CS 6343 CRYPTOGRAPHY

EXAM #1, SPRING 2022

TIME: 60 MINUTES

Name: SAINI YANALA

R Number: R11801029

Exam Conditions:

This is a closed book exam; No dictionary, "cheat sheet", or calculator is allowed.

You are not allowed to go out of the exam room during examination.

Turn off all communication devices (i.e., smart shoes, mobile phone, smart watch, etc.) for the duration of the exam.

PART 1 (MULTIPLE CHOICE QUESTIONS — 7 POINTS)

1. In a monoalphabetic cipher based on the English alphabet, the size of the keyspace is:
   a. 26!
   b. 26^n
   c. n^{26}
   d. 2^n
2. Which of the following is the reason why DES was retired decades ago as the US encryption standard
   a. Frequencies of English characters were easily analyzed
   b. The S-boxes had significant vulnerabilities given fast growing computing power
   c. The key was too short given fast growing computing power
   d. The number of rounds was too few given fast growing computing power

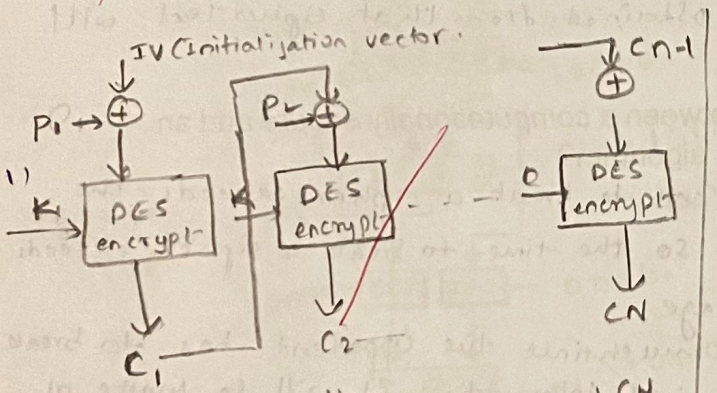
3. In an ideal block cipher using a block size of *n* bits, how big is the key in bits?
   a. 2^n
   b. $2^n!$
   c. $n2^n$
   d. $n2^n!$
4. The onetime pad is an example of a:
   a. Block cipher
   b. Feistel cipher
   c. Stream cipher
   d. Monoalphabetic cipher
5. The avalanche effect of a cipher is a property that stipulates that
   a. A small change in the key and (or) plain text causes a significant change in the cipher text (e.g., about 50% of the bits in the cipher text flip)
   b. A small change in the key and (or) plain text causes none of the bits in the cipher text flip
   c. A large number of rounds must be used by the cipher
   d. A small change in the key and (or) plain text causes all the bits in the cipher text flip
6. In a chosen cipher text attack, the following is required to be known to the cryptanalyst except:
   a. Cipher text
   b. Encryption algorithm
   c. Cipher text chosen by cryptanalyst together with its corresponding plain text decrypted with the secret key
   d. Cipher text chosen by the cryptanalyst together with a plain text having a minimum of 64-bits in length
7. In which of the following scenarios might the Electronic Code Book (ECB) mode of operation still be useful
   a. In the encryption of images
   b. For encryption of messages which have repetitive elements with a period of repetition a multiple of the block size.

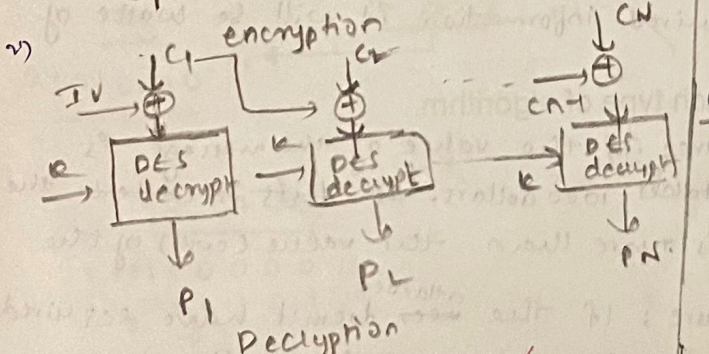
c. For secure transmission of very short amounts of random data, e.g., transmission of a DES or AES key
d. For Facebook live or Google hangout transactions

PART 2 (STRUCTURED QUESTIONS — 13 POINTS)

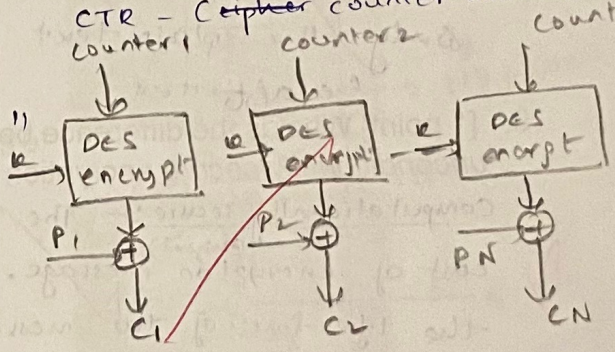
8. [3 points] Describe the difference in operation between the CBC and CTR (counter) modes of operations as used for data encryption (You are required to use diagrams to support your descriptions).

