ISSN:0975-9646

A Study on RSA Algorithm for Cryptography

Saranya[1], Vinothini[2], Vasumathi[3]

[1& 2]*Research Scholar, Department of Computer Science, PGP college of Arts & Science, Namakkal, Tamilnadu, India*

[3]*Assistant Professor, Department of Computer Science, PGP college of Arts & Science, Namakkal, Tamilnadu, India*

***Abstract*— The RSA algorithm has solved an intimidating challenge in network security, enabling the secure but transparent exchange of encrypted communications between users and other parties (rsa.com, 2011). The following paper explores the history of RSA and the method.**

***Keywords*— RSA algorithm, security, key size.**

I. LITERATURE REVIEW

The idea of the RSA public key cryptosystem was from Diffie and Hellman, who introduced the method of the exponential key exchange. The Diffie-Hellman key exchange is the second most popular public key algorithms, after the RSA. However, the first ever known description of a similar system was made in 1973 by Cifford Cocks, a mathematician working at the GCHQ, a UK intelligence agency. The system was never set up considering the relatively expensive computers required to implement it at the time. Because of its top secret classification, it was not until, 1998 that his discovery was revealed. During the fall of 1976, Ronald Rivest, Adi Shamir and Leonard Adleman, all young faculty members at the Masschusettes Institute of Technology began working on a novel type of cryptographic design. Rivest and Shamir were computer scientists at the MIT while Adleman was a number theorist at the Institution. In their project, Ronald and Adi would develop ideas while Leonard would attempt to bring the ideas down, by cracking them. Leonard was time and again successful at cracking them until one night when Ronald developed an algorithm that Leonard could not crack. The Algorithm was named RSA from their names Rivest, Shamir, and Adleman. To this day, the algorithm has never been broken (Ohya & Volovich 2011).

The core of RSA has withstood every attack from the best cryptographic minds. The robustness of the algorithm, the absence of rigorous proof notwithstanding, provides a sense of security. According to Dan Boney, a computer science professor at the Stanford University, "we kind to chip at the sides, but no one have figured out how to get at the heart of it." (Robinson, 2003, pp.6)

RSA has come to play a vital role in electronic communications. Being the first example in history of the public key cryptosystem and, worth nothing, the only type that has withstood more than three decades of attacks, the RSA has become the choice algorithm for functions such as authenticating phonecalls, encrypting credit-card transactions over the Internet, Security e-mail and providing numerous other Internet security functions. The functions of the RSA continue to increase, and to award their efforts, Rivest, Shamir, and Adleman received one of the highest awards in the field of mathematics, the Association for Computing Machinery's 2002 Alan Turing Award. It is without surprise that the security of RSA remains a major focus of cryptographic research, in theoretical as well as practical functions (Abhijit, 2009).

II. METHODOLOGY

The following is a description of how RSA is used:

- The RSA is a block cipher whereby the plaintext and ciphertext are integers between 0 and n-1, for some n.
- A typical size for n is 1024 bits.
- In the RSA algorithm, one party uses a public key and the other party uses a secret key, known as the private key. Each station randomly and independently choose two large primes p and q number, and multiplies them to produce n=pq. This is the modulus used in the arithmetic calculations of the RSA algorithm (Rivest, Shamir, & Adleman, 1978).
- The process of the RSA algorithm is as described below:

1. Select p and q (both should be prime numbers)
2. Calculate n=pq
3. Calculate z=(p-1)(q-1)
4. Select integer D which is relatively prime to 2. Gcd φ(n) D=1(φ9n)=z)
5. Calculate ED-1 mod(φ(n))

6. For Encryption:
   $C=P^E \bmod n$
7. Where P is Plaintext, C is Cipertext (encryption)
8. For Decryption:
   $P=C^D \bmod n$

- Public key encryption algorithm uses a public key of PU=(e,n) and private key of PR=(d,n).

Requirements

- It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M<n$.
- It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all value of $m<n$.
- It is infeasible to determine d given e and n.

III. RSA ALGORITHM

The RSA algorithm methods are described below:

1. Select two prime numbers, that is, p and q.
2. Calculate n=pq.
3. Calculate z=φ(n)= (p-1)(p-1).
4. Select integer e, gcd(φ(n),e)=1; 1<e<φ(n).
5. Calculate d, e=1 modφ(n).
6. For encryption, Ciphertext $C=M^e \bmod n$.
7. For Decryption, Plaintext $M=C^d \bmod n$.

