**NATIONAL INSTITUTE OF TECHNOLOGY DELHI**

**Department of Computer Science & Engineering**

**CSB451 – Network Security & Cryptography**

***Assignment – 8***

**Submitted By:**

**Himanshu Verma 201210023**

**Submitted To: Dr. Karan Verma**

**Question- 1**

**Solution:**

P = 61 and Q = 53.

A)     Choose a third integer E, such that E > 1, E < PQ, and E and (P-1) \* (Q-1) are relatively prime. This is extremely simple with the aid of a computer, but otherwise, you can use the Euclidean algorithm to make sure that the GCD of E and (P-1) (Q-1) is 1. In this instance, (P-1) (Q-1) is 3120. A suitable E is 17.

B) Compute D, such that DE = 1 mod (P-1) (Q-1). In this example, we want to solve 17E = 1 mod 3120. This can be solved as a linear congruence by hand, or a computer can be used to find a suitable value. One possible value for D in this case, is 2753.

At this point, all the values needed have been generated, to define the encryption algorithm, and the decryption algorithm.

The encryption algorithm is defined as C = (T^E) mod PQ. C is the “ciphertext”, which will be some positive integer. Words and phrases are typically broken into manageable sizes and converted into some numerical representation. Let’s pretend that the number “123” is representative of some letter. Thus, we let T = 123, and the encryption algorithm then produces (123 ^ 17) mod (3233), which can be deduced to be 855.

In general, the value of (PQ) and E are published openly, while the individual values of P, Q, and D are kept secret. This way, anybody can use the known values of PQ and E to send encrypted messages, but only the creator of these values can decipher these messages.

To decrypt the message, one must simply solve T = (C^D) mod PQ. So, to decrypt 855, solve (855^2753) mod 3233. The solution to this, as expected, is 123, the original number.

**Question- 2**

**Solution:**

p = 93, q=47, e= 21

n = pq = 93x47 = 4371,

m=(p-1)(q-1) = 92x46 = 4232

e=21 encryption exponent

public key = (21, 4371)

we calculate the decryption exponent d using euclid’s algorithm as given below

4232 = 21 (201) + 11 11 = 4232 – 21(201)

21 = 11 (1) + 10 10 = 21 – 11(1)

11 = 10 (1) + 1 1 = 11 – 10(1)

10 = 1(10) + 0

1 = 11 – 10(1)

1 = 11 – [21-11(1)](1)

1 = 11(2) – 21(1)

1 = [4232-21(201)](2) – 21(1)

1 = 4232(2) – 21(403)

1 = 4232(2) + 21(-403)

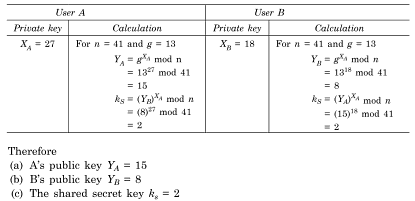
Multiplicative inverse of 21 is -403 = 3829

Therefore, decryption exponent d = 3829

Private key = (3829, 4371)

**Question- 3**

**Solution:**



**Question- 4**

**Solution:**

Formulas to generate public keys:

X\*A = gXa mod n

X\*B = gXb mod n

Given g = 11 and n = 93,

1. YA = 115 mod 93 = **68**
2. YB = 1112 mod 93 = **16**
3. Formula to generate Shared Keys:

KA = YBXA mod n

KB = YAXB mod n

Putting the values:

KA = 165 mod 93 = **1**

KB = 6812 mod 93 = **1, Hence the Shared Key is 1.**