USN | | | | | | | | | |

INTERNAL ASSESSMENT TEST – II

Sub:	CRYPTOGRAPHY							Code:	18EC744
Date:	05/ 12 / 2023	Duration:	90 mins	Max Marks:	50	Sem:	VII	Branch:	ECE

Answer any 5 full questions

		Marks	CO	RBT
1	With the help of a neat diagram, explain the AES Key expansion. Write the pseudocode for the same	[10]	CO2	L2
2	With suitable examples describe the AES Mix Column transformation.	[10]	CO2	L1
3	a) What are groups? With an example explain the group axioms. b) Define abelian group and cyclic group	[10]	CO3	L1
4	For the group $G = \langle Z11 + , \times \rangle$ (i)Find the primitive roots in the group (ii)Show that the group is cyclic. (iii) Make a table of discrete logarithms	[10]	CO3	L3
5	State and prove Fermat's Theorem. Using Fermat's theorem compute the following a) $7^{18}\ mod\ 19$ b) $456^{17}\ mod\ 17$ c) $5^{15}\ mod\ 1$ d) $3^{201}\ mod\ 11$	[10]	CO4	L3
6	Perform encryption using RSA algorithm for p=5, q = 11, e = 3, m = 9.	[10]	CO4	L2
7	With a neat diagram, explain public-key cryptosystem secrecy and Authentication.	[10]	CO3	L3
8	a) Define Euler's Totient function (n). Determine $\phi\ (10)\ and\ \phi\ (97)$. b) If m and n are co-prime numbers the $\phi\ (mn)$=$\phi(m)\phi(n)$. Using this property find ϕ (231),(440).	[10]	CO3	L3

IAT-2 Scheme of solutions

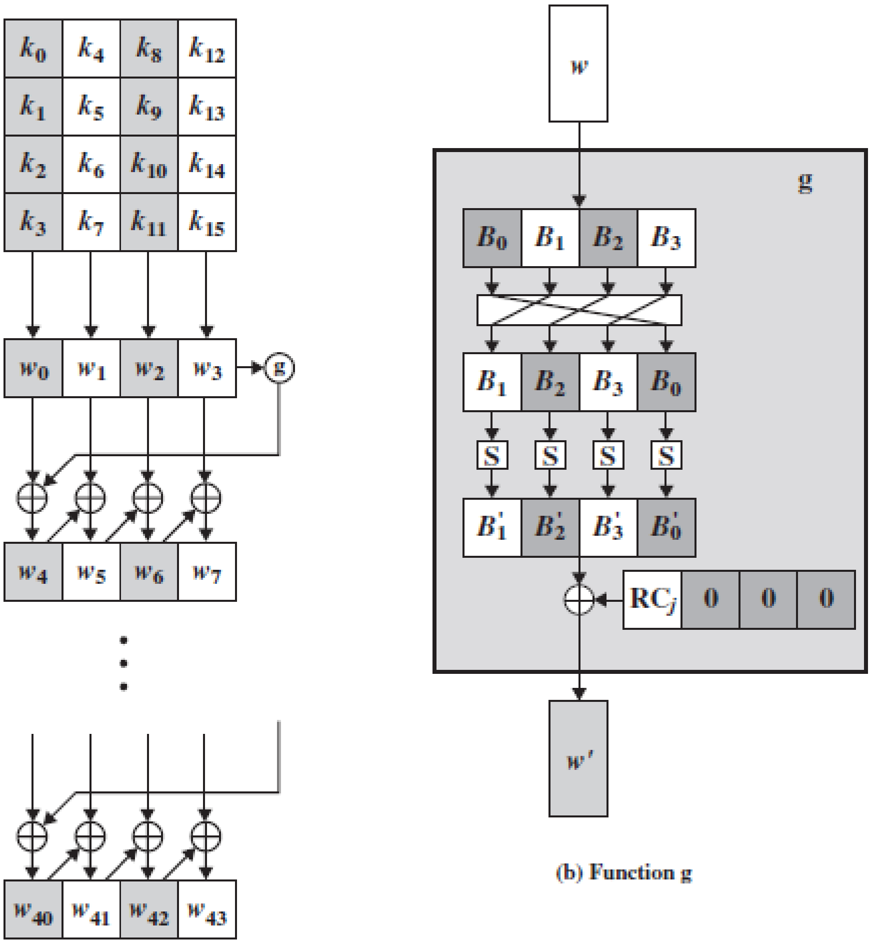
Q. no.	Questions	Marks
1.	With the help of a neat diagram, explain the AES Key expansion. Write the pseudocode for the same	10M

Key Expansion Algorithm

The AES key expansion algorithm takes as input a four-word (16-byte) key and produces a linear array of 44 words (176 bytes). This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher. The pseudocode on the next page describes the expansion.