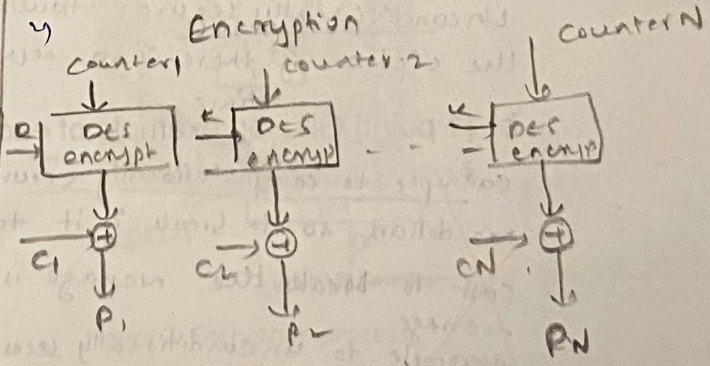
CBC Mode – (Cipher Block chaining mode)





CTR – (Cipher counter mode)





3) Here input to the encryption algorithm is plain text XORed with preceding ciphertext block

4) for encryption we have used encryption algorithm and for decryption used decryption algorithm

5) For the first block the input (plaintext) XOR with initialization vector &

6) Ciphertext block value is carried to next block in encryption

3) Here input to the encryption is counter only.

4) for encryption and decryption we used only encryption algorithm this is simplicity and advantage of CTR mode

5) Here counter 1 is nonce

6) Here no value is carried forward to next block.

7) In decryption previous value of cipher text block is carry forwarded

8) $C_N = E(K, [P_N, C_{N-1}])$

7) In decryption there is no carry forward of cipher text or plain text

8) $C_N = E(k, counter) \oplus P_N$

(b) [1 point] Make remarks on their properties with regard to propagation of errors in cipher text

1) In CBC mode if the error in ciphertext block then the error is carry forwarded to atmost 2 blocks

2) In CTR mode if the error occurs in ciphertext block only the plain text obtained from that ciphertext will be affected

9. [1 point] What is the difference between a *computationally secure* and an *unconditionally secure* encryption algorithm?

Computationally secure (original) :- The cost to break a cipher exceeds the cost of encryption message. so the time to break a cipher exceeds the life time of the message.

Unconditionally secure: how much time the opponent has to break the cipher if there is no required information it will be waste of time.

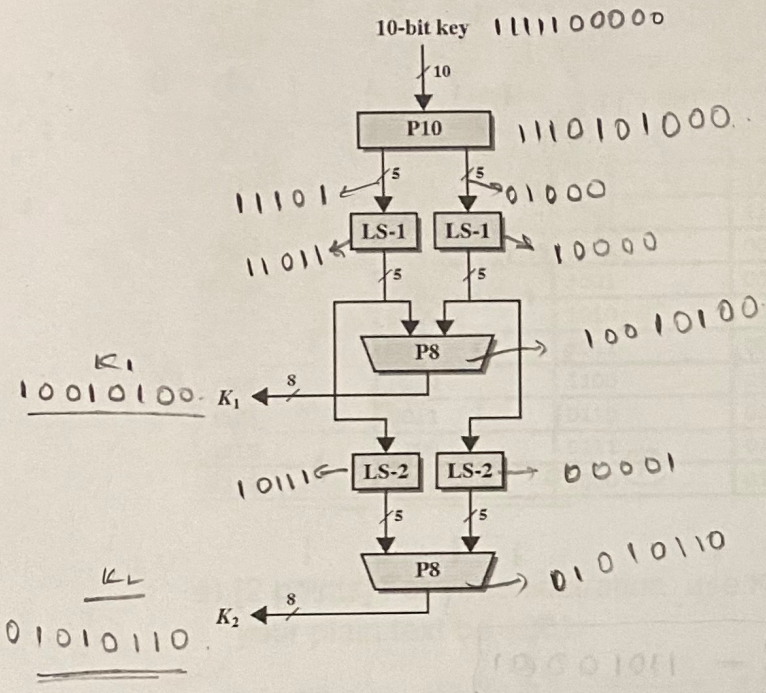
b. [1 point] Give an example of each type of algorithm.

example to computationally secure: If the value of the message is 100 dollars, so to break if it takes 1000 dollars. so ~~this is called~~ the cost to ~~break~~ the message is more than the value (cost) of the message.

example to unconditionally secure: If the ~~user~~ attacker doesn't have required information like plaintext (or) ciphertext then he cannot break the message.

