Assignment- 4

Q1. Encrypt and decrypt a message "network" using RSA algorithm.

Ans: Let p=5 and q=17 are two prime numbers.

Thus, n=p*q=5*17=85 and

m=(p 1)*(q-1)=(5-1)*(17-1)=64

tus we get e=5 after calculation such that e and m are relatively prime.

Thus, d=13.

Encryption and Decryption is as shown in the table below:

Letters	P	P^e	C=P^e mod n(encryption	C^d	P=C^d mod (n)[Decryption]	Letters
N	14	537824	29	1.0261E+19	14	N
E	5	3125	65	3.6972E+23	5	E
T	20	3200000	5	1220703125	20	T
W	23	6436343	58	8.4055E+22	23	W
O	15	759375	70	9.6889E+23	15	O
R	18	1889568	18	2.0823E+16	18	R
K	11	161051	61	1.6192E+23	11	K

Q2. Explain RSA algorithm with example.

Ans: RSA is named for its inventors Rivest, Shamir, and Adleman (RSA) and it uses two numbers, e and d, as the public and private keys. The operation of RSA is described below with Example: Selecting Keys.

Bob uses the following steps to select the private and public keys:

1. Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.

2. Bob multiplies the above two primes to find n, the modulus for encryption and decryption. In other words, n ::: p X q.

3. Bob calculates another number ::: (p -1) X (q - 1).

4. Bob chooses a random integer e. He then calculates d so that d x e::: 1 mod .

5. Bob announces e and n to the public; he keeps and d secret.

Example:

Generating public key:

Select two prime no's. Suppose P = 3 and Q = 11.

Now First part of the Public key : n = P*Q = 33

We also need a small exponent say e :

But e Must be An integer.

Not be a factor of n.

$1 < e < \Phi(n)$ [$\Phi(n)$ is discussed below],

Let us now consider it to be equal to 3.

Public key(33,3)

Generating private key:

We need to calculate $\Phi(n)$:

Such that $\Phi(n) = (P-1)(Q-1)$

so, $\Phi(n) = 20$

Now calculate Private Key, d :

$d = (k*\Phi(n) + 1) / e$ for some integer k

For k = 1, value of d is 7.

Private key: (33,7)

Now if we encrypt number AE

Convert letters to numbers : A = 1 and E = 5

Thus Encrypted Data $c = 15^e \bmod n$.

Thus our Encrypted Data comes out to be 9

Now we will decrypt 9

Decrypted Data = $c^d \bmod n$.

Thus our Encrypted Data comes out to be 15

1 = A and 5 = E i.e. "AE"

Q3. Write down the steps involved in RSA algorithm. Encrypt and decrypt the message "encrypt" using RSA algorithm.

Ans:RSA is named for its inventors Rivest, Shamir, and Adleman (RSA) and it uses two numbers, e and d, as the public and private keys.

The operation of RSA is described below: Selecting Keys:
1.We use the following steps to select the private and public keys:

2.We choose two very large prime numbers p and q since a prime number is one that can be divided evenly only by 1 and itself.

3.We multiply the above two primes to find n, the modulus for encryption and decryption. In other words, n: p X q. We calculate another number: (p - 1) X (q - 1).

4.We choose a random integer e and then calculates d so that d x e: 1

mod 5. We announce e and n to the public but keep s and d a secret.

Here,

Let p=3 and q=23 are two prime numbers. Thus,

n=p*q=3*23=69 and m=(p -1)*(q-1)=(3-1)*(23-1)=44
we get e=3 such that e and m are relatively prime.

Thus, d=15.

Encryption and Decryption is as shown in the table below:

Letters	P	P^e	C=P^e mod n(encryption	C^d	P=C^d mod (n)[Decryption]	Letters
E	5	125	56	1.6704E+26	5	E
N	14	2744	53	7.31372E+25	14	N
C	3	27	27	2.95431E+21	3	C
R	18	5832	36	2.21074E+23	18	R
Y	25	15625	31	2.34653E+22	25	Y
P	16	4096	25	9.31323E+20	16	P
T	20	8000	65	1.56207E+27	20	T

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message .