The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word **w**[i] depends on the immediately preceding word, **w**[i − 1], and the word four positions back, **w**[i − 4]. In three out of four cases, a simple XOR is used. For a word whose position in the **w** array is a multiple of 4, a more complex function is used. Figure 5.9 illustrates the generation of the expanded key, using the symbol g to represent that complex function. The function g consists of the following subfunctions.

```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)   w[i] = (key[4*i], key[4*i+1],
                                      key[4*i+2],
                                      key[4*i+3]);
     for (i = 4; i < 44; i++)
     {
      temp = w[i - 1];
      if (i mod 4 = 0)    temp = SubWord (RotWord (temp))
                                 ⊕ Rcon[i/4];
      w[i] = w[i-4]  ⊕  temp
     }
}
```



(b) Function g

Figure 5.9 AES Key Expansion

1. RotWord performs a one-byte circular left shift on a word. This means that an input word [B_0, B_1, B_2, B_3] is transformed into [B_1, B_2, B_3, B_0].
2. SubWord performs a byte substitution on each byte of its input word, using the S-box (Table 5.2a).
3. The result of steps 1 and 2 is XORed with a round constant, Rcon[j].

The round constant is a word in which the three rightmost bytes are always 0. Thus, the effect of an XOR of a word with Rcon is to only perform an XOR on the leftmost byte of the word. The round constant is different for each round and is defined as Rcon[j] = (RC[j], 0, 0, 0), with RC[1] = 1, RC[j] = 2 · RC[j−1] and with multiplication defined over the field GF(2^8). The values of RC[j] in hexadecimal are

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

For example, suppose that the round key for round 8 is

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

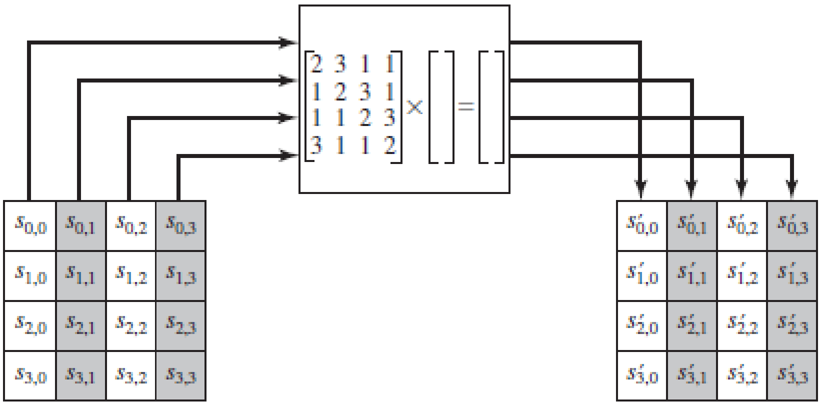
Then the first 4 bytes (first column) of the round key for round 9 are calculated as follows:

i (decimal)	temp	After RotWord	After SubWord	Rcon (9)	After XOR with Rcon	w[i−4]	w[i] = temp ⊕ w[i−4]
36	7F8D292F	8D292F7F	5DA515D2	1B000000	46A515D2	EAD27321	AC7766F3

2. With suitable examples describe the AES Mix Column transformation. 10M

MixColumns Transformation

Forward and Inverse Transformations The **forward mix column transformation**, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The transformation can be defined by the following matrix multiplication on **State** (Figure 5.7b):



(b) Mix column transformation

Figure 5.7 AES Row and Column Operations

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} \quad \textbf{(5.3)}$$

Each element in the product matrix is the sum of products of elements of one row and one column. In this case, the individual additions and multiplications[5] are performed in GF(2^8). The MixColumns transformation on a single column of **State** can be expressed as

$$\begin{aligned} s'_{0,j} &= (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \\ s'_{1,j} &= s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j} \oplus s_{3,j} \\ s'_{2,j} &= s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j}) \\ s'_{3,j} &= (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j}) \end{aligned} \quad \textbf{(5.4)}$$

The following is an example of MixColumns:

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

→

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

Let us verify the first column of this example. In

GF(2^8), addition is the bitwise XOR operation and that multiplication can be performed according to the rule established in Equation (4.14). In particular, multiplication of a value by x (i.e., by {02}) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (0001 1011) if the leftmost bit of the original value (prior to the shift) is 1. Thus, to verify the MixColumns transformation on the first column. we need to show that

It follows that multiplication by x (i.e., 00000010) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (00011011), which represents $(x^4 + x^3 + x + 1)$. To summarize,

$$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_00) & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_00) \oplus (00011011) & \text{if } b_7 = 1 \end{cases} \quad \textbf{(4.14)}$$