10. [4 points] Figure 1 and Figure 2 summarize the process followed by the S-DES algorithm (a simplified version of DES). Use this cipher to encrypt the plain text: 10000001, using the key: 1111100000. In your solution please clearly show K_1, K_2, the output after round #1, and the final encryption output. Details of the S-boxes and permutation operations are included in the appendices.

Figure 1: Generating the sub keys



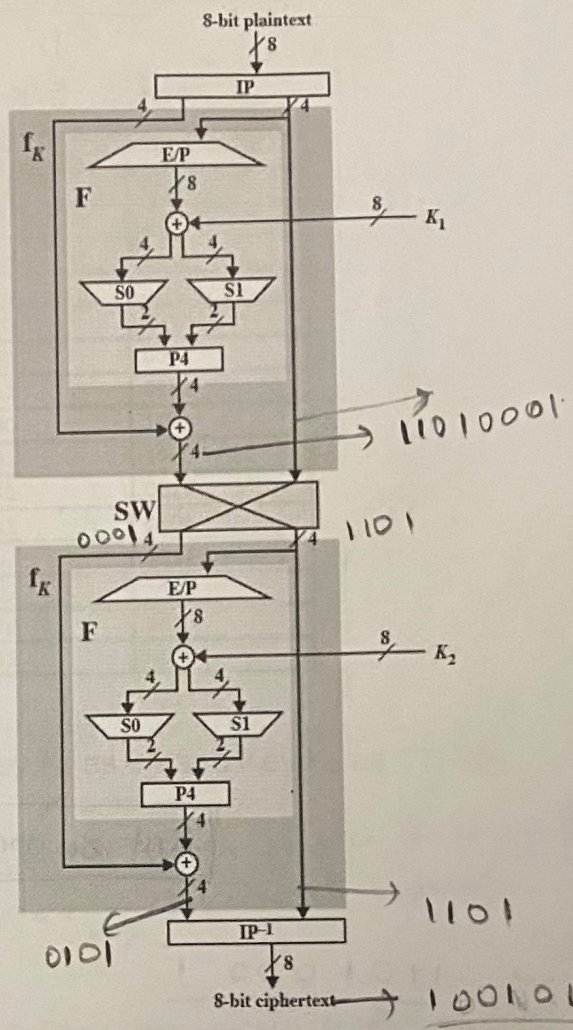
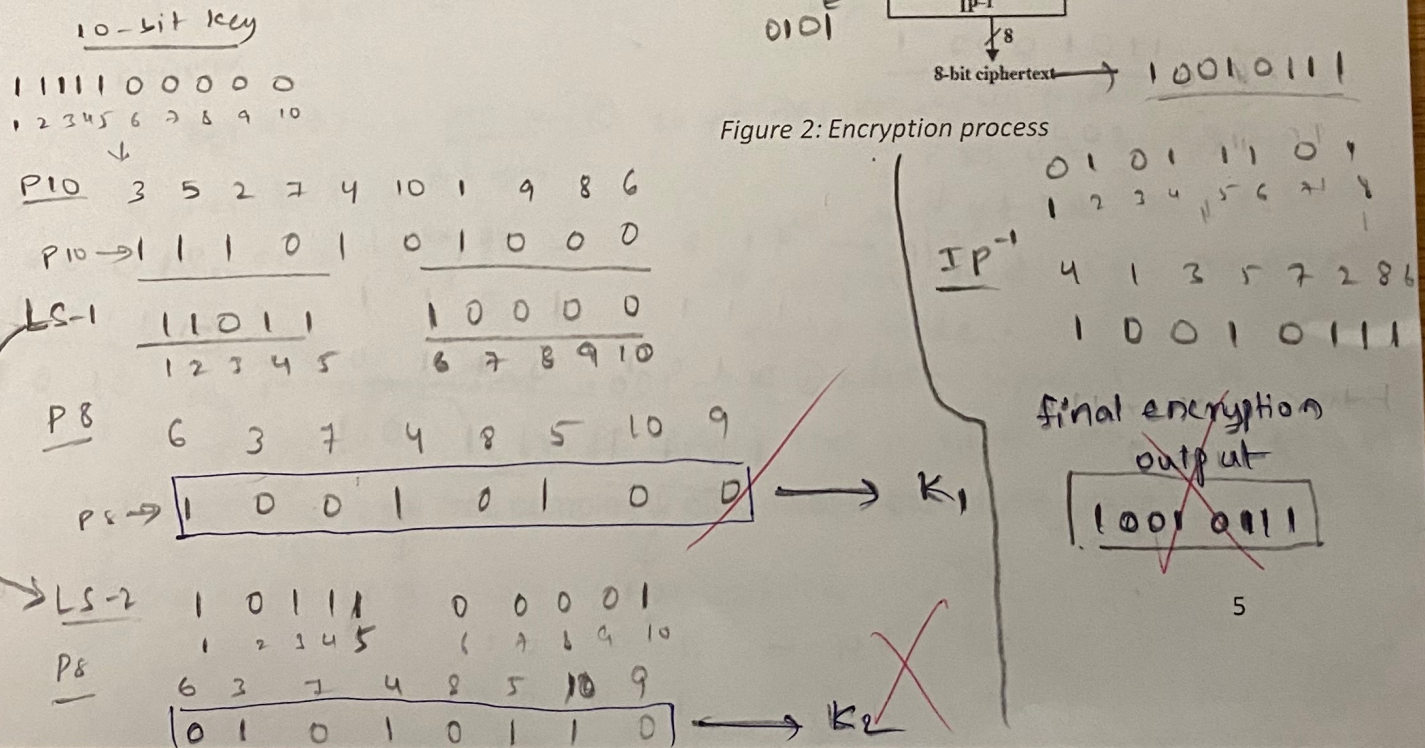


