Cryptography IIITS
Practice Problems

INSTRUCTIONS : Question No. 1 consists of problems from Module 1 and Question No. 2 consists of problems from Module 2. Within Question 1 and 2 there are parts namely a,b,c... and so on. Each alphabet consists of problems from the same topic. Eg. Q1 b(i,ii,iii) consists of problems from Eucledian Algorithm.

***************MODULE 1***************

1. Answer the following questions :

a(i). Suppose Alice send a message m to Bob as $c = E_k(m)$, where k is shared key and E is secure encryption algorithm. In this communication from Alice to Bob, which of the following properties can be achieved: confidentiality, integrity, authentication, and non-repudiation. Justify your answer in 2-3 lines.

a(ii). Suppose Alice send a message m to Bob as $c = E_k(m), H(m)$, where k is shared key, E is secure encryption algorithm, and H is cryptographic hash function. In this communication from Alice to Bob, which of the following properties can be achieved: confidentiality, integrity, authentication, and non-repudiation. Justify your answer in 2-3 lines.

b(i). Given $a = 10$ and $b = 26$, find the linear combination of a and b using the Euclidean algorithm, that is, find x and y such that $ax + by = GCD(a, b)$.

Solution b(i). $GCD(a, b) = GCD(10, 26) = 2$

			Rewrite and solve:
26	= 10 (2) + 6	2	= 6 - 4(1)
10	= 6 (1) + 4		= 6 - [10-6(1)](1)
6	= 4 (1) + 2		= 6(2) + 10(-1)
4	= 2(2) + 0		= [26-10(2)](2) + 10(-1)
			= 26(2) + 10(-5)

So, $x = -5$ and $y = 2$.

b(ii). Given $a = 14$ and $b = 27$, find the linear combination of a and b using the Euclidean algorithm, that is, find x and y such that $ax + by = GCD(a, b)$.

b(iii). Given $a = 48$ and $b = 62$, find the linear combination of a and b using the Euclidean algorithm, that is, find x and y such that $ax + by = GCD(a, b)$.

c(i). Find the inverse of 7 mod 29.

c(ii). Find the inverse of 48 mod 366.

c(iii). Find the inverse of 12 mod 29.

d(i). Suppose $k = 12, 17$ then $c = E_k(m) =$ 12m+17 (mod 26). Find the decryption algorithm.

d(ii). Let m = 'alphabets', $k = (a, b) = (11, 2), E_k(m) =$ 11m+2 (mod 26). Find the Affine Cipher of m for k. Find the Decryption Algorithm.

e(i). Find the remainder of 8^{1232} upon division by 1231.

e(ii). Find the last 2 decimal digits of 413^{402}. Hint : The last 2 digits of a positive integer n are given by the least non-negative residue of n mod 100.

e(iii). Find all the integer solutions (x,y) for the equation 17x+19y = 3.

e(iv). Find all the integer solutions (x,y) for the equation 23x+11y = 7.

f(i). Solve :
x= 12 mod 11
x=7 mod 16
x = 9 mod 21
x= 17 mod 25

f(ii). Find all solutions of :
(i). $x^2 \equiv 1 mod 144$
(ii). $x^2 \equiv 1 mod 2^3.5^2$
(iii). $x^2 \equiv 1 mod 2^4.3^4$

g(i). Check for Quadratic Residue or Quadratic Non Residue:
(i). $\left(\frac{8}{5}\right)$
(ii). $\left(\frac{4}{13}\right)$
(iii). $\left(\frac{11}{3}\right)$
(iv). $\left(\frac{18}{7}\right)$

h(i). Using Rabin-Miller Algorithm check if the following numbers are prime or not :
(i). 171
(ii). 37
(iii). 271

*****************MODULE 2******************

2. Answer the following:

a(i). Suppose $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ is a cryptosystem. Given a key $k \in \mathcal{K}$, there exist only one $x \in \mathcal{P}$ with the condition $x = D_k(y)$, for any $y \in C(k)$. Prove or disprove the above statement.

