CS 5153/6053 Network Security, Spring 2023  
Homework 1

Margi amin

Problem 1 (1 point). Given a message bearcats, if we encrypt it with Hill Cipher, what is the corresponding ciphertext? Assume n = 2 (each block as 2 characters) and the encryption key is below:  
K = / 2, 5

For easy calculation, a mapping table between characters (a, ..., z) and integers (0, ..., 25) is listed below.  
a b c d e f g h i j k l m n o p q r s t u v w x y z  
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Answer:

M = bearcats , four blocks: be ar ca ts

M1 = BE -> [1, 4 ] -> [15, 22] -> [R, W]

K X M1 =C1

x = (mod 26) =

M2 = AR -> [0,17 ] -> [25, 9] -> [Z, N]

K X M2 =C2

x = (mod 26) =

M3 = CA -> [2,0 ] -> [6, 4] -> [G, E]

K X M3 =C3

x = (mod 26) =

M4 = TS -> [19,18 ] -> [3, 2] -> [H, W]

K X M4 =C4

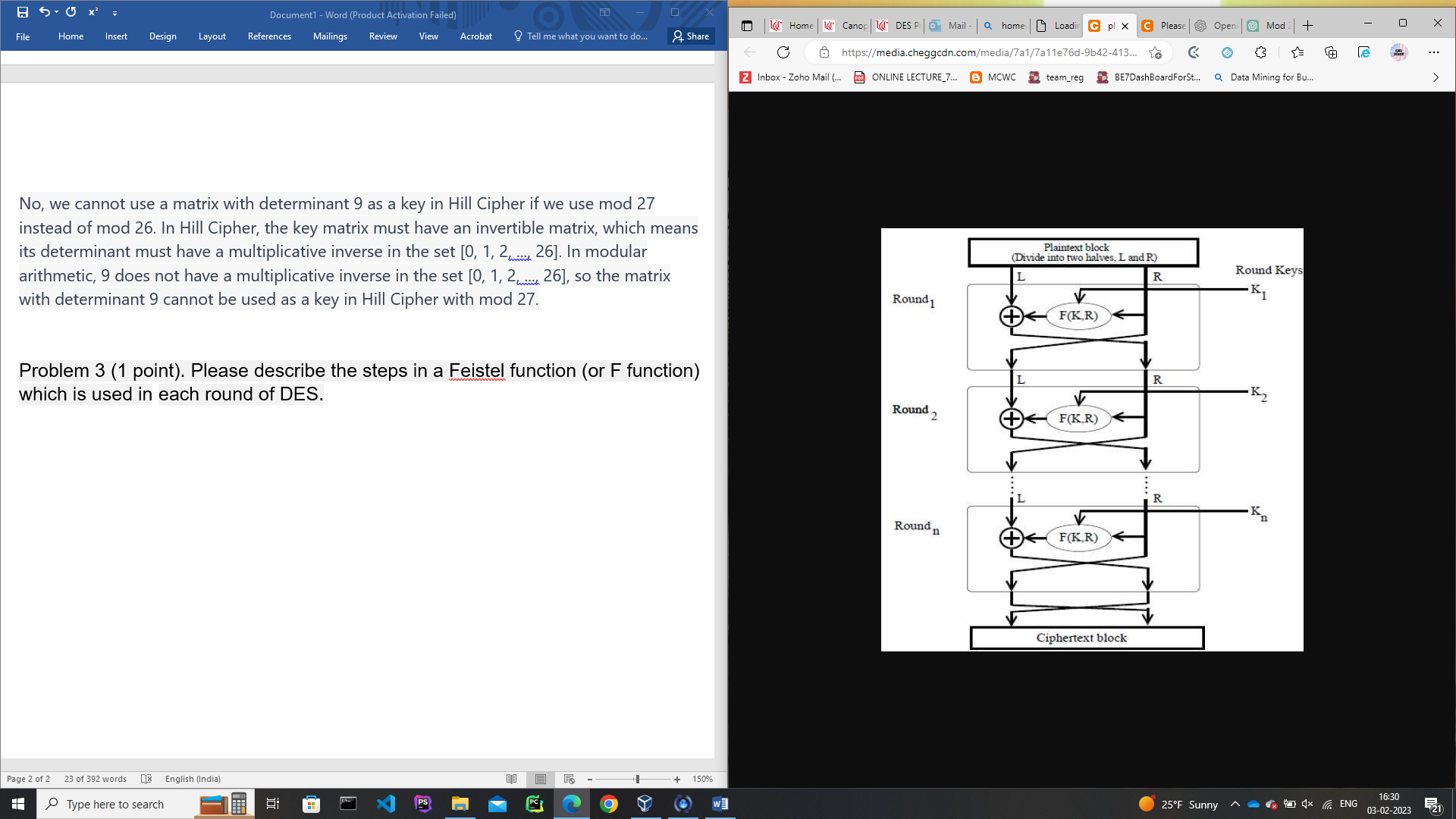
x = (mod 26) =

Encryption Results : bearcats = RWZNGEHW

Problem 2 (1 point). If we use mod 27 instead of mod 26 in Hill Cipher, if the determinant of a  
matrix is 9, can we use this matrix as a key? If yes (or no), please explain the reason.