Figure 2: Encryption process



8bit plaintext — 1 0 0 0 0 0 0 1

IP — 2 6 3 1 4 8 5 7

0 0 0 1 0 1 0 0

E/p — 4 1 2 3 2 3 4 1

0 0 1 0 1 0 0 0

K_1 — ⊕ 1 0 0 1 0 1 0 0

1 0 1 1 1 1 0 0

S0 S1

0 1 0 1

P4 — 2 4 3 1

1 1 0 0

⊕ 0 0 0 1

→ 1 1 0 1

first round — 11010001

→ 1 1 0 1 0 0 0 1

SW→ 0 0 0 1 1 1 0 1

E/p — 4 1 2 3 2 3 4 1

1 1 1 0 1 0 1 1

K_2 — ⊕ 0 1 0 1 0 1 1 0

1 0 1 1 1 1 0 1

S0 S1

0 1 0 0

P4 — 2 4 3 1

1 0 0 0

1 0 0 0

⊕ 1 1 0 1

0 1 0 1

11. Using the toy cipher below as done in class; you will illustrate how double encryption falls to a meet-in-the-middle attack.

Plain Text	K=00	K=01	K=10	K=11
	Cipher Text			
0000	0110	1101	1000	0011
0001	0111	1110	1001	1001
0010	1000	1111	1010	1100
0011	1001	0000	1011	1110
0100	1010	0010	1100	1101
0101	1011	0011	1101	0110
0110	1100	0100	1110	0001
0111	1101	0101	1111	0100
1000	1110	0001	0000	1011
1001	1111	1001	0001	1000
1010	0000	1010	0010	0010
1011	0001	1011	0011	0101
1100	0010	1100	0100	0111
1101	0011	0110	0101	1111
1110	0100	0111	0110	1010
1111	0101	1000	0111	0000

a) [2 points] For your illustration, use Key K_1 as 01 and Key K_2 as 11. Let your plain text be 1001.

Encryption

$E(1001)$ — using $K_1 = 01$ — 1001 — cipher text (middle) — (X)

$E(1001)$ — $K_2 = 11$ — 1000 — cipher text — final

Decryption

$D_{K_2}(1000)$ — 1001 — (X) so we try for every possible value of K_2 using decryption we will get list so we have to compare that with encrypted stored table.

$D_{K_2}(1101) = 0100$

$D_{K_2}(0010) = 1011$

so it matches with 1001 which middle cipher text so plaintext is 1001 & cipher text is 1000 with $K_1 = 01$ & $K_2 = 11$.

b) [1 point] What is the time complexity of: i) meet-in-the-middle attack,

Time complexity of meet in the middle 2^{57}

ii) conventional brute-force attack on double encryption?

Appendices

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

S-boxes

S0

	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S1

	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

Part	8	9	10	11
7	4	1	1	2

blackboard	
10	4
4	3

Total 19/20