Multiplication by a higher power of x can be achieved by repeated application of Equation (4.14). By adding intermediate results, multiplication by any constant in GF(2^8) can be achieved.

$$\begin{array}{lllll} (\{02\}\cdot\{87\}) & \oplus (\{03\}\cdot\{6E\}) & \oplus \{46\} & \oplus \{A6\} & = \{47\} \\ \{87\} & \oplus (\{02\}\cdot\{6E\}) & \oplus (\{03\}\cdot\{46\}) & \oplus \{A6\} & = \{37\} \\ \{87\} & \oplus \{6E\} & \oplus (\{02\}\cdot\{46\}) & \oplus (\{03\}\cdot\{A6\}) & = \{94\} \\ (\{03\}\cdot\{87\}) & \oplus \{6E\} & \oplus \{46\} & \oplus (\{02\}\cdot\{A6\}) & = \{ED\} \end{array}$$

For the first equation, we have $\{02\}\cdot\{87\} = (0000\ 1110) \oplus (0001\ 1011) = (0001\ 0101)$ and $\{03\}\cdot\{6E\} = \{6E\} \oplus (\{02\}\cdot\{6E\}) = (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$. Then,

$$\begin{array}{lcl} \{02\}\cdot\{87\} & = & 0001\ 0101 \\ \{03\}\cdot\{6E\} & = & 1011\ 0010 \\ \{46\} & = & 0100\ 0110 \\ \{A6\} & = & \underline{1010\ 0110} \\ & & 0100\ 0111 = \{47\} \end{array}$$

The other equations can be similarly verified.

The **inverse mix column transformation**, called InvMixColumns, is defined by the following matrix multiplication:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} \quad \textbf{(5.5)}$$

	It is not immediately clear that Equation (5.5) is the **inverse** of Equation (5.3). We need to show $$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$ which is equivalent to showing $$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \textbf{(5.6)}$$ That is, the inverse transformation matrix times the forward transformation matrix equals the identity matrix. To verify the first column of Equation (5.6), we need to show $$\begin{aligned} (\{0E\} \cdot \{02\}) \oplus \{0B\} \oplus \{0D\} \oplus (\{09\} \cdot \{03\}) &= \{01\} \\ (\{09\} \cdot \{02\}) \oplus \{0E\} \oplus \{0B\} \oplus (\{0D\} \cdot \{03\}) &= \{00\} \\ (\{0D\} \cdot \{02\}) \oplus \{09\} \oplus \{0E\} \oplus (\{0B\} \cdot \{03\}) &= \{00\} \\ (\{0B\} \cdot \{02\}) \oplus \{0D\} \oplus \{09\} \oplus (\{0E\} \cdot \{03\}) &= \{00\} \end{aligned}$$ For the first equation, we have $\{0E\} \cdot \{02\} = 00011100$ and $\{09\} \cdot \{03\} = \{09\} \oplus (\{09\} \cdot \{02\}) = 00001001 \oplus 00010010 = 00011011$. Then $$\begin{aligned} \{0E\} \cdot \{02\} &= 00011100 \\ \{0B\} &= 00001011 \\ \{0D\} &= 00001101 \\ \{09\} \cdot \{03\} &= \underline{00011011} \\ & 00000001 \end{aligned}$$ The other equations can be similarly verified.	
3.	a) What are groups? With an example explain the group axioms. b) Define abelian group and cyclic group **a) GROUP:** 1. A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms). It is denoted as **{*G*, • }** 2. A commutative group is also called abelian group. Abelian group is a group in which the operator satisfies the four properties for group plus an extra property i.e. commutativity property. 3. The 4 properties plus commutativity are defined as follows: **(A1) Closure:** If a and b belong to G, then $a \cdot b$ is also in G. **(A2) Associative:** $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G. **(A3) Identity element:** There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G. **(A4) Inverse element:** For each a in G, there is an element a' in G such that $a \cdot a' = a' \cdot a = e$.	10M

Let N_n denote a set of n distinct symbols that, for convenience, we represent as $\{1, 2, \ldots, n\}$. A **permutation** of n distinct symbols is a one-to-one mapping from N_n to N_n.[5] Define S_n to be the set of all permutations of n distinct symbols. Each element of S_n is represented by a permutation of the integers π in $1, 2, \ldots, n$. It is easy to demonstrate that S_n is a group:

A1: If $(\pi, \rho \in S_n)$, then the composite mapping $\pi \cdot \rho$ is formed by permuting the elements of ρ according to the permutation π. For example, $\{3, 2, 1\} \cdot \{1, 3, 2\} = \{2, 3, 1\}$. Clearly, $\pi \cdot \rho \in S_n$.

