Assignment no 10 - 04

Date : / /20

Aim - Write a Java / C / C++ / python program to implement RSA algorithm

Theory -

1] RSA of Rivest - Shamir - Adleman is an algorithm worked as encrypt and decrypt message It is an asymmetric cryptographic algorithm Asymmetric means that there are two different keys. This is also called public-key cryptography because one of the keys are often given to anyone. the other is the private key which is kept private

2] As their names suggest a public key is shared publicly while a private key is secret and must not be shared with anyone this public key will be used for the encryption and corresponding private key will be used for the decryption

3] RSA keys can be typically 1024 or 2048 bits long so that key could not be broken easily the RSA scheme is based on the fact that it is difficult to factorize a large integer

4] The integer used by this method are sufficiently large making it difficult to solve the public key generally consists of two numbers where one number is multiplication of two large prime numbers

Pooja

Date : / /20

And private key is also derived from the same two prime numbers.

5) So, if factorization of this large number is done the private key can be compromised therefore, strength of encryption totally lies on the key size and if the key size is doubled or tripled the strength of encryption increases exponentially.

Encryption -

consider a sender who sends the plain text message to someone whose public key is (n,e) calculate corresponding ciphertext as

$C = p^e \bmod n$

Decryption -

considering receiver has the private key d given a block of ciphertext C the corresponding plaintext will be calculated as

$plaintext = C^d \bmod n$

public key and private key. As the name describes that the public key is given to every one and private key is kept private the RSA algorithm is named after Ron-Rivest Adi Shamir and leonard adleman those who invented it in 1978.

Pooja

Date : / /20

Advantages of RSA

1) RSA has overcome the weakness of symmetric algorithm i.e authenticity and confidentialy

2) Asymmetric encryption algorithm are mainly used for the encryption key of the Symmetric algorithm.

disadvantages of RSA -

1) RSA has too much computation.

2) RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer.

3) It requires a third party to verify the reliability of public keys.

4) Data transferred through RSA algorithm could be compramised through middlemen who might tempee with the public key system.

5)

5) Brute force mathematical attacks timing attacks and chosen ciphertext attacks are some possible approaches to attacks RSA algorithm.

Pooja

Date : / /20

Algorithm -

① consider two prime numbers p and q
② compute $n = p * q$
③ compute $\phi(n) = (p-1) * (q-1)$
④ choose e such $gcd(e, \phi(n)) = 1$
⑤ calculate d such $e * d \bmod \phi(n) = 1$
⑥ public key $\{e, n\}$ private key $\{d, n\}$
⑦ cipher text $c = p^e \bmod n$ where p = plaintext
⑧ for decryption $p = c^d \bmod n$ where D will refund the plaintext.

Conclusion -

We learned how to implement RSA algorithm.