Robust RSA for Digital Signature

Mr.Virendra Kumar, Mr. Puran Krishen Koul

Department of Computer Science
MTU Noida
CET-IILM-AHL
Knowledge Park-2
Greater Noida
G.B.Nagar
UP 201306,India

Department of Computer Science
MTU Noida
CET-IILM-AHL
Knowledge Park-2
Greater Noida
G.B.Nagar
UP 201306,India

Abstract

The RSA cryptosystem is currently used in a wide variety of products, platforms, and industries around the world. It is found in many commercial software products and is planned to be in many more. In hardware, the RSA algorithm can be found in secure telephones, on ethernet network cards, and on smart cards.It offers encryption and digital signatures (authentication). In this paper we will illustrate the application and problem associated with RSA Algorithm.

Keywords:*RSA,Digital Signature,Cryptosystem,Public Key ,Private Key,Co-prime ,Prime Number*

1. INTRODUCTION

The RSA algorithm (1977) is widely used for public-key encryption.Developed by Ron Rivest, Adi Shamir, and Len Adleman (MIT).

The RSA digital signature has been adopted by Visa and Master Cards in the Secure Electronic Transactions (SET) standard for providing security of electronic transfers of credit and payment information over the Internet. In SET, signatures are used to provide certificates for public keys and to authenticate messages. Since public-key cryptography requires intensive computations, it is desirable to speed up these public-key computations by using either special-purpose hardware or efficient software algorithms.

2.RSA ALGORITHM:

Following steps are given below ,that are involve in RSA Algorithm.

2.1Key Generation

- Choose two distinct prime numbers, such as
- Compute $n = pq$ giving
- Compute the totient of the product as $\varphi(n) = (p - 1)(q - 1)$ giving
- Selects number e, such that $0 < e < \varphi(n)$ and e is relatively prime to $\varphi(n)$
- Compute d, where d = e^−1 mod φ(n).
- **Public key** is (n, e).
- **Private key** is (n, d).

2.2 RSA signing

S = m^d mod n ,Where **S** is the signature on m, m is the massage to be signed.

2.3 RSA verification

To verify that s is really the signer’s signature on m, we verify if m **= S^e mod n = YES or NO**
If the result is **YES** then **S** is the signer’s signature on m.

2.4 Example of RSA algorithm

We can illustrate RSA algorithm using sender (Viru) and Receiver (Puru) .Viru want to send a secure message to Puru , he perform the following steps according to the RSA Algorithm.

2.1 Key Generation

- First Viru choose two large prime numbers p and q.

Note:***Prime Number :****A number that is not divisible by any other number than itself and 1.*

$p = 61$ and $q = 53$.

- He Compute $n = pq$ giving $n = 61 \cdot 53 = 3233$.
- Then Compute(the totient) $\varphi(n) = (p - 1)(q - 1)$ giving $\varphi(3233) = (61 - 1)(53 - 1) = 3120$.

- Now he Choose any number e where $1 < e < 3120$ that is coprime to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120. Let $e = 17$.

Note:***Co- Prime:*** *Two numbers are said to be relatively prime or coprime if the only number that they are both divisible by is 1.*

- He Compute d $d = 2753$.

- The **public key** is ($n = 3233$, $e = 17$). For a padded plaintext message m, the encryption function is m^{17} (mod 3233).
- The **private key** is ($n = 3233$, $d = 2753$). For an encrypted ciphertext c, the decryption function is c^{2753} (mod 3233).

2.2 RSA Signing.

Now Viru sign the message using computed Public Key =17

For instance, in order to encrypt $m = 65$,

we calculate $S = 65^{17} \pmod{3233} = 2790$.

2.3 RSA Verification.

Now Puru receive the encrypted message and he verify the signature by decrypting the signed message using computed Private Key=275

Where **S**= 2790, we calculate

$$m = 2790^{2753} \pmod{3233} = 65.$$

Hence the value of original message (m) is=Value of decrypted message that is means **YES** Thus **S** is the signer's signature on m.