A2: The composition of mappings is also easily seen to be associative.

A3: The identity mapping is the permutation that does not alter the order of the n elements. For S_n, the identity element is $\{1, 2, \ldots, n\}$.

A4: For any $\pi \in S_n$, the mapping that undoes the permutation defined by π is the inverse element for π. There will always be such an inverse. For example $\{2, 3, 1\} \cdot \{3, 1, 2\} = \{1, 2, 3\}$.

b) Abelian Group:

If a group has a finite number of elements, it is referred to as a finite group, and the order of the group is equal to the number of elements in the group. Otherwise, the group is an infinite group.
A group is said to be abelian if it satisfies the following additional condition:

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

The set of integers (positive, negative, and 0) under addition is an abelian group. The set of nonzero real numbers under multiplication is an abelian group. The set S_n from the preceding example is a group but not an abelian group for $n > 2$.

Cyclic Group

CYCLIC GROUP We define exponentiation within a group as a repeated application of the group operator, so that $a^3 = a \cdot a \cdot a$. Furthermore, we define $a^0 = e$ as the identity element, and $a^{-n} = (a')^n$, where a' is the inverse element of a within the group. A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.

The additive group of integers is an infinite cyclic group generated by the element 1. In this case, powers are interpreted additively, so that n is the nth power of 1.

4. For the group $G = \langle Z11 + , \times \rangle$

(i)Find the primitive roots in the group (ii)Show that the group is cyclic. (iii) Make a table of discrete logarithms

10M

Ans: For a given No, *p=11*, we define the finite field of order *11*, GF(*11*), as the set $Z_{11}$of integers {0,1,2,3,4,5,6,7,8,9,10}

(i)Find the primitive roots in the group

(ii)Show that the group is cyclic

The order of the group is 10 as the elements are {1,2,3,4,5,6,7,8,9,10}.

The generators are: 2, 6, 7 and 8

$1^0 \ mod \ 11 = 1$

$2^0 \ mod \ 11 = 1$
$2^1 \ mod \ 11 = 2$
$2^2 \ mod \ 11 = 4$
$2^3 \ mod \ 11 = 8$
$2^4 \ mod \ 11 = 5$
$2^5 \ mod \ 11 = 10$
$2^6 \ mod \ 11 = 9$
$2^7 \ mod \ 11 = 7$
$2^8 \ mod \ 11 = 3$
$2^9 \ mod \ 11 = 6$
$2^{10} \ mod \ 11 = 1$

$6^0 \ mod \ 11 = 1$
$6^1 \ mod \ 11 = 6$
$6^2 \ mod \ 11 = 3$
$6^3 \ mod \ 11 = 7$
$6^4 \ mod \ 11 = 9$
$6^5 \ mod \ 11 = 10$
$6^6 \ mod \ 11 = 5$
$6^7 \ mod \ 11 = 8$
$6^8 \ mod \ 11 = 4$
$6^9 mod \ 11 = 2$
$6^{10} \ mod \ 11 = 1$

$8^0 \ mod \ 11 = 1$
$8^1 \ mod \ 11 = 8$
$8^2 \ mod \ 11 = 9$
$8^3 \ mod \ 11 = 6$
$8^4 \ mod \ 11 = 4$
$8^5 \ mod \ 11 = 10$
$8^6 \ mod \ 11 = 3$
$8^7 \ mod \ 11 = 2$
$8^8 \ mod \ 11 = 5$
$8^9 \ mod \ 11 = 7$
$8^{10} \ mod \ 11 = 1$

$3^0 \ mod \ 11 = 1$
$3^1 \ mod \ 11 = 3$
$3^2 \ mod \ 11 = 9$
$3^3 \ mod \ 11 = 5$
$3^4 \ mod \ 11 = 4$
$3^5 \ mod \ 11 = 1$

$4^0 \ mod \ 11 = 1$
$4^1 \ mod \ 11 = 4$
$4^2 \ mod \ 11 = 5$
$4^3 \ mod \ 11 = 9$
$4^4 \ mod \ 11 = 3$
$4^5 \ mod \ 11 = 1$

$5^0 \ mod \ 11 = 1$
$5^1 \ mod \ 11 = 5$
$5^2 \ mod \ 11 = 3$
$5^3 \ mod \ 11 = 4$
$5^4 \ mod \ 11 = 9$
$5^5 \ mod \ 11 = 1$

