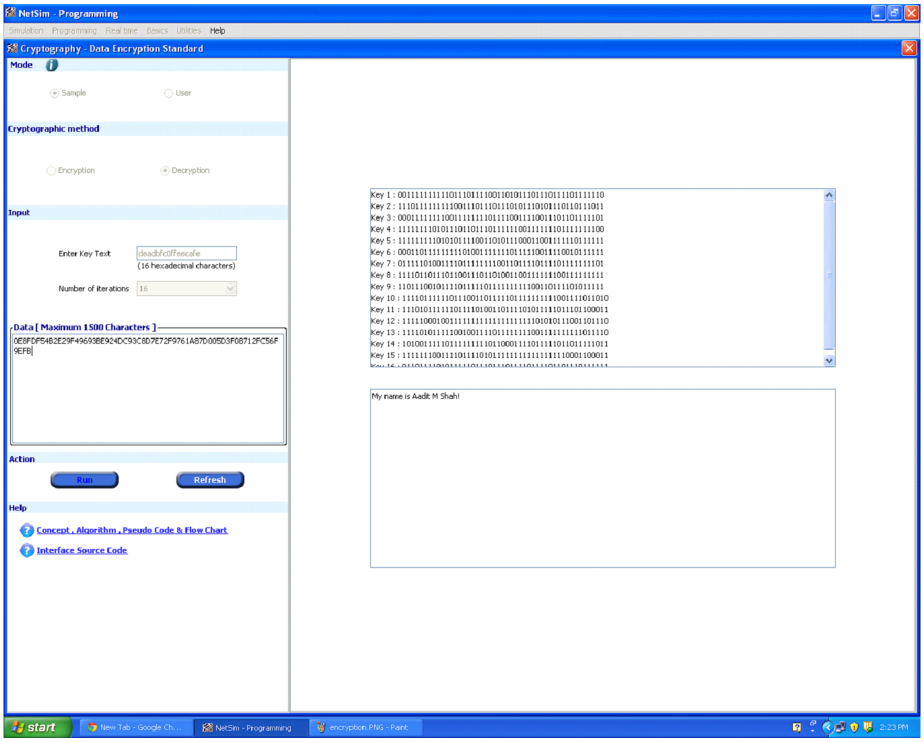
Enter Key Text: deadbfc0ffeecafe
(16 hexadecimal characters)

Number of iterations: 16

Data [Maximum 1500 Characters]: My name is Aadit M Shah!

```
Key 1 : 001111111111011101111001101011101110111101111110
Key 2 : 111011111111100111011101110101110101110110111011
Key 3 : 000111111110011111111011110011110011101101111101
Key 4 : 111111101011101101110111111001111110111111111100
Key 5 : 111111111010101111001101011100011001111110111111
Key 6 : 000110111111111010011111110111110011110010111111
Key 7 : 011111010011110111111110011011110111101111111101
Key 8 : 111101101110110011101101001100111111100111111111
Key 9 : 110111001011110111101111111111001101111010111111
Key 10 : 111101111110111001101111101111111111001111011010
Key 11 : 111010111111011110100110111101011111011101100011
Key 12 : 111110001001111111111111111111010101110011101110
Key 13 : 111101011111001001111011111111001111111111011110
Key 14 : 101001111101111111110110001111011111011011111011
Key 15 : 111111100111101111010111111111111111110001100011
```

```
0E8FDF54B2E29F49693BE924DC93C8D7E72F9761A87D005D3F08712FC56F9EFB
```



● Sample ○ User

○ Encryption ● Decryption

Enter Key Text: deadbfc0ffeecafe
(16 hexadecimal characters)

Number of iterations: 16

Data [Maximum 1500 Characters]

```
0E8FDF54B2E29F49693BE924DC93C8D7E72F9761A87D005D3F08712FC56F
9EFB
```

```
Key 1 : 0011111111111011101111100110101110111011110111111
Key 2 : 111011111111100111011101110101110101110110111011
Key 3 : 000111111110011111111011110011110011101101111101
Key 4 : 111111110101110110111011111100111111011111111100
Key 5 : 111111111010101111001101011100011001111110111111
Key 6 : 000110111111111010011111101111100111100101111111
Key 7 : 011111010011110111111110011011110111101111111101
Key 8 : 111101101110110011101101001100111111100111111111
Key 9 : 110111001011110111110111111111100110111101011111
Key 10 : 111101111110111001101111101111111110011110110100
Key 11 : 111010111111011110100110111101011110111011100011
Key 12 : 111110001001111111111111111111101010111001101110
Key 13 : 111101011111001001110111111111001111111111011110
Key 14 : 101001111101111111110110001110111110110111111011
Key 15 : 111111100111101111010111111111111111110001100011
```

My name is Aadit M Shah!