Jessica Braganza
BE comp 2
F17112151

PAGE NO:
DATE:

ICS Assignment 6

1) Explain in brief working of RSA Algorithm

Ans. The RSA Algorithm is an asymmetric cryptography algorithm, this means that it uses a public key and a private key (i.e. two different mathematically linked keys).

- Following steps highlight the working of RSA Algorithm.

1) Generating the keys

- Select two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out.
- Calculate $n = x * y$
- Calculate the totient function: $\phi(n) = (x-1)(y-1)$
- Select an integer e, such that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) makes up the public key.
- Calculate d such that $e, d = 1 \bmod \phi(n)$. d can be found using the extended euclidean algorithm. The pair (n, d) makes up the private key.

2) Encryption

- Given a plaintext P, represented as a number, the ciphertext C is calculated as: $C = P^2 \bmod n$.

3) Decryption:

- Using the private key (n, d), the plaintext can be found using: $P = C^d \bmod n$

2) Give mathematical importance of Euler's Totient function.

Ans - Euler's totient function counts the positive integers upto a given integer n that are relatively prime to n. It is written using Greek letter phi as $\phi(n)$.

- It is the number of integers k in the range $1 \le k \le n$ for which the greatest common divisor gcd(n, k) is equal to 1.
- The integers k of this form are sometimes referred to as totatives of n.
- It is a multiplicative function, meaning that if two numbers m and n are relatively prime, then $\phi(mn) = \phi(m) \cdot \phi(n)$.
- This function gives the order of the multiplicative group of integers modulo n.

3) Perform encryption and decryption using the RSA algorithm, for the following : p = 3, q = 11, e = 7, M = 5

$n = p * q = 3 * 11 = 33$

$f(n) = (p-1)(q-1) = 2 * 10 = 20$

Now, we need to compute $d = e^{-1} \bmod f(n)$ by using backward substitution of GCD algorithm:

According to GCD :

$20 = 7 * 2 + 6$

$7 = 6 * 1 + 1$

$6 = 1 * 6 + 0$

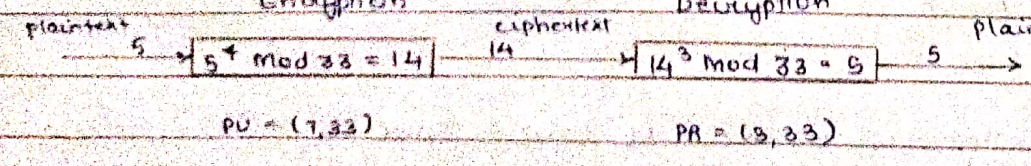
Therefore, we have,

$1 = 7 - 6 = 7 - (20 - 7 * 2) = 7 - 20 + 7 * 2 = -20 + 7 * 3$

Hence, we get $d = e^{-1} \bmod f(n) = e^{-1} \bmod 20 = 3 \bmod 20 = 3$

So the public key is {7, 33} and the private key is {3, 33}

RSA encryption and decryption is as follows :



4) What is one-way function in RSA cryptosystem ?

Ans - One-way function is a function that is easy to compute but

computationally hard to reverse.

1. Easy to calculate $f(x)$ from x.
2. Hard to invert : to calculate x from $f(x)$.

- There is no proof that one-way functions exist or even real evidence that they can be constructed.
- Even so, there are examples that seem one way, they are easy to compute but we know of no easy way to reverse them, for example, x^2 is easy to compute but $x^{1/2}$ is not.
- One way functions are used in pseudorandom generators.

Q) What is trapdoor in RSA?

Ans. - Trapdoor one-way functions are types of one-way functions that contain a kind of "back door" (trapdoor)

- As in the case of ordinary one-way functions it is easy to compute their values for given data but it is very difficult to compute their inverse functions.
- However, if one has some additional secret information, he/she can easily compute the inverse function as well.
- A trapdoor one-way function is easy to compute but computationally hard to reverse.

1. Easy to calculate $(x^e \bmod n)$ from x.
2. Hard to invert : to calculate x from $(x^e \bmod n)$

- Examples of such trapdoor one-way functions may be finding the prime factors of large numbers.