Solution a(i). Assume that there exists $x_0 \neq x_1$ with $x_0 = D_k(y)$ and $x_1 = D_k(y)$. We know that a cryptosystem should satisfy the equation $x = D_k(E_k(x))$. Then we have, $x_0 = D_k(y) = D_k(E_k(x_0)$ and $x_1 = D_k(y) = D_k(E_k(x_1))$. From these two equations, we get $x_0 = D_k(y) = D_k(E_k(x_1)) = x_1$. This is a contradiction to our assumption. Therefore, Given a key $k \in \mathcal{K}$, there exist only one $x \in \mathcal{P}$ with the condition $x = D_k(y)$, for any $y \in C(k)$. Proved.

a(ii). In the ancient Caesar cipher, the key is a uniformly random "shuffle," or permutation, of the alphabet (including spacing and punctuation). For example, a random key might be: A becomes L, B becomes Z, C becomes A, space becomes J, etc. To encrypt a message, the sender simply applies the permutation to the message; to decrypt, the receiver reverses the shuffle. Suppose we use the Caesar cipher to encrypt just one message that is shorter than the alphabet size. Does it attain perfect secrecy? Give a convincing argument (or formal proof) why or why not?

a(iii). Every key is used with equal probability $\left(\frac{1}{|K|}\right)$ and for every $x \in \mathcal{P}$and for every $y \in \mathcal{C}$ there is a unique $key\mathcal{K}$ such that $E_k(m)$ = y. Prove the cryptosystem attains perfect secrecy.

b(i) Suppose $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$, and $\mathcal{C} = \{1, 2, 3, 4, 5\}$. The distributions are given as $\{Pr[a] = 1/6,\ Pr[b] = 1/3,\ Pr[c] = 1/3,\ Pr[d] = 1/6\}$ and $\{Pr[k_1] = 1/4,\ Pr[k_2] = 1/2,\ Pr[k_3] = 1/8,\ Pr[k_4] = 1/8\}$. The encryption mapping is as follows:

	a	b	c	d
k_1	1	2	3	4
k_2	2	1	5	3
k_3	4	2	1	5
k_4	3	1	5	2

(i). Find the distribution of ciphertext space $\mathcal{C}$?

(ii). Find the entropy $H(\mathcal{C})$?

Solution b(i) (i) We have the distribution of the ciphertext as follows:

$$Pr[Y = y] = \sum_{\{k:y \in C(k)\}} Pr[k]Pr[X = D_k(y)]$$

$$\begin{aligned}
Pr[Y = 1] &= \sum_{\{k:1 \in C(k)\}} Pr[k]Pr[X = D_k(1)] \\
Pr[Y = 1] &= Pr[k_1]Pr[X = a] + Pr[k_2]Pr[X = b] + Pr[k_3]Pr[X = c] + Pr[k_4]Pr[X = b] \\
&= (\frac{1}{4})(\frac{1}{6}) + (\frac{1}{2})(\frac{1}{3}) + (\frac{1}{8})(\frac{1}{3}) + (\frac{1}{8})(\frac{1}{3}) \\
&= 0.2916
\end{aligned}$$

$$\begin{aligned}
Pr[Y = 2] &= \sum_{\{k:2 \in C(k)\}} Pr[k]Pr[X = D_k(2)] \\
Pr[Y = 2] &= Pr[k_1]Pr[X = b] + Pr[k_2]Pr[X = a] + Pr[k_3]Pr[X = b] + Pr[k_4]Pr[X = d] \\
&= (\frac{1}{4})(\frac{1}{3}) + (\frac{1}{2})(\frac{1}{6}) + (\frac{1}{8})(\frac{1}{3}) + (\frac{1}{8})(\frac{1}{6}) \\
&= 0.2291
\end{aligned}$$

$$\begin{aligned}
Pr[Y = 3] &= \sum_{\{k:3 \in C(k)\}} Pr[k]Pr[X = D_k(3)] \\
Pr[Y = 3] &= Pr[k_1]Pr[X = c] + Pr[k_2]Pr[X = d] + Pr[k_4]Pr[X = a] \\
&= (\frac{1}{4})(\frac{1}{3}) + (\frac{1}{2})(\frac{1}{6}) + (\frac{1}{8})(\frac{1}{6}) \\
&= 0.1875
\end{aligned}$$

