Mid-Semester Examination | Sub: Cryptography and Network Security (CSD505)
Session: 2022-23 (Winter) | Marks: 30 | Time: 2 Hours

(Answer ALL questions)

1(a) Explain the brute-force and frequency analysis attacks on monoalphabetic cipher. (3)

ANS: It is secure against brute-force attacks, because we have a total of 26! ≈ 4 x 10^{26} keys, which is much more than in Cesar, Additive, Multiplicative and Affine ciphers. Thus, it is secure against brute-force attacks.

However, it is insecure against frequency analysis attack as explained below:

Human languages are not random. In English (or any language) certain letters are used more often than others. For examples, *E* is by far the most common letter, followed by *T*, *R*, *N*, *I*, *O*, *A*, *S* etc. If we look at a ciphertext, certain ciphertext letters are going to appear more often than others. It would be a good guess that the letters that occur most often in the ciphertext are actually the most common English letters as mentioned here (i.e., e). The procedure of making this attack is

Count relative letter frequencies in a ciphertext.
Compare this distribution against the known one. For example, there is a good chance that the most frequently occurred character from ciphertext will map corresponds to e, and so on.
Proceeding with trial and error to finally get the probable plain text.

(b) Justify the perfect securities of one-time-pad cryptosystem. (2)

ANS: Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. 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. Because 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.

In fact, given any plaintext of equal length to the ciphertext, there is a key that produces that plaintext. Therefore, if you did an exhaustive search of all possible keys, you would end up with many legible plaintexts, with no way of knowing which was the intended plaintext. Therefore, the code is unbreakable. The security of the one-time pad is entirely due to the randomness of the key. If the stream of characters that constitute the key is truly random, then the stream of characters that constitute the ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

(c) Use Vegenere Tableau, encrypt and decrypt the message 'send more money' (drop blanks) using key stream: 9 0 1 7 23 15 21 14 11 11 2 8 9. (3)

ANS: Refer to the tableau given and use 1st row is for plaintext to be encrypted and 1st column is for key to be used, where columns are to be selected based on the letters corresponding to the numbers given from 0-25. The encryption is given below and similarly for decryption:

s	9	B
e	0	E
n	1	O
d	7	K
m	23	J
o	15	D
r	21	M
e	14	S
m	11	X
o	11	Z
n	2	P
e	8	M
y	9	H

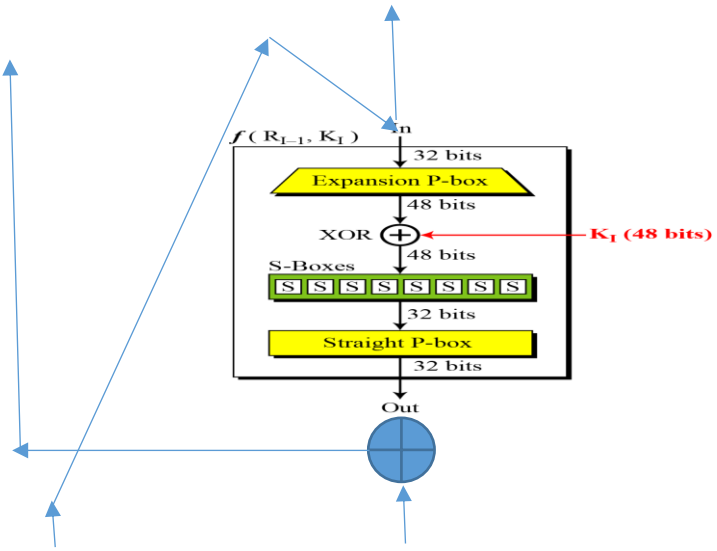
2(a) Clarify the design aspects of DES based on the Feistel cipher structure. (3)

ANS: DES design aspects with respect to Feistel require to select the following parameters as obtained from Feistel, provided below:

Block size: The larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed for a given algorithm. DES uses 64-bit block size with w =32 as in Feistel, which is considered reasonable and is nearly universal in block cipher design.
Key size: Larger key size means greater security but may decrease encryption/decryption speed. The greater security is achieved by greater resistance to brute-force attacks and greater confusion. Key sizes of 64 bits (which is selected for DES) or less are now widely considered to be inadequate, and 128 bits has become a common size. **Number of rounds:** The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds used in DES.
Subkey generation algorithm: Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
Round function F: Again, greater complexity generally means greater resistance to cryptanalysis. DES has a round function used in each round.