$7^0 \ mod \ 11 = 1$
$7^1 \ mod \ 11 = 7$
$7^2 \ mod \ 11 = 5$
$7^3 \ mod \ 11 = 2$
$7^4 \ mod \ 11 = 3$
$7^5 \ mod \ 11 = 10$
$7^6 \ mod \ 11 = 4$
$7^7 \ mod \ 11 = 6$
$7^8 \ mod \ 11 = 9$
$7^9 \ mod \ 11 = 8$
$7^{10} \ mod \ 11 = 1$

$9^0 mod \ 11 = 1$
$9^1 \ mod \ 11 = 9$
$9^2 \ mod \ 11 = 4$
$9^3 \ mod \ 11 = 3$
$9^4 \ mod \ 11 = 5$
$9^5 \ mod \ 11 = 1$

$10^0 \ mod \ 11 = 1$
$10^1 \ mod \ 11 = 10$
$10^2 \ mod \ 11 = 1$

Since a^i mod $11 \in Z_{11}$ for all a and i $\in Z_{11}$ the group is cyclic.

(iii) Make a table of discrete logarithms

The discrete logarithm table is:

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

A	1	2	3	4	5	6	7	8	9	10
$b = \text{dlog}_{2,11}(a)$ $a \equiv 2^b \pmod{11}$	10	1	8	2	4	9	7	3	6	5

5	State and prove Fermat's Theorem. Using Fermat's theorem compute the following a) $7^{18}\ mod\ 19$ b) $456^{17}\ mod\ 17$ c) $5^{15}\ mod\ 13$ d) $3^{201}\ mod\ 11$	10M

Ans: Fermat's Theorem: $a^{p-1} \equiv 1 \pmod p$

- Consider the set of positive integers less than p: $\{1, 2, \ldots\ldots\ldots, p - 1\}$
- Let us multiply each element by $a \pmod p$
- Get the set $X = \{a \pmod p, 2a \pmod p, \ldots\ldots., (p - 1)a \pmod p\}$
- None of the elements of X is equal to zero because p does not divide a. Furthermore, the $(p - 1)$ elements of X are all positive integers with no two elements equal.
- We can conclude the X consists of the set of integers $\{1, 2, \ldots\ldots\ldots, p - 1\}$ in some order
- $a \times 2a \times \ldots.. \times (p - 1)a \equiv [(1 \times 2 \times \ldots.. \times (p - 1)] \pmod p$
- $a^{p-1}(p - 1)! \equiv (p - 1)! \pmod p$
- $a^{p-1} \equiv 1 \pmod p$, $\because (p - 1)!$ is relatively prime to p

a) $7^{18}\ mod\ 19$

$a = 7, p = 19$

$\boldsymbol{a^{p-1} = 7^{18} = 7^{16} \times 7^{2} \equiv 7 \times 11 \equiv 1 \pmod{19}}$

b) $456^{17}\ mod\ 17$

$a = 456, p = 17$

$\boldsymbol{a^{p-1} = 456^{17} = 456 \bmod 17 \equiv 14 \bmod 17}$

c) $5^{15}\ mod\ 13$

$a = 5, p = 13$

$\boldsymbol{a^{p-1} \bmod p = 1}$

$\boldsymbol{5^{12} \bmod 13 = 1}$

$\boldsymbol{5^{12} \equiv 1 \pmod{13}}$

$\boldsymbol{5^{15} = 5^{12} \times 5^{3}}$

$\boldsymbol{5^{12} \times 5^{3} \bmod 13 \equiv 1 \pmod{13} \times 5^{3}}$

$\boldsymbol{5^{15} \equiv 125 \bmod 13}$

$\boldsymbol{5^{15} \equiv 8 \pmod{13}}$

$\boldsymbol{5^{15} \bmod 13 \equiv 8}$

d) $3^{201}\ mod\ 11$

$a = 3, p = 11$

$\boldsymbol{a^{p-1} \bmod p = 1}$

$\boldsymbol{3^{11-1} \bmod 11 = 1}$

$\boldsymbol{3^{10} \bmod 11 = 1}$

$\boldsymbol{3^{10} \equiv 1 \pmod{11}}$

$\boldsymbol{(3^{10})^{20} \times 3 \pmod{11} \equiv 1 \pmod{11} \times 3}$

$\boldsymbol{3^{201} \bmod 11 \equiv 3}$

6	Perform encryption using RSA algorithm for p=5, q = 11, e = 3, m = 9.	10M

$n = pq = 5 \times 11 = 55$

$\emptyset(n) = (p-1) \times (q-1) = 4 \times 10 = 40$

$e = 3 \quad and \quad m = 9$

$ed \bmod \emptyset(n) \equiv 1 \Rightarrow d = e^{-1} \bmod \emptyset(n) \Rightarrow d = 3^{-1} \bmod 40 \Rightarrow d = -13 \bmod 40 = \mathbf{27}$