$$
\begin{aligned}
Pr[Y=4] &= \sum_{\{k:4\in C(k)\}} Pr[k]Pr[X=D_k(4)] \\
Pr[Y=4] &= Pr[k_1]Pr[X=d] + Pr[k_3]Pr[X=a] \\
&= (\frac{1}{4})(\frac{1}{6}) + (\frac{1}{8})(\frac{1}{6}) \\
&= 0.0625
\end{aligned}
$$

$$
\begin{aligned}
Pr[Y=5] &= \sum_{\{k:5\in C(k)\}} Pr[k]Pr[X=D_k(5)] \\
Pr[Y=5] &= Pr[k_2]Pr[X=c] + Pr[k_3]Pr[X=d] + Pr[k_4]Pr[X=c] \\
&= (\frac{1}{2})(\frac{1}{6}) + (\frac{1}{8})(\frac{1}{6}) + (\frac{1}{8})(\frac{1}{3}) \\
&= 0.1458
\end{aligned}
$$

(ii). The entropy of ciphertext space computed as folows:

$$
\begin{aligned}
H((C)) = -\sum_y Pr[Y=y]\log Pr[Y=y] \\
= -(Pr[Y=1]\log Pr[Y=1] + Pr[Y=2]\log Pr[Y=2] \\
+ Pr[Y=3]\log Pr[Y=3] + Pr[Y=4]\log Pr[Y=4] \\
+ Pr[Y=5]\log Pr[Y=5]) \\
= 2.1132
\end{aligned}
$$

b(ii) Suppose $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$, and $\mathcal{C} = \{1, 2, 3, 4, 5\}$. The distributions are given as $\{Pr[a] = 1/4,\ Pr[b] = 1/2,\ Pr[c] = 1/8,\ Pr[d] = 1/8\}$ and $\{Pr[k_1] = 1/6,\ Pr[k_2] = 1/3,\ Pr[k_3] = 1/3,\ Pr[k_4] = 1/6\}$. The encryption mapping is as follows:

	a	b	c	d
k_1	1	2	5	4
k_2	2	1	4	3
k_3	3	2	1	5
k_4	4	1	5	2

(i). Find the distribution of ciphertext space $\mathcal{C}$?

(ii). Find the entropy $H(\mathcal{C})$?

b(iii) Suppose $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $\mathcal{P} = \{a, b, c, \}$, $\mathcal{K} = \{k_1, k_2, k_3\}$, and $\mathcal{C} = \{1, 2, 3, 4\}$. The distributions are given as $\{Pr[a] = 1/2,\ Pr[b] = 1/3,\ Pr[c] = 1/6\}$ and $\{Pr[k_1] = 1/3,\ Pr[k_2] = 1/3,\ Pr[k_3] = 1/3\}$. The encryption mapping is as follows:

	a	b	c
k_1	1	2	3
k_2	2	1	4
k_3	3	4	1

(i). Find the entropy $H(\mathcal{C})$, $H(\mathcal{P})$, $H(\mathcal{K})$

(ii). Find $H(\mathcal{K}|\mathcal{C})$

b(iv) Suppose $(\mathcal{P}, \mathcal{K}, \mathcal{C}, \mathcal{E}, \mathcal{D})$ is a cryptosystem, where $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$, and $\mathcal{C} = \{1, 2, 3, 4, 5\}$. The distributions are given as $\{Pr[a] = 1/2,\ Pr[b] = 1/8,\ Pr[c] = 1/4,\ Pr[d] = 1/8\}$ and $\{Pr[k_1] = 1/4,\ Pr[k_2] = 1/4,\ Pr[k_3] = 1/4,\ Pr[k_4] = 1/4\}$. The encryption mapping is as follows:

	a	b	c	d
k_1	3	2	5	4
k_2	2	1	4	3
k_3	3	4	1	5
k_4	4	1	3	2

(i). Find the distribution of ciphertext space $\mathcal{C}$?

(ii). Find the entropy $H(\mathcal{C})$, $H(\mathcal{P})$, $H(\mathcal{K})$

(iii). Find $H(\mathcal{K}|\mathcal{C})$