3. PROBLEM ASSOCIATED WITH RSA ALGORITHM

The RSA algorithm suffers from the following weaknesses:

3.1 Multiplicative Property

The RSA signature scheme has the following multiplicative property, sometimes referred to as the *homomorphic* property.

$$\text{If} \quad S_1 = m_1^{\,d} \bmod n$$

$$\text{and} \quad S_2 = m_2^{\,d} \bmod n$$

are the signatures on messages m1 and m2 then

$$S_1 S_2 \bmod n = (m_1 m_2)^d \bmod n$$

On getting two different signed messages from a person it would be computationally feasible to derive the person's private key (d). This is because in this case, the values of S_1, S_2, n, m_1 and m_2 are known.

3.2 Integer Factorization

If an adversary is able to factor the public modulus n of someone then the adversary can compute φ(n)(Totient) and then, using the extended Euclidean algorithm, deduce the private key d from φ(n) and the public exponent e by solving

$$ed = 1 \bmod \varphi(n)$$

This constitutes a total break of the system. To guard against this p and q must be sufficiently large numbers so that factoring n is a computationally infeasible task.
However, with the rapid enhancement in computational power of modern computers it would be difficult to guarantee the computational infeasibility of factorization of large numbers.

4. CONCLUSION

This will be disastrous for the entire public key infrastructure sought to be implemented in India with the licensing of the Certifying Authorities. A breakdown of the RSA algorithm would mean that forging of the digital signatures of a Certifying Authority would be computationally feasible. This would result in the generation of fake digital signature certificates, thus defeating the very purpose of the appointment of certifying authorities and hence a public rejection of E-commerce.

Secondly, if due to a technological or mathematical breakthrough, factorization of large numbers becomes computationally feasible, the strength of the asymmetric crypto system would be shattered.

This can be achieved by removing all references to asymmetric crypto system, hash function, public key, private key etc from the legislation. Moreover the term digital signature should be replaced by the term electronic signature and this term must have a very wide definition.

REFERENCES

[1]. Niels Ferguson and Bruce Schneier, Practical Cryptography, Wiley, 2003. IEEE P1363 Standard Specifications for Public Key Cryptography, IEEE, November.
[2]. Alfred Menezes, Paul C. Van Oorschot, Scott A. Vanstone. (October 1996), Handbook of Applied Cryptography, CRC Press.
[3]. R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystem. Communications of the ACM, 21 (2), pp. 120-126, February 1978.
[4]. Clifford Cocks, A Note on 'Non-Secret Encryption', CESG Research Report, 20 November 1973. 1993.
[5]. RSA Laboratories, PKCS #1 v2.1: RSA Encryption Standard, June 2002.
[6]. William Stalling, Book ‘Cryptography and Network Security’
[7]. D. E. Denning. Cryptography and Data Security. Addison-Wesley, Reading, MA, 1982.
[8]. T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. In *IEEE Trans. Inform. Theory*, Vol. IT-31, pp. 469-472, July, 1985
[9]. R. Gennaro, D. Katz, H. Krawczyk, T. Rabin: Secure network coding over the integers. PKC 2010.
[10]”Applied Cryptography”, Second Edition, Schneider, 1996.

AUTHORS PROFILE

1. **First Author**:**Mr.Virendra Kumar**

(Assistant Professor in CS Department),Educational Qualification :B.Tech(Computer science and Engg.) from UPTU,Lucknow,M.Tech(Computer science and Engg) from Jamia Hamdard University New Delhi), worked as Network Administrator in NIIT Lucknow,Current Employer is CET-IILM-academy of Higher Learning,Gr. Noida India,My achievements are Certification in VPN from HCL Infinate Ltd. Lucknow India, academic achievements: two books are Publised on title '*Computer Organization' &' Information Security and Cyber Law'*.Currently working on GIS based Cloud Computing.

2. **Second Author**:**Mr. Puran Krishna Kaul**

(Assistant Professor in CS Department),Educational Qualification :M.Sc(Information technology.) Sikkim M.Tech(Spl Language Technology) from Centre For Devlopment Of Advance Computing Noida NCR), worked as Software developer at CDAC for nearly 2 years Noida current employer is CET-IILM-academy of Higher Learning,Gr. Noida India,acedamic achievements: paper presented "verstality of indian information and technology act 2000".