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
13	40	3	1	0	1	−13
3	3	1	0	1	− 13	40
	1	0		**−13**	40	

$PU = \{3,55\} \quad and \quad PR = \{27,55\}$

$C = M^e \bmod n \Rightarrow C = 9^3 \bmod 55 = 14$

$M = C^d \bmod n = 14^{27} \bmod 55 = 9$

$14^{27} \bmod 55$

$(27)_{10} = (11011)_2$

$1: 14 \bmod 55 = 14$

$1: (14)^2 \times 14 \bmod 55 = 49$

$0: (49)^2 \bmod 55 = 36$

$1: (36)^2 \times 14 \bmod 55 = 49$

$1: (49)^2 \times 14 \bmod 55 = 9$

7	With a neat diagram, explain public-key cryptosystem secrecy and Authentication.	10M

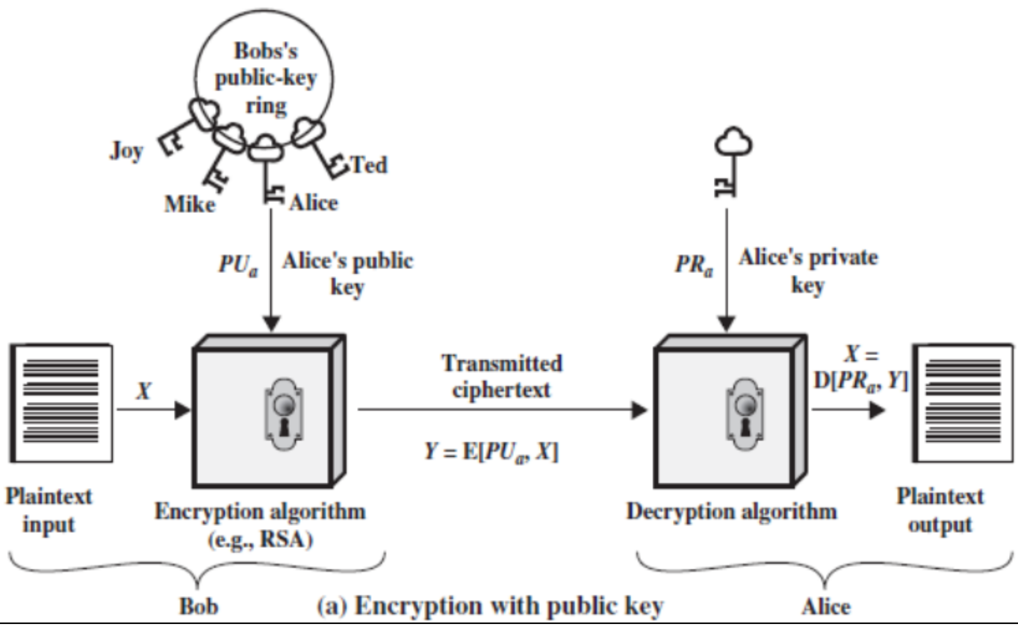
Ans:

Essential steps in public key cryptosystem:

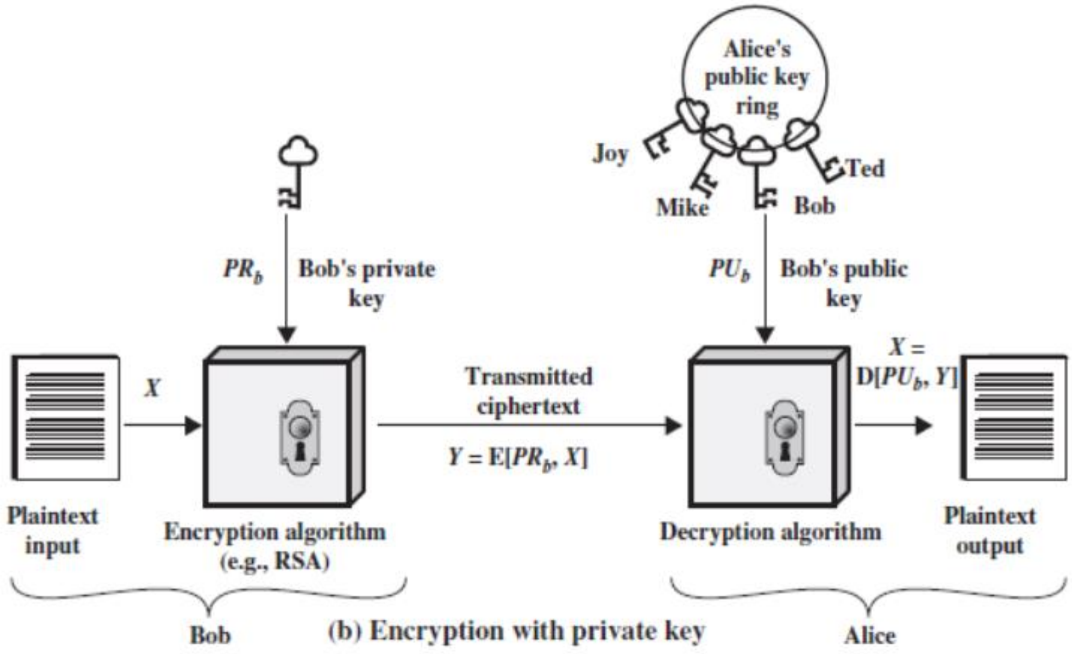
1. Each user generates a pair of key to be used for encryption and decryption.
2. Each user place one of the key in public register and other one is kept private. Each user maintains a collection of public keys obtained from others.
3. If Bob wants to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, it decrypts the message using its private key.
5. As long as the user's private key is protected the communication is secure. At any time a system can change its private key and publish the companion public key to replace its old public key
6. The key used in symmetric key is named as secret key and the 2 keys used in public key cryptography are named as public key and private key.

