TUTORIAL QUESTIONS

1. We set up a correspondence between alphabetic characters and residues modulo 26 as follows:

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

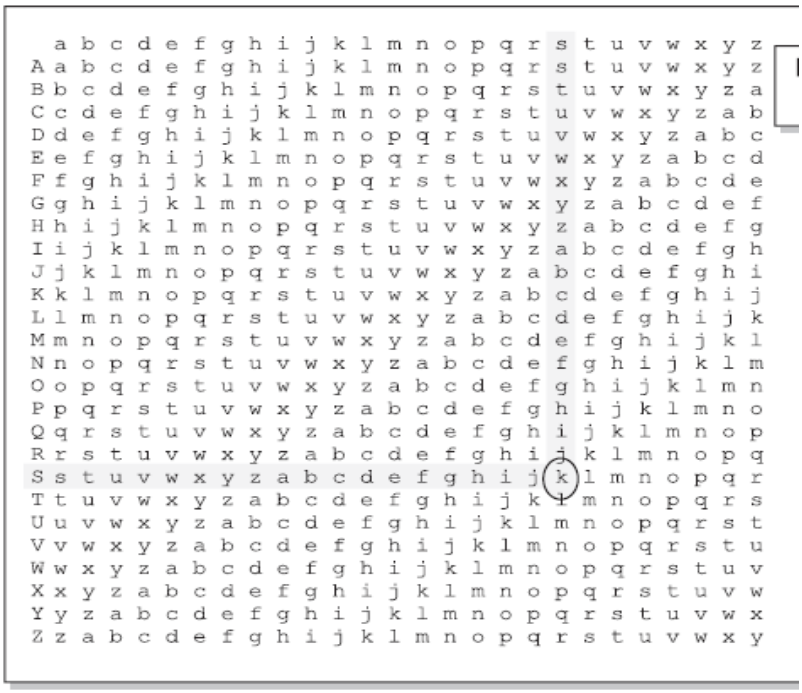
   Let the encryption algorithm be **c = (11m+7) mod 26** where **m** is the message and **c** is the ciphertext. Encrypt and decrypt the following plaintext. Show how your computation was done.

   i) HASH FUNCTION
   ii) INFORMATION SECURITY
   iii) ENCRYPTION AND DECRYPTION
   iv) CRYPTOGRAPHIC ALGORITHM
   v) COMPUTER SCIENCE

2. Using one-time pad, compute the cipher text for the following message stream and their keys
   i) Message Stream: 1111111001
      Key Stream: 1000000011
      Ciphertext stream:
   ii) Message Stream: 0000011100
      Key Stream: 1110000000
      Ciphertext stream:
   iii) Message Stream: 1110001111
      Key Stream: 0101001111
      Ciphertext stream:
   iv) Message Stream: 0000011111
      Key Stream: 1110000000
      Ciphertext stream:
   v) Message Stream: 1111111000
      Key Stream: 1000000011
      Ciphertext stream:

3. Differentiate between symmetric key cryptography and asymmetric key cryptography
4. List and explain three examples of cyber-attacks.
5. What is steganography and list five types of digital steganography

Vigenere Table



	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

6. Using the Vigenere Table above, encrypt the following plaintext with the key **COMPUTER**
   - i) SECURE COMMUNICATION MODEL
   - ii) THE STRENGTH OF THE CRYPTOSYSTEM
   - iii) ENCRYPTION SCHEME
   - iv) EXAMPLES OF SYMMETRIC ALGORITHMS

7. Prove the following equation
   - i) $S_{A,B} = S_{B,A}$ (Using Diffie Hellman)
   - ii) $Dec_K(Enc_K(m)) = m$

8. Suppose Bob chooses p = 11 and $e_1 = 3$ and d = 7 and Alice chooses r = 5, compute the ciphertext C_1 and C_2 for the plaintext 7 and decrypt C_1 and C_2 to obtain the plaintext 7 using ElGamal Cryptosystem.

9. With the aid of a diagram, draw the conceptual scheme for
   - i) Data Encryption Standard (DES)
   - ii) Advanced Encryption Standard (AES)

10. Differentiate between the following:
    - i) Substitution cipher and Transposition cipher
    - ii) Block cipher and Stream cipher

11. Prove the ElGamal cryptosystem: $[C_2 \times (C_1^d)^{-1}] = P$

12. Using Diffie Hellman Key exchange algorithm, compute the key for the following:
    i) p = 53, g = 3, x = 97, y = 157
    ii) p = 71, g = 5, x = 31, y = 29

13. Outline the RSA key generation, encryption and decryption process.

14. With the aid of a diagram, describe the two scenarios of Symmetric Cipher Model

15. We set up a correspondence between alphabetic characters and residues modulo 26 as follows:

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

Let the encryption algorithm be **c = 9m + 5 mod 26** where **m** is the message and **c** is the ciphertext. **Encrypt** and **decrypt** the following plaintext. Show how your computation was done.

    v) COMMUNICATION MODEL
    vi) THE CRYPTOSYSTEM

16. Using one-time pad, prove the correctness of $\mathbf{Dec_K(Enc_K(m)) = m}$

17. List and explain four cryptosystem services

18. Differentiate between active and passive attacks. Give two examples of each.

19. Using Diffie Hellman Key exchange algorithm, compute the key for the following:
    i) p = 53, g = 3, x = 97, y = 157
    iii) p = 71, g = 5, x = 31, y = 29

20. Using RSA, Encrypt and decrypt the message m = 3 where p = 3, q = 11, e = 7.

21. Suppose Bob chooses p = 11 and $e_1 = 3$ and d = 7 and Alice chooses r = 5, compute the ciphertext C_1 and C_2 for the plaintext 7 and decrypt C_1 and C_2 to obtain the plaintext 7 using ElGamal Cryptosystem.

22. Prove the following equation:
    iii) $S_{A,B} = S_{B,A}$ (Using Diffie Hellman)
    iv) $Dec_K(Enc_K(m)) = m$

23. If $S_1 = e_1^r \bmod p$, $S_2 = (m - dS_1)^{-r} \bmod (p-1)$ and $V_1 = e_1^m \bmod p$ and $V_2 = e_2^{S1} S_1^{S2}$. Verify that $V_1 = V_2$.

24. Describe the Diffie-Hellman Key Agreement in a diagram

25. Outline five (5) challenges of computer security