Lecture No - 17

* Public key Cryptography
* RSA Algorithm
* Problems on RSA Algorithm

1. Public key Cryptography

In Asymmetric Key Cryptography or Public Key Cryptography, 2 different keys are used.

One key is used for encryption and only the other corresponding key must be used for decryption.

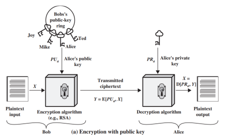
No other key can decrypt the message - NOT EVEN THE ORIGINAL KEY USED FOR ENCRYPTION.

Every communicating parties need to have just a key pair to communicate with any number of other communicating parties.

Once someone obtains a key-pair, he/she can communicate with each other.

Suppose A wants to send a message to B without having to worry about its security. Then A and B should each have a private key and a public key.

. A should keep her private key secret
. B should keep her private key secret
. A should inform B about her public key
. B should inform A about her public key



2. RSA Algorithm

The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm. The RSA scheme is a cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n. A typical size for n is 1024 bits.

The RSA Algorithm can be summarised as follows:

1. Select two prime numbers p and q , for example p = 17 and q = 11.
2. Calculate n = pq = 17 * 11 = 187.
3. Calculate Φ(n) = (p - 1)(q - 1) = 16 * 10 = 160.
4. Select e such that e is relatively prime to Φ(n) = 160 and less than Φ(n); we choose e = 7.
5. Determine d such that d.e ≡ 1 (mod Φ(n)) and d < 160. $(d \times e) \bmod \phi(n) \equiv 1$

The correct value is
d = 23, because 23 * 7 = 161 = (1 * 160) + 1; d can be calculated using the extended Euclid's algorithm

6. This gives us a pair of keys.

Public Key , PU = (e,n) = (7,187)

Private Key , PR =(d,n) = (23, 187).

7. FOR ENCRYPTION:

CT= (PT)^e mod n

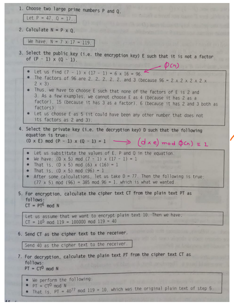
8. FOR DECRYPTION:

PT = (CT)^d mod n

9. FOR EXAMPLE:

For PT = 88, CT= ???

3. Problems on RSA Algorithm



1. Choose two large prime numbers P and Q.

   Let P = 47, Q = 17.

2. Calculate N = P x Q.

   We have, N = 7 x 17 = 119.

3. Select the public key (i.e. the encryption key) E such that it is not a factor of (P - 1) x (Q - 1).
   * Let us find (7 - 1) x (17 - 1) = 6 x 16 = 96. ← $\phi(n)$
   * The factors of 96 are 2, 2, 2, 2, 2, and 3 (because 96 = 2 x 2 x 2 x 2 x 2 x 3).
   * Thus, we have to choose E such that none of the factors of E is 2 and 3. As a few examples, we cannot choose E as 4 (because it has 2 as a factor), 15 (because it has 3 as a factor), 6 (because it has 2 and 3 both as factors).
   * Let us choose E as 5 (it could have been any other number that does not its factors as 2 and 3).
4. Select the private key (i.e. the decryption key) D such that the following equation is true:
   (D x E) mod (P - 1) x (Q - 1) = 1 → $(d \times e) \bmod \phi(n) \equiv 1$
   * Let us substitute the values of E, P and Q in the equation.
   * We have: (D x 5) mod (7 - 1) x (17 - 1) = 1
   * That is, (D x 5) mod (6) x (16) = 1
   * That is, (D x 5) mod (96) = 1
   * After some calculations, let us take D = 77. Then the following is true: (77 x 5) mod (96) = 385 mod 96 = 1, which is what we wanted.
5. For encryption, calculate the cipher text CT from the plain text PT as follows:
   $CT = PT^E \bmod N$

   Let us assume that we want to encrypt plain text 10. Then we have,
   $CT = 10^5 \bmod 119 = 100000 \bmod 119 = 40$
6. Send CT as the cipher text to the receiver.

   Send 40 as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as follows:
   $PT = CT^D \bmod N$
   * We perform the following:
   * $PT = CT^D \bmod N$
   * That is, $PT = 40^{77} \bmod 119 = 10$, which was the original plain text of step 5.

By Extended Euclidean Algorithm

$$ax + by = GCD(a, b)$$

Where,

$a = \phi(n) = 96$

$b = e = 5$

∴ The equation reduces to

$$96x + 5y = GCD(96, 5)$$

We need to solve this equation for the value of y. $y \Rightarrow d$

4. We can solve for 'd' using the following table

Row	a	b	d	k
1	1	0	96	—
2	0	1	5	19
3	1	−19	1	5

$a_3 = a_1 - (a_2 k_2)$

$\Rightarrow 1 - (0 \times 19)$

Just stop calculations once you get 1 in the d column.

Now put the above values in th eq:–

$$\phi x + ey = gcd(\phi, e)$$

$\Rightarrow 96(1) - 5(19) = gcd(96, 5)$

$\Rightarrow 96 - 95 \Rightarrow 1 = gcd(96, 5) = 1$

Hence LHS = RHS

But as value of 'd' is negative, we need to perform some corrections,

i.e if d is -ve

$d = d + \phi(n)$

$d = -19 + 96$

$= 77$

$\boxed{\text{Hence } d = 77}$

Q.1: p=7, q= 11, e=13 , PT= 17

Calculate CT.

Q.2: p= 7 , q=17 , M= 6

Q.3: p=3 , q= 11, e= 7, M=12

Q.4: p= 7, q= 11 , e= 17, M=25

Q.5: For the given parameters P= 3 & Q = 19, find the value of 'e' & 'd' using RSA algorithm & encrypt the message M= 6