No, we cannot use a matrix with determinant 9 as a key in Hill Cipher if we use mod 27 instead of mod 26. In Hill Cipher, the key matrix must have an invertible matrix, which means its determinant must have a multiplicative inverse in the set [0, 1, 2, ..., 26]. In modular arithmetic, 9 does not have a multiplicative inverse in the set [0, 1, 2, ..., 26], so the matrix with determinant 9 cannot be used as a key in Hill Cipher with mod 27.

Problem 3 (1 point). Please describe the steps in a Feistel function (or F function) which is used in each round of DES.



The Feistel Cipher is a symmetric encryption algorithm that operates on an input block of data and produces a ciphertext block as output.

The input block is divided into two halves, referred to as the left half (L) and the right half (R).

In each round, the right half (R) remains unchanged, while the left half (L) undergoes an operation that depends on both the right half (R) and the encryption key.

The Feistel Cipher is a symmetric encryption algorithm that operates on an input block of data and produces a ciphertext block as output. The input block is divided into two halves, referred to as the left half (L) and the right half (R). In each round, the right half (R) remains unchanged, while the left half (L) undergoes an operation that depends on both the right half (R) and the encryption key.

At the end of each round, a permutation step takes place, which swaps the modified left half with the unchanged right half. As a result, the right half of the current round becomes the left half of the next round, and the output of the modified left half becomes the right half of the next round. These substitution and permutation steps form a single round. The number of rounds is determined by the design of the algorithm.

Once all the rounds are completed, the two halves (R and L) are concatenated in the specified order to form the ciphertext block. This block represents the encrypted version of the original input block, providing confidentiality for the data being transmitted or stored.

Problem 4 (2 points). Assume the DES only has 3 rounds instead of 16 rounds. Please explain why a weak key in DES will cause self-inverting (i.e., Enck(Enck(m)) = m, where k is a weak key)

In DES, a weak key is a specific key for which the encryption and decryption operations are equivalent, meaning that applying the encryption twice results in the original message. This is because the key schedule in DES generates the same round subkeys for a weak key as its inverse.

If DES only had 3 rounds instead of 16 rounds, the number of possible subkeys generated by the key schedule would be significantly reduced. This would increase the probability of two subkeys being the same, which would result in the encryption and decryption operations being equivalent.

Therefore, with only 3 rounds, the likelihood of a weak key existing in DES increases, causing self-inverting, where Enck(Enck(m)) = m. This is why it's important for DES to have 16 rounds, so that the number of possible subkeys is large enough to reduce the likelihood of weak keys and maintain the security of the encryption.

Problem 5 (1 point). Please generate the 16 subkeys of this key 0x011f011f010e010e (the 8 parity bits are included) by using DES subkey schedule algorithm and demonstrate that this key is a semi-weak key (i.e., there are only 2 different subkeys that can be generated by this key). Please represent the subkeys you generate in hexadecimal.

