Assignment- 4

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

=>

Let p=3 and q=11 are two prime numbers.

Thus, n=p\*q=3\*11=33 and m=(p-1)\*(q-1)=(3-1)\*(11-1)=20 Let e=3 such that e and m are relatively prime.

Thus, d=7.

Encryption and Decryption is as shown in the table below:

| Letter s | P | Pe | C=Pe mod  Cd P=Cd mod  (n)  (n)  [Encryptio  [Dencrypt  n]  ion] | Lette  rs |
| --- | --- | --- | --- | --- |
| N | 14 | 2744 | 5 78125 14 | N |
| E | 5 | 125 | 26 8031810176 5 | E |
| T | 20 | 8000 | 14 105413504 20 | T |
| W | 23 | 12167 | 23 3404825447 23 | W |

O 15 3375 9 4782969 15 O R 18 5832 24 4586471424 18 R K 11 1331 11 19487171 11 K

Q2. Explain RSA algorithm with example.

=>

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 RS A i s described below with Example:

Selecting Keys

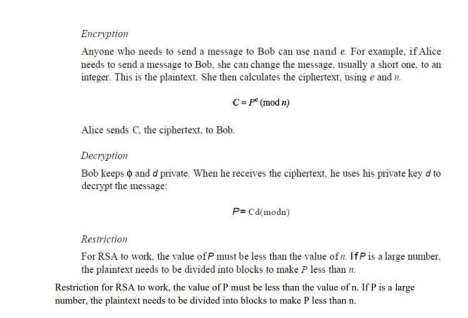
Bob uses the following steps to select the private and public keys:

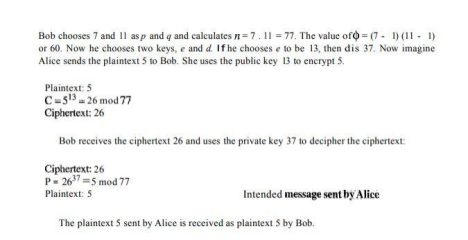
1. Bob chooses two very large prime numbers p and q. Remember that a prime number is one that can be divided evenly only by 1 and itself.

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 <1> ::: (p -1) X (q - 1). 4. Bob chooses a random integer e. He then calculates d so that d x e::: 1 mod <1>.

5. Bob announces e and n to the public; he keeps <1> and d secret.



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

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 RS A i s 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=11 are two prime numbers.

Thus, n=p\*q=3\*11=33 and m=(p-1)\*(q-1)=(3-1)\*(11-1)=20 Let e=3 such that e and m are relatively prime.

Thus, d=7.

Encryption and Decryption is as shown in the table below:

| Letter s | P | Pe | C=Pe mod  Cd P=Cd mod  (n)  (n)  [Encryptio  [Dencrypt  n]  ion] | Lette  rs |
| --- | --- | --- | --- | --- |
| E | 5 | 125 | 26 8031810176 5 | E |
| N | 14 | 2744 | 5 78125 14 | N |
| C | 3 | 27 | 27 1046035320 3 | C |
| R | 18 | 5832 | 24 4586471424 18 | R |
| Y  P  T | 25  16  20 | 15625  4096  8000 | 16 268435456 25  4 16384 16  14 105413504 20 | Y  P  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

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption

Rivest, Shamir, and Adleman (RSA) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator. It uses two numbers, e and d, as the public and private keys 1. Choose two different large random prime numbers p and q 2. Calculate n = pq o n is the modulus for the public key and the private keys 3. Calculate the totient: Φ(n) = (p-1)(q-1) 4. Choose �� an integer such that 1< �� < Φ(n), �� is co − prime to Φ(n) i.e.: �� ������ Φ(n) share no factors other than 1; gcd (�� , Φ(n) ) = 1. o �� is released as the public key exponent 5. Simply to say : Calculate d = 1+x Φ(n))/ �� to be integer o d is kept as the private key exponent Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax − C = Pe mod n The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as − Plaintext = Cd mod n