International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A FAST AND WEINER ATTACK RESISTANT CRYPTOSYSTEM

Swati Paliwal,M.tech Student,SSSIST Sehore,India; Ravindra Gupta,Assistant Professor,Department-CSE,SSSIST Sehore,India

Abstract

The paper discusses encryption schemes such as public key algorithms (RSA) and One Time Pads. It also discusses various attacks on the RSA algorithm. A brief introduction to Modular Arithmetic, which is the core arithmetic of almost all public key algorithms, has been given. In this paper We propose a variant to the RSA algorithm which is effective in terms of speed. Also it is more secure against low decryption exponent attack. The security and the efficiency of the proposed variant have also been discussed.

Keywords

RSA, one-time pad, Wiener's attack, modular arithmetic, plaintext, ciphertext.

Introduction

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted/scrambled by any encryption algorithm using the 'key'. Only the user having the access to the same 'key' can decrypt/de-scramble the encrypted data. This method is known as private key or symmetric key cryptography. There are several standard symmetric key algorithms defined. Examples are AES, 3DES etc. These standard symmetric algorithms defined are proven to be highly secured and time tested. But the problem with these algorithms is the key exchange. The communicating parties require a shared secret, 'key', to be exchanged between them to have a secured communication. The security of the symmetric key algorithm depends on the secrecy of the key. Keys are typically hundreds of bits in length, depending on the algorithm used. Since there may be number of intermediate points between the communicating parties through which the data passes, these keys cannot exchange online in a secured manner. In a large network, where there are hundreds of system connected, offline key exchange seems too difficult and even unrealistic. This is where public key cryptography comes to help. Using public key algorithm a shared secret can be established online between communicating parties with out the need for exchanging any secret data.

In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online. In public key cryptography, keys and messages are expressed numerically and the operations are expressed mathematically. The private and public key of a device is related by the mathematical function called

ISSN:2319-7900

the one-way function. One-way functions are mathematical functions in which the forward operation can be done easily but the reverse operation is so difficult that it is practically impossible. In public key cryptography the public key is calculated using private key on the forward operation of the one-way function. Obtaining of private key from the public key is a reverse operation. If the reverse operation can be done easily, that is if the private key is obtained from the public key and other public data, then the public key algorithm for the particular key is cracked. The reverse operation gets difficult as the key size increases. The public key algorithms operate on sufficiently large numbers to make the reverse operation practically impossible and thus make the system secure. For e.g. RSA algorithm operates on large numbers of thousands of bits long.

Mathematical Background-Modular Arithmatic

Modular Arithmetic [1] is also known as "clock" arithmetic. Basically a : b (mod n) if a= b+kn for some integer k. If a is non negative and b is between 0 and n, one can think of b as the remainder of a when divided by n. Sometimes, b is called the residue of a, modulo n. a is called congruent to b, modulo n. ':' denotes congruence

The set of integers from 0 to n-1 form what is called a complete set of residues modulo n. This means that, for every integer a, its residue modulo n is some number from 0 to n-1. This operation is called modular reduction.

The general problem that arises during public key encryption schemes is to find two number 'x' such that 1 = (a*x) mod n where 'a' is the one of the keys used in public key encryption. This is also written as a-1 : x (mod n). This modular inverse problem is difficult to solve. Sometimes it has a solution sometimes not. For example inverse of 5 modulo 14 is 3, and on the other hand 2 has no inverse modulo 14. In general a-1 : x (mod n) has a unique solution if a and n are relatively prime. If n is a prime number then every number from 1 to (n-1) is relatively prime to n and has exactly one inverse modulo n in that range.

Proposed Cryptosystem

1. Choose random "large" prime integers p and q of roughly the same size, but not too close together.
2. Calculate the product n = pq (ordinary integer multiplication)
3. Choose a random *encryption exponent* e = 3 that has no factors in
common with either p-1 or q-1 .
4. Calculate ed mod (p-1) * (q-1) = 1
5. Encryption: $c = m^e \bmod n$
6. Decryption: choose a large value of d

M= c^d mod n is similar to

$\mathbf{v_1 = c^d \bmod p}$ and $\mathbf{v_2 = c^d \bmod q}$

It is equivalent to

$\mathbf{v_1 = c^{d \bmod (p-1)} \bmod p}$ and $\mathbf{v_2 = c^{d \bmod (q-1)} \bmod q}$.

or

$\mathbf{C_2 = p^{-1} \bmod q}$, and

$\mathbf{u = (v_2 - v_1)C_2 \bmod q}$.

Or

The final answer is:

$\mathbf{c^d \bmod n = v_1 + u\,p}$.

A. Advantages of Proposed Cryptosystem

1.In our proposed cryptosystem, the encryption is faster in comparison to current variants of RSA cryptosystem because we are using e = 3. The binary representation of 3 is 011. It contains only two 1's. so it takes only 17 multiplications to exponentiate.

2.Also our proposed cryptosystem is more secure against low decryption exponentiation attack, because we are using a large value of d.

Conclusion

In this paper, we discussed some existing variants of RSA cryptosystem. We also proposed a novel cryptosystem. The proposed cryptosystem is faster & it is also more secure.

References

[1] Applied Cryptography by Bruce Schneier ISBN 9971-51- 348-X.

[2] D. Khan, The Code Breakers: The story of secret Writing, New York: Macmillan publishing co., 1967.

[3] R.L. Rivest and A. Shamir, "How to Expose an Eavesdropper" Communication Of the ACM,v.27,n.4 april 1984.

[4] D. Gordon. Discrete Logarithms in GF(p) using the Number Field Sieve,SIAMJ.Discrete Math.,Vol.6,ppt.124-138,1993.

[5] S. Cavallar, B. Dodson, A. K. Lenstra, W. Lioen, P. L. Montgomery, B. Murphy, H. te Riele, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand, F. Morain, A. Muffett, C. Putnam, C. Putnam, and P. Zimmermann. Factorization of 512 bit RSA key using the number field sieve. In proceedings Eurocrypt 2000, Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000. Factorization announced in August, 1999.

[6] J. Hastad. Solving simultaneous modular equations of low degree. SIAM Journal on Computing, vol. 17, no. 2,PP.336-341,1988.

[7] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. Journal of Cryptology,vol.10,pp.233-260,1997.

[8] E.F Brickell, "Survey of Hardware Implementations Of RSA,"Advances in Cryptology-CRYPTO'89 Proceedings,Springer-Verlag,1990

[9] D. Coppersmith, M. Franklin, J. Patarin, and M. Reiter. Low exponent RSA with related messages. In proceedings Eurocrypt'96, Lecture Notes in Computer Science, vol.1070, Springer-Verlag, pp.1–9, 1996.

[10] M. Wiener. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol. 36, no. 3, pp. 553–558, 1990.

Biographies

FIRST A. AUTHOR received the B.E. degree in Computer Engineering from the University of R.GP.V., Bhopal, M.P., in 2005, Persuing M.tech in Computer Science from the University of R.G.P.V., Bhopal, M.P..Currently, I m M.tech final year student in SSSIST,Sehore College,India.

SECOND B. AUTHOR received the M.tech degree in Computer Science from the University R.G.P.V., Bhopal, M.P., in 2010, Persuing Ph.D. in Computer Science from B.U., Bhopal, M.P. Currently, He is an associate Professor of computer science & engineering at SSSIST Sehore,india.