IV. NUMERICAL STUDY ON RSA ALGORITHM

Example: 1

1. Select two prime numbers, p=17 and q=11
2. Calculate n=pq=17*11=187
3. Calculate φ(n)=(p-1)(q-1)=(17-1)(11-1)
   =16*10=160
4. Select e such that e is relatively prime to φ(n)-160. So, we select e=7
5. Determine d such that ed=1 mod φ(n)
   7d=1 mod 160
   7*23=1 mod 160
   161=1 mod 160
   (d is calculated using extended Euclid's Algorithm)

Here, Public key PU(e, n)=7, 187
Private key PR(d, n)=23, 187
Suppose, the Plaintext value (M) is 88 then,

6. For Encryption,
   Ciphertext $C = M^e \bmod n$
   $= (88)^7 \bmod 187$
   $= 888832 \bmod 187$
   $= 11$
7. For Decryption,\
   Plaintext $P = C^d \bmod n$
   $= 11^{23} \bmod 187$
   $= 79720245 \bmod 187$
   $= 88$

Example: 2

1. Select two prime numbers, p=3 and q=11
2. Calculate n=pq=3*11=33
3. Calculate φ(n)=(p-1)(q-1)=(3-1)(11-1)
   =2*10=20
4. Select e such that e is relatively prime to φ(n)-20. So, we select e=7
5. Determine d such that ed=1 mod φ(n)
   7d=1 mod 20
   7*3=1 mod 20
   21=1 mod 20
   (d is calculated using extended Euclid's Algorithm)

Here, Public key PU(e, n)=7, 33
Private key PR(d, n)=3, 33
Suppose, the Plaintext value (M) is 5 then,

6. For Encryption,
   Ciphertext $C = M^e \bmod n$
   $= (5)^7 \bmod 33$
   $= 78125 \bmod 33$
   $= 14$
7. For Decryption,\
   Plaintext $P = C^d \bmod n$
   $= 11^3 \bmod 33$
   $= 2744 \bmod 33$
   $= 5$

V. DISCUSSION

When encrypting with low encryption exponent, (e.g., e=3) and small values of the m, (i.e., $m<n^{1/e}$) the result of m^e is strictly less than the modules n. in this case, ciphertext can be easily decrypted by taking the e^{th} root of the ciphertext over the integers. If the value of m is high, ciphertext can't be easily decrypted. In the above example, the exponent value 7 is produce the better security than the exponent value of 3 in RSA algorithm.

CONCLUSION

In this article, we have analysed on the value of the exponent in the RSA algorithm. If the value of exponent is high, the security of RSA algorithm also high. So, we proposed to implement the high value of exponent in RSA algorithm to produce a better security.

REFERENCES

[1] Abhijit Das, C. E. (2009). *Public-Key Cryptography:Theory and Practice.* Mumbai: Pearson Education India.

[2] Ohya, M., & Volovich, I. (2011). *Mathematical Foundations of Quantum Information and Computation and Its Applications to Nano- and Bio-systems.* New york: Springer.

[3] Rivest, R., Shamir, A., & Adleman, a. L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* , 120- 126.

[4] Robinson, S. (2003). Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders. *SIAM News*, p. 6.

[5] RSA.com. (2011). *RSA history.* Retrieved December 8, 2011 from <http://www.rsa.com/node.aspx?id=2760.>.

[6] *Tariq Alturkestani & Saeed Al Jaberi, RSA-Algorithm for Public-Key Cryptography*

[7] Boneh, Dan (1999). "Twenty Years of attacks on the RSA Cryptosystem". *Notices of the American Mathematical Society* **46** (2): 203–213.

[8] Håstad, Johan (1986). "On using RSA with Low Exponent in a Public Key Network". *Advances in Cryptology — CRYPTO '85 Proceedings*. Lecture Notes in Computer Science **218**. pp. 403–408.

[9] Coppersmith, Don (1997). "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities". *Journal of Cryptology* **10** (4): 233–260.

[10] Bidzos, Jim, "Threats to Privacy and Public Keys for Protection", *COMPCON Spring '91 Digest of Papers*, IEEE Computer Society Press, p. 189-94.

[11] Cryptography And Network Security - By William Stallings.Principles Of Key Management - By W .Fumy And P. Landrock.A Comparative Study Of RSA Encryption And Decryption – By R.E Ting And S.T. Barnum.