$Notation\ Used\!: \ K_a = Secret\ key\ of\ sender\ 'A'$

$PU_a = Public\ key\ of\ sender\ 'A' \qquad PR_a = Private\ key\ of\ sender\ 'A'$



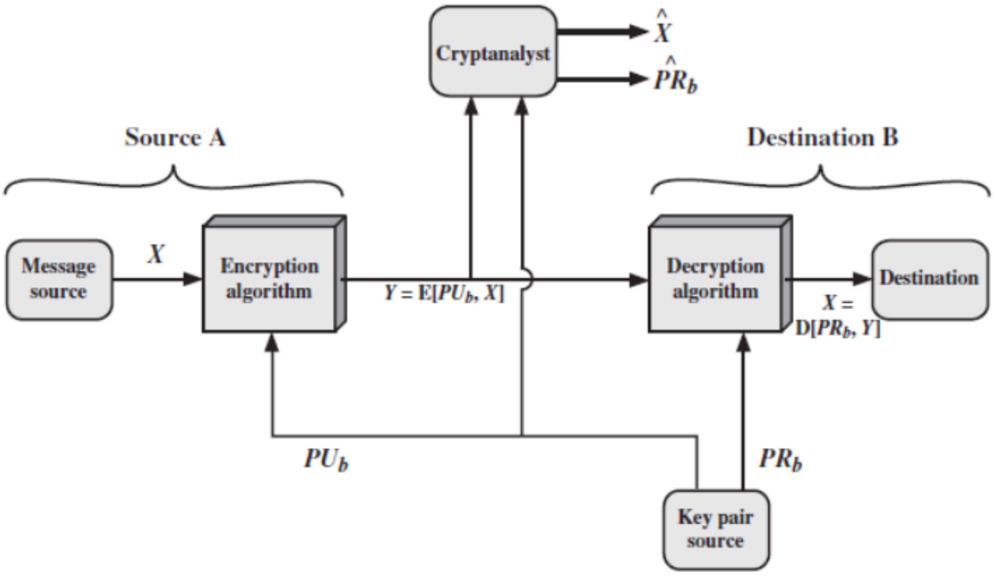
(a) Encryption with public key



(b) Encryption with private key

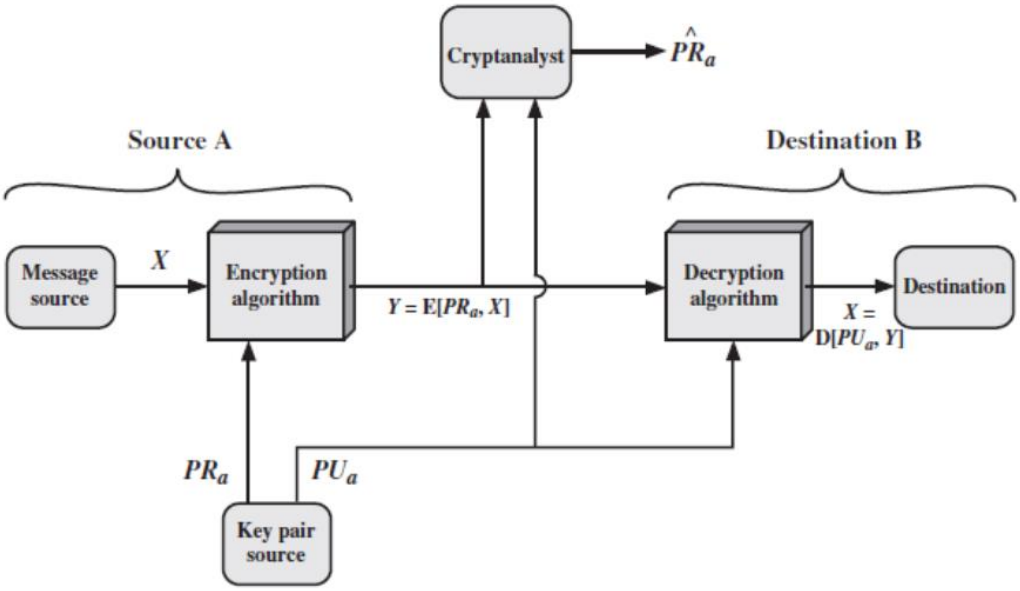
Public Key Cryptosystem-Secrecy:

1. Source 'A' sends the plaintext $X = [X1, X2, \ldots \ldots Xm]$. The m element of X is some alphabet in
the message.
2. As the message is intended for user 'B' , 'B' generates 2 keys
a) Private Key (PRb)
b) Public Key (PUb) and PUb is publicly available so that it is accessible by A.
3. With the message X and encryption key PUb, sender forms the cipher text
$Y = [Y1, Y2, \ldots \ldots N]$ $where Y = E(PUb, X)$
4. At the receiver, the intended receiver matches the key and find the message
$X = (PRb, Y)$
5. It is assumed that the cryptanalysts have the knowledge of encryption (E) and decryption (D) algorithms. If the cryptanalyst is interested only in this particular message, then its focus
is to recover X, by generating a plaintext estimate X. But if Cryptanalyst is interested in being
able to read future message as well, it will try to recover PRb, by generating an estimate $PR\hat{}b$.
6. Either of the 2 keys can be used for encryption, with other being used for decryption. This
above scheme provides confidentiality.
7. As anybody can encrypt the message using $B's$ public key and claim to be came from $'A'$



Public-Key Cryptosystem: Secrecy

Public Key Cryptosystem-Authentication:



Public-Key Cryptosystem: Authentication

If $'A'$ wants to communicate to $'B'$, then $'A'$ encrypt the message using $A's$private key.
2. $'B'$ can decrypt the message using $A's$public key.
3. As message was encrypted using $A's$private key, only $'A'$ could prepare the message. This entire message serves as a digital signature.
4. It is important to alter the message without access to $A's$private key. So this message is authenticated both in terms of source and data integrity.
5. The encryption and decryption can be represented as :
$Y = E(PRa, X)$
$X = D(PUa, Y)$
6. This public key encryption doesn't provide confidentiality because all will have $A's$public key hence can decrypt the message easily.
7. It is safe from alteration but not from eavesdropping.

8	a) Define Euler's Totient function $\phi\ (n)$. Determine $\phi\ (10)\ and\ (97)$. b) If m and n are co-prime numbers the $\phi\ (mn)$=$\phi(m)\phi(n)$. Using this property find(231), $\phi(440)$. a) Define Euler's Totient function (n). Determine $(10)\ and\ (97)$.	10M

Euler's Totient Function

Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as **Euler's totient function**, written $\phi(n)$, and defined as the number of positive integers less than n and relatively prime to n. By convention, $\phi(1) = 1$.

$\phi\,(10)$=?

Set 10 = {1,2,3,4,5,6,7,8,9,10}

For ϕ (10) Set 10 = {1, 3,7,9}

$\phi\,(10) = 4$

or

$\phi\,(10) = \phi\,(5) \times \phi\,(2)$

$= (5\text{-}1) \times (2\text{-}1)$, Since 5 & 2 are prime numbers

$= 4 \times 1$

$\phi\,(10) = 4$

$\phi\,(97) = 97\text{-}1$, Since 97 is a prime numbers

$= 96$

b) If m and n are co-prime numbers the $\phi\,(mn)$=$\phi(m)\phi(n)$.

Using this property find (231), $\phi(440)$.

$\phi\,(231)$= ?

$231 = 11\times 7\times 3$

$\phi\,(231) = \phi\,(11) \times \phi\,(7) \times \phi\,(3)$

$= (11\text{-}1) \times (7\text{-}1) \times (3\text{-}1)$

$= 10\times 6\times 2$

$\phi\,(231) = 120$

$\phi\,(440)$= ?

$440 = 11\times 5\times 2\times 2\times 2$

$= 11\times 5\times 2^3$

$\phi\,(440) = \phi\,(11) \times \phi\,(5) \times \phi\,(2^3)$

$= (11\text{-}1) \times (5\text{-}1) \times (2^3\text{-}2^2)$

$= 10\times 4\times 4$

$\phi\,(231) = 160$