Mid Semester Examination Sub:Cryptography and Network Security (CSD505)
Session: 2023-24 (Winter) Marks: 28 Time: 2 Hours
(Answer ALL questions)

1(a) What do the message- Integrity, Authentication and Availability mean? Explain them. (3)

Ans: **Message Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. The message modification cannot be protected, however, if it is modified, the same can be detected at the receiving-end. The assurance that data received are exactly as sent by an authorized entity (i.e., contain modification, insertion, deletion, or replay). It is achieved for, example, by digital signature.

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source. That, the receiver must receive data/information from authorized source and source is authenticated to receives. The authentication service is concerned with assuring that a communication is authentic. It is achieved by MAC- Message Authenticated Code (for example).

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. Mainly, we should not apply arbitrary cryptographic techniques to protect our information so that the availability is reduced.

(b) Compare chosen plaintext and ciphertext attacks, and discuss their effects on encryption techniques. (4)

Ans:

In chosen plaintext Attack:

- Encryption algorithm is known
- Ciphertext (to be attacked)
- Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

In chosen cipkertext Attack:

- Encryption algorithm is known
- Ciphertext (to be attached)
- Additional Ciphertexts chosen by cryptanalyst, together with their corresponding decrypted plaintexts generated with the secret key.

If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a *chosen-plaintext* attack is possible. An example of this strategy is differential cryptanalysis. In general, if the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

The same is applicable for chosen ciohertext attack, however, some tricks may be adopted such that plaintext obtained reveals better patter to get the secret key.

(c) Define additive cipher. Is Caesar cipher additive? Justify your answer. (3)

Ans:

Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet**.- It is a shift cipher (during world war II, no mod 26 addition/subtraction was used**). Basically, Caesar cipher was extended to Additive cipher.

For example,

plain: meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

plain: 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
cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Let us assign a numerical equivalent to each letter:

a b c d e f g h i j k l m
0 1 2 3 4 5 6 7 8 9 10 11 12
n o p q r s t u v w x y z
13 14 15 16 17 18 19 20 21 22 23 24 25

Then the algorithm can be expressed as follows. For each plaintext letter *p*, substitute the ciphertext letter *C* is

$C = E(3, p) = (p + 3) \bmod 26$ and $p = D(3, C) = (C - 3) \bmod 26$

Now, a shift may be of any amount (1 to 25), so that the general Caesar algorithm or Additive Cipher is

$C = E(k, p) = (p + k) \bmod 26$

(d) Encrypt and decrypt 'cryptography is cool' using auto-key cipher with key *24*. Show the details of the computation. (4)

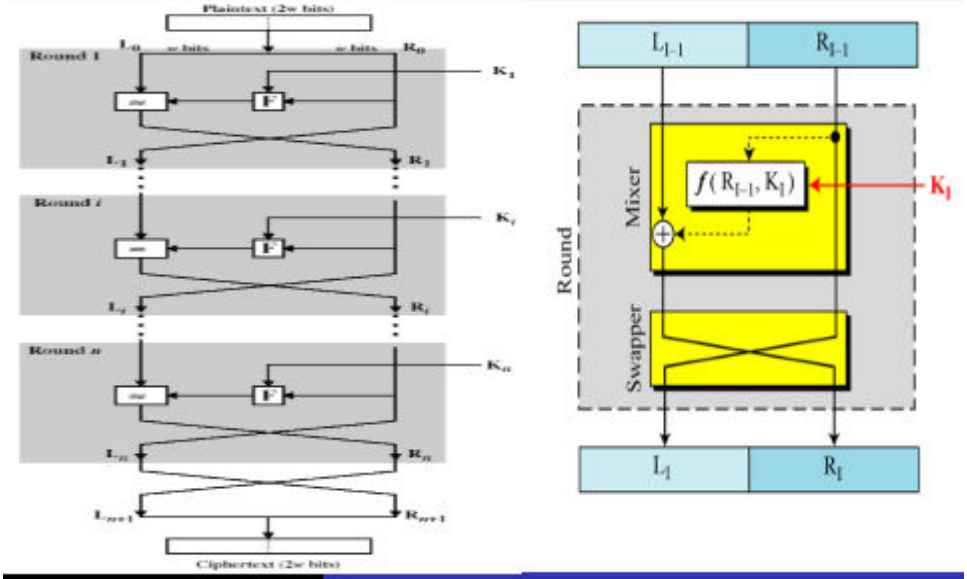
Ans:

2 (c) + 24 (mod 26) = 26 mod 26 = 0 (A)
17 (r) +2 (mod 26) = 19 mod 26 = 19 (T) and so on and similarly for decryption
(you have to show entire E/D in the answer book to get full mark)

2(a) Explain Feistel and DES ciphers and compare them with necessary diagrams. (3+3)

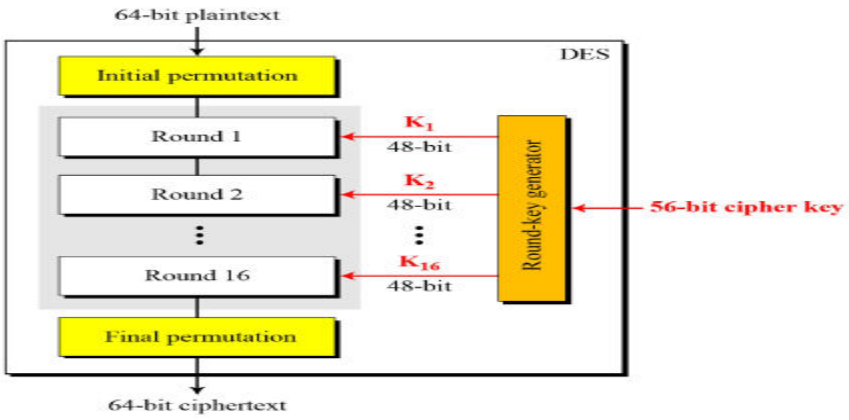
Ans:

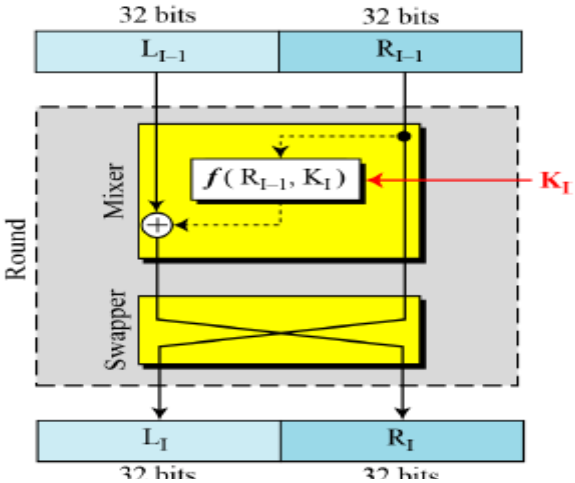
Feistel Cipher Structure

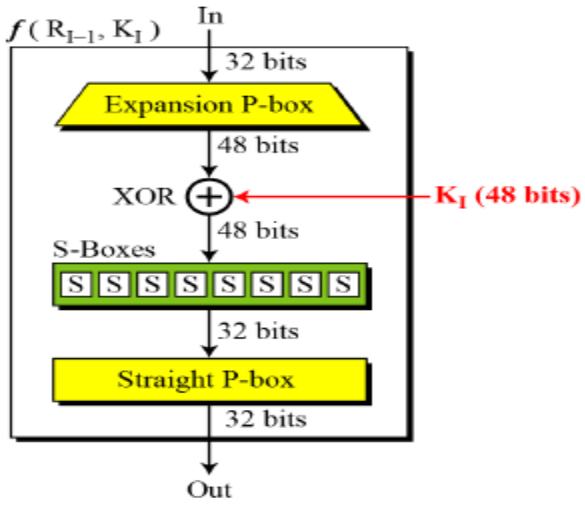


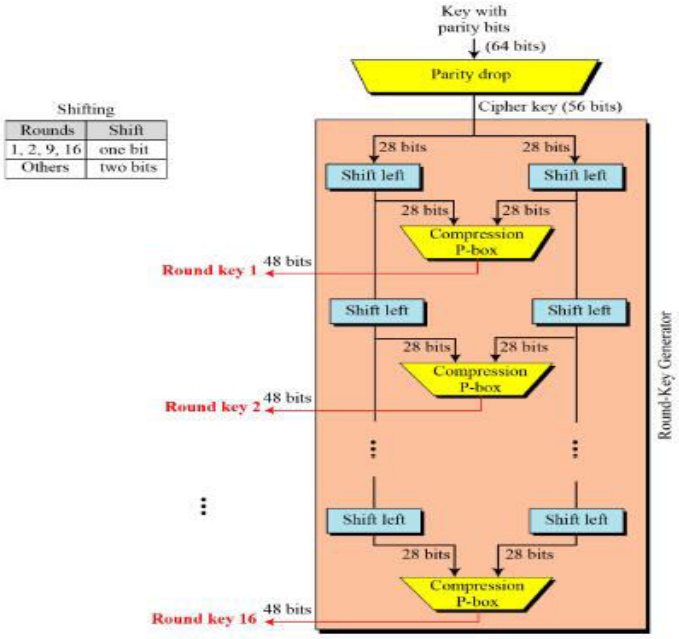
- The encryption and decryption processes are:
  - $LE_i = RE_{i-1}$
  - $RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$

  - $RE_{i-1} = LE_i$
  - $LE_{i-1} = RE_i \oplus F(RE_{i-1}, K_i) = RE_i \oplus F(LE_i, K_i)$









Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

(b) If DES *56*-bit key in hexadecimal is *1A2B3C4*, then compute the first four subkeys K_1, K_2, K_3 and K_4, where the key-compression table is (4)

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Ans:

0 0 0 0 0 0 0 0 0001 1010
0 0 0 0 0 0 0 0 0010 1100
0 0 0 0 0 0 0 0 0011 1101
0 0 0 0 0 0 0 0 0100

Ist Round 1 bit left circular shift:

0 0 0 0 0 0 0 0
0 1 1 01 0 0 0
0 0 0 0 0 0 0 1
0 1 1 0 0 0 0 0
0 0 0 0 0 0 1 1
1 1 0 1 0 0 0 0
0 0 0 0 1 0 0 0

1st round key : 0 0 1 1 0 0 0 0
0 0 0 1 0 0 0 0
1 0 0 0 1 0 1 0
1 0 0 0 0 0 0 1
0 0 0 0 1 0 1 0
0 1 0 0 0 0 0 0

And so on.

3(a) Explain OTP (One Time Pad) cipher and evaluate its security aspect with justification. (2+2)

Ans:

One Time Pad (OTP) Cipher

- An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security.
  - Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated.
  - In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
  - Each new message requires a new key of the same length as the new message. Such a scheme, known as a one-time pad, is unbreakable.
  - It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

Also, for a given ciphertext produced using OTP, suppose a cryptanalyst has managed to find two keys such that to possible plaintexts are produced. How is the the cryptanalyst to decide which is the correct decryption and which is the correct key? If the actual key were produced in a truly random fashion, then the cryptanalyst cannot say that one of the two keys is more likely than the other. Thus, there is no way to decide which is the correct and which plaintext is correct. Hence OPT is not breakable and perfectly secure.