SC205(Discrete mathematics) Project

RSA(Rivest–Shamir–Adleman)Algorithm

Name: Chaudhari Sagar B.

SID: 201901117

Instructor:Professor Manish K Gupta

1 Abstract

Here i talk about an RSA(Rivest–Shamir–Adleman) algorithm which is used for secure communications.RSA algorithm contains discrete mathematics concept.

2 Problem

The internet has revolutionised the way we shop. Customers can order goods and services without the need to leave the house but Fraudsters send out emails claiming to be from your bank. When you click on the link you are directed to a website which looks identical to the bank's real website and through they stole our private information.

3 Introduction

The RSA algorithm is the basis of a cryptosystem, a suite of cryptographic algorithms that are used for specific security services or purposes which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet.

4 An Analytical Solution

RSA encryption is a system that uses two separate kinds of key.
1)public key.
2)Private key.

RSA algorithm is as follow:
1) Take two very large prime number A an B.Product of A and B is N which is very large number.

$$N = A \times B.$$

2) Subtract 1 From A and B and get Product T.

$$T = (A - 1) \times (B - 1).$$

3) Choose a public key E randomly which doesn't have any common factors with T and obtain private key D as follows:

$$\mathrm{D} = (1/E\ ) \bmod \mathrm{T}.$$

4) The rule for encryption of plaintext M into ciphertext C is as follows:

$$\mathrm{C} = M^E \bmod \mathrm{N}.$$

5) The mod term Equation indicates that the remainder of the division is sent as the ciphertext c as shown in fig 1.

6) The receieved message C at the receiver is decrypted to obtain plaintext back by using the following rule:

$$\mathrm{M} = C^D \bmod \mathrm{N}.$$

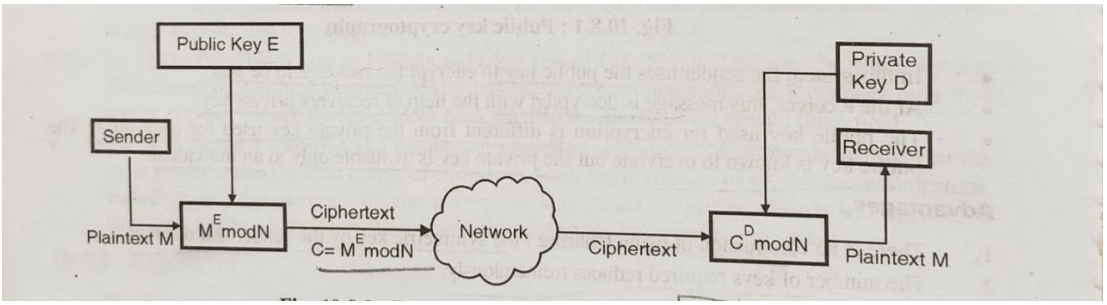

Figure 1: Encryption and Decryption in RSA

5 Security of RSA

The security of RSA is decided by the ability of the hacker computer factorize numbers.

RSA provides a very good security because it uses very large numbers A an B their product is so large that an attempt to break the code using the fastest computer will need a few years.
A key size of 768 bits is recommended for the personal use.1024 bits for the corporate use and 2048 bits for extremely valuable keys.
The user's key should be changed regularly in order to enhance security.

6 Conclusion

If we use this kind of algorithm in a security system then there is very low risk that your private information is being stolen from any site and we can buy any product from the internet without fear.

7 References

1) https://en.wikipedia.org/wiki/RSA_(cryptosystem)
2) book: data Communication and Networking(GTU) by J.S.Katre