Sudesh Pawar
BE Comp A
F1711037(24)

ICS A6

Q1) Explain in brief working of RSA algorithm.

Ans. RSA is based on finding prime factors for very large numbers. The length of no. that we are referring to here is around 500 Digits.

RSA Key length	No. of Digits.
1024 bit	309
2048 bit	617
4096 bit	1233

Steps:

1) Choose 2 randomly large prime nos. p and q.
2) Multiply numbers = $n = p \times q$.
3) Choose random integer to be encryption key e such that e & $(p-1)(q-1)$ are relatively prime
4) Decryption key is computed as
$$d = e^{-1} \bmod [(p-1) * (q-1)]$$
5) Public Key = (n, e)
6) Private Key = (n, d)
7) For encryption message M with public key (n, e), you get ciphertext $C = M^e \bmod n$.
8) For decrypting ciphertext, with private key (n, d), you get plaintext $M = c^d \bmod n$.

Q.2) Perform encryption & decryption using RSA algorithm for the following:
$p = 3, q = 11, e = 7, M = 5$.

Ans. $n = p \times q$, $3 \times 11 = 33$
$r = (p-1)(q-1) = 2 \times 10 = 20$
$d = e^{-1} \bmod r$.
$ed = 1 \bmod 20$
$fd = 1 \bmod 20$

For $d=3$, we get,

$7 \times 3 = 1 \bmod 20$.

Hence, value of decrypting key, $d = 3$

As per RSA, $C = M^e \bmod n$

$= 5^7 \bmod 33$

$C = 14$

$M = C^d \bmod n$

$= 14^3 \bmod 33$

$= 5$

Q.3) Give mathematical importance of Euler's Totient function.

Ans. In number theory, Euler's totient function counts the positive integers up to a given integer n that are primeton

- Euler's totient function 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 integer modulo n.
- It is also used for defining the RSA encryption system.

Q-4) What is Trapdoor in RSA.

Ans. A Trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction without special information, is called trapdoor.

Q-5) What is one-way function in RSA cryptosystem.

Ans.
- RSA is based on finding prime factors for very large no.
- The length of numbers that we are referring to here is ~~assumed~~ around 500 digits.
- A trapdoor function is a function that is easy to compute in one direction, yet difficult to compute in the opposite direction without special information.
- The public key is (n, e).
- The private key is (n, d).

where $n = p \times q$ (p & q are large prime numbers).
e is encryption key
d is decryption key.