(b) Explain the reversibility of a DES round function for encryption and decryption. (2)

ANS: DES round function is shown for encryption, where the direction of processing is mentioned by arrows from top-to below and it is not reversible, and so it cannot be reversed during decryption. And instead, one-input to the XOR-gate of a round is reversed so that Li-1 and Ri-1 is obtained from Li and Ri at ith round.



(c) Describe the differential cryptanalysis attack with a simplified DES. (3)

ANS: Let P1 and P2 are two inputs to DES and the corresponding ciphertexts are C1 and C2 with the same key K. If we XORed (take difference) them, we have

C1 xor C2 = (P1 xor K) xor (P2 xor K)= P1 xor P2

The relation of C1 xor C2 = P1 xor P2 without key K is the basic idea of this attack.

Now, consider a simplified DES; 3-bit plaintext, 3-bit key and a single S-box table as shown below: where P xor K = X

X:	000	001	010	011	100	101	110	111
C:	11	00	10	10	01	00	11	00

We now form a table with P1 xor P2 as rows and C1 xor C2 as columns, where there are 8 cases for each xor in the input and there are 4 cases for C1 xor C2 as 00, 01, 10 and 11. The table is shown below w.r.t. to the S-box considered:

P1 xor P2	C1 xor C2			
	00	01	10	11
000	8 (1)	-	-	-
001	2 (.25)	2 (.25)	-	4 (.5)
010	2 (.25)	2 (.25)	4 (.5)	-
011	-	4 (.5)	2 (.25)	2 (.25)
100	2 (.25)	2 (.25)	4 (.5)	-
101	-	4 (.5)	2 (.25)	2 (.25)
110	4 (.5)	-	2 (.25)	2 (.25)
111	-	-	2 (.25)	6 (.75)

Table shows that the probabilities are not uniformly distributed, because of weakness of S-box and hence, the chosen plaintext attack (or Differential cryptanalysis attack is made.

3(a) Justify the rationality of S-Box and Inv-S-Box used in AES cipher. (3)

ANS: To see that InvSubBytes is the inverse of SubBytes transformation, label the matrixes in SubBytes and InvSubBytes as X and Y, respectively. For some 8-bit vector, we have $B' = XB \oplus C$, where C = 63_X, and we need to show that $Y(B') \oplus D = Y(XB \oplus C) \oplus D = B$, where D =$05_x$. Since XY = I, we have, $B \oplus YC \oplus D = B \oplus D \oplus D = B$ as proved, where YC = D

(b) Compute the multiplicative inverse of 45_{16} using the irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$ (2)

ANS: 45_{16} = 0100 0101 = 69_{10} and m(x)- 10001 1011 = 283_{10}

Now, $69 \times 125 \equiv 1 \; mod \; 539$, and 242 = 1111 0010_2 (F2) – $x^7+x^6+x^5+x^4+x$ which is the multiplicative inverse of 45_{16} with mod m(x).

4(a) Explain the security aspects of RSA. Why is it not perfectly secure? (3+1)

ANS: RSA is designed using a hard prime factorization problem of an integer. In RSA, a public modulus *n* is computed as n = p×q, where p and q be the two large prime numbers that are kept secret. Now, if an attacker can factorize n into p and q, then the private key d is exposed as $d \equiv e^{-1} \; mod \; \emptyset)(p-1)(q-1))$, where e is a public value. Since it is assumed that no efficient algorithm is available for factorization of a very large integer (but it does not assure such efficient algorithm can never exist), thus, RSA is assumption based secure, and it cannot be perfectly secure as Ont-Time-Pad.

(b) Mention the underlying hard problem of ElGamal cryptosystem with justification. (2)

ANS: ElGamal cryptosystem is developed based on DH key exchange protocol, which is based on DH problem and DL problem, DLP: Computing x from $X= g^x$ mod p, where X, g and p are known, DHP: Computing $K = g^{xy}$ mod p from $X= g^x$ mod p and $Y= g^y$ mod p ElGamal hard problem: Computing g^{rd} mod p and $(g^{rd})^{-1}$ mod p from g^r mod p and g^d mod. All are hard problem.

(c) Consider RSA, if *e = 7, n = 143* and ciphertext *C = 57*, compute plaintext *p*. (3)

ANS: n=143 = 13×11, thus $\varphi(143) = 12 \times 10 = 120$, now $7 \times \equiv 1 \; mod \; 120$, thus, d = 103
The plaintext p = $(57)^{103}$ mod 143 = 8

Table 3.3 *A Vigenere tableau*

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