Input = 0001 1111 0001 1111 0000 1110 0000 1110

0001 1111 0001 1111 0000 1110 0000 1110 0001 1111 0001 1111 0000 1110 0000 1110

Left 28 bits

0000 0000 0000 0000 0011 0000 1111

Left shift

0000 0000 0000 0000 0110 0001 1110

Right 28 bits

0011 1111 1111 1111 1111 1111 0011

Right shift

0111 1111 1111 1111 1111 1110 0110

Subkey 1 =

0000 0000 0000 0000 0110 0001 1110 0111 1111 1111 1111 1111 1110 0110

61E7FFFFE6

Left shift

000 0000 0000 0000 0110 0001 11100

Right shift

111 1111 1111 1111 1111 1110 01100

Subkey2 =

000 0000 0000 0000 0110 0001 11100 111 1111 1111 1111 1111 1110 01100

C3CFFFFFCC

Left shift

0000 0000 0000 0001 1000 0111 1000

Right shift

1111 1111 1111 1111 1111 1001 1001

Subkey 3=

0000 0000 0000 0001 1000 0111 1000 1111 1111 1111 1111 1111 1001 1001

1878FFFFF99

Left shift

000 0000 0000 0001 1000 0111 10000

Right shift

111 1111 1111 1111 1111 1001 10011

Subkey 4=

000 0000 0000 0001 1000 0111 10000 111 1111 1111 1111 1111 1001 10011

30F0FFFFF33

Left shift

00 0000 0000 0001 1000 0111 100000

Right shift

11 1111 1111 1111 1111 1001 100111

Subkey 5=

00 0000 0000 0001 1000 0111 100000 11 1111 1111 1111 1111 1001 100111

61E0FFFFE67

Left shift

0 0000 0000 0001 1000 0111 1000000

Right shift

1 1111 1111 1111 1111 1001 1001111

Subkey 6=

0 0000 0000 0001 1000 0111 10000001 1111 1111 1111 1111 1001 1001111

C3C0FFFFCCF

Left shift

0000 0000 0001 1000 0111 10000000

Right shift

1111 1111 1111 1111 1001 10011111

Subkey 7=

0000 0000 0001 1000 0111 100000001111 1111 1111 1111 1001 10011111

18780FFFF99F

Left shift

000 0000 0001 1000 0111 100000000

Right shift

111 1111 1111 1111 1001 100111111

Subkey 8=

000 0000 0001 1000 0111 100000000111 1111 1111 1111 1001 100111111

30F00FFFF33F

Left shift

00 0000 0001 1000 0111 1000000000

Right shift

11 1111 1111 1111 1001 1001111111

Subkey 9=

00 0000 0001 1000 0111 100000000011 1111 1111 1111 1001 1001111111

61E00FFFE67F

Left shift

0 0000 0001 1000 0111 10000000000

Right shift

1 1111 1111 1111 1001 10011111111

Subkey 10=

0 0000 0001 1000 0111 100000000001 1111 1111 1111 1001 10011111111

C3C00FFFCCFF

Left shift

0000 0001 1000 0111 1000 0000 0000

Right shift

1111 1111 1111 1001 1001 1111 1111

Subkey 11=

0000 0001 1000 0111 1000 0000 0000 1111 1111 1111 1001 1001 1111 1111

187800FFF99FF

Left shift

000 0001 1000 0111 1000 0000 00000

Right shift

111 1111 1111 1001 1001 1111 11111

Subkey 12=

000 0001 1000 0111 1000 0000 00000 111 1111 1111 1001 1001 1111 11111

30F000FFF33FF

Left shift

00 0001 1000 0111 1000 0000 000000

Right shift

11 1111 1111 1001 1001 1111 111111

Subkey 13=

00 0001 1000 0111 1000 0000 000000 11 1111 1111 1001 1001 1111 111111

61E000FFE67FF

Left shift

0 0001 1000 0111 1000 0000 0000000

Right shift

1 1111 1111 1001 1001 1111 1111111

Subkey 14=

0 0001 1000 0111 1000 0000 0000 0001 1111 1111 1001 1001 1111 1111 111

C3C000FFCCFFF

Left shift

0001 1000 0111 1000 0000 0000 0000

Right shift

1111 1111 1001 1001 1111 1111 1111

Subkey 15=

0001 1000 0111 1000 0000 0000 00001111 1111 1001 1001 1111 1111 1111

1878000FF99FFF

Left shift

001 1000 0111 1000 0000 0000 00000

Right shift

111 1111 1001 1001 1111 1111 11111

Subkkey 16=

001 1000 0111 1000 0000 0000 00000111 1111 1001 1001 1111 1111 11111

30F0000FF33FFF

Problem 6 (1 point). What are the 4 steps we have in each round in AES encryption? Please list the main differences between AES and DES.

The four steps in each round of AES encryption are:

1. Byte substitution using a substitution table (SubBytes)
2. Shift rows of the block horizontally (ShiftRows)
3. Mix columns of the block (MixColumns)
4. Add the round key to the block using bitwise XOR (AddRoundKey)

The main differences between AES and DES are:

1. Key size: AES has three key sizes (128, 192, and 256 bits) while DES has a fixed key size of 56 bits.
2. Number of rounds: AES uses 10 to 14 rounds, depending on the key size, while DES uses 16 rounds.
3. Block size: AES has a fixed block size of 128 bits, while DES has a block size of 64 bits.
4. S-Box size: AES uses a larger substitution table (S-Box) than DES.
5. Speed and security: AES is faster and considered more secure than DES.