International Research Journal of Advanced Engineering and Science

ISSN: 2455-9024

A Survey on Various Asymmetric Algorithms

S. Sathish Kumar[1], S. R. Akshay Prabhu[2], R. Durga[3], S. Jeevitha[4]

[1]AP(SG)/CSE, SNS College of Technology, India

[2, 3, 4]UG Student, SNS College of Technology, India

***Abstract*— *In this fast moving world, communication among several systems through networks play a vital role. Being available to everybody, this also shares a risk factor of being easily traceable by anyone in the network. The need for network security is never fully satisfied. Making every communication through a network strictly secured is something next to impossible. And so we ought to choose a method where even if the transmitted data is hacked, it can be made to remain inaccessible or not understandable. This method is called encryption. The method that acts vice versa (i.e) making a data that is not understandable text into an understandable data is called decryption. The cryptosystem consists of both symmetric cryptography algorithms and asymmetric cryptography algorithms. Some of the asymmetric cryptography algorithms are discussed in this paper*.

***Keywords*— *RSA, A-RSA, Rabin, cipher text, plain text, encryption, decryption*.

I. Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. The process of converting a plain text from sender side into an unreadable format is called encryption. The process by which this unreadable text is converted into a readable format again in the receiver side is called decryption.

Types of Ciphers

- Block Cipher - Uses a single shift key for all the characters
- Stream Cipher - Uses a series of hash values

  i) Asynchronous Stream Cipher- Static series of hash values

  ii) Synchronous Stream Cipher- Dynamic series of hash values

The asymmetric cryptography is one of the branches of cryptography where a secret key can be divided into two parts namely private key and public key. The private key must be kept secret and the public key can be shared to anyone. The primary uses of asymmetric cryptography is authentication and confidentiality. Using asymmetric cryptography messages can be signed with a private key of the sender and using the public key the receiver can ensure that the message is sent by the person containing the corresponding private key.

The encryption with asymmetric cryptography is a different one compared to symmetric cryptography. Any person with the public key can encrypt the message and then only the person who possess the private key can decrypt it.

The asymmetric algorithms are RSA, Diffie-Hellman, Digital signature algorithm, ElGamal, etc.

II. RSA Algorithm

The RSA algorithm was proposed by Rivest, Shamir and Adleman. RSA is the most widely used asymmetric algorithm. RSA is used for encryption and also digital signatures.

RSA algorithm uses private key cryptosystem. It overcame the difficulties faced by public key cryptosystems. This algorithm was a break through for security by providing encryption and decryption of data using different keys that need not be shared between the sender and the receiver. Every character in a text data is assigned a default value from its parent string. This value is used for computing a different cipher value that may correspond to a different character in the parent string. The text data so obtained is the cipher text that is sent through the transmission medium.

There is a common value n that is product of two prime numbers. The value of n is shared commonly shared between the sender and receiver.

Encryption is done by

$$c=m^e \bmod n$$

Decryption is done by

$$m=c^d \bmod n$$

RSA algorithm can be summarized as follows:

1. Select two large prime numbers p and q.
2. Calculate n=p*q; where n is modulus for both keys.
3. Select e (public key) such that it is not a factor of (p-1)(q-1).
4. Calculate d (private key) such that:
   d*e mod (p-1)(q-1)=1.
5. For encryption, calculate the cipher text C from plaintext M as $C=M^e$ mod n.
6. For decryption, calculate the plaintext M from the cipher text C as $M=C^d$ mod n

III. Diffie-Hellman Algorithm

The Diffie Hellman algorithm was invented in 1976. Two users can be allowed to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman is a mostly used key exchange. Usually two parties wish to begin communication but they suffer by the lacking of commonly shared secret key and hence cannot use secret key cryptosystems. The Diffie-Hellman algorithm provides a solution for this by allowing the construction of a common secret key through an insecure communication channel. It is based on problem related to discrete logarithms. The Diffie-Hellman will be a secure on when appropriate mathematical group is used. The Diffie-Hellman algorithm is not implemented on hardware.

Steps involved in Diffie-Hellman Algorithm:

1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob (g^a mod p).
3. Bob chooses a secret number b, and sends Alice (g^b mod p).
4. Alice computes ((g^b mod p)^a mod p)

S. Sathish Kumar, S. R. Akshay Prabhu, R. Durga, and S. Jeevitha, “A survey on various asymmetric algorithms,” *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 117-119, 2016.

5. Bob computes $((g^a \bmod p)^b \bmod p)$

IV. Digital Signature Algorithm

The digital Signature Algorithm (DSA) is a Federal Information Processing Standard for Digital signatures. It was proposed by National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard.

The key generation in DSA has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system. The second phase computes the public and private keys for a single user.
The secrecy and uniqueness of random key signature value are critical such that violating any of these requirements can reveal the original secret key to the hacker.

Generally a digital signature scheme satisfies the following:
G (key-generator) generates a public key, pk, and a corresponding private key, sk, on input 1^n,where n is the security parameter.
V (verifying) outputs accepted or rejected on the inputs: the public key, pk, a string, x, and a tag, t.

V. Optimal Asymmetric Encryption Padding (OAEP)

OAEP was introduced by Bellare and Rogaway. Optimal Asymmetric Encryption Padding is a padding scheme that is often used together with RSA Algorithm. The OAEP is a form of Feistal network which uses a pair of random oracles G and H to process the plaintext prior to asymmetric encryption. OAEP is proved to be more secure than cipher attacks.
Steps for OAEP algorithm:
n is the number of bits in the RSA modulus.
k0 and k1 are integers fixed by the protocol.
m is the plaintext message, an (n − k0 − k1)-bit string
G and H are cryptographic hash functions fixed by the protocol. To encode,
1. messages are padded with k1 zeros to be n − k0 bits in length.
2. r is a random k0-bit string
3. G expands the k0 bits of r to n − k0 bits.
4 $X = m00..0 \oplus G(r)$
5. H reduces the n − k0 bits of X to k0 bits.
6. $Y = r \oplus H(X)$ 7. The output is $X \parallel Y$ where X is shown in the diagram as the leftmost block and Y as the rightmost block.
To decode,
1. recover the random string as $r = Y \oplus H(X)$
2. recover the message as $m00..0 = X \oplus G(r)$

VI. The Elgamal Algorithm

The ElGamal Algorithm provides an alternative to the RSA for public key encryption. Security of the RSA depends on the difficulty of factoring large integers. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus. ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext. It has the advantage that the same plaintext gives a different ciphertext each time it is encrypted.
Alice chooses
i) A large prime pA (say 200 to 300 digits),
ii) A primitive element αA modulo pA,
iii) A (possibly random) integer dA with 2 ≤ dA ≤ pA –2.
Alice computes
iv) βA ≡ αA dA (mod pA).

Alice's public key is (pA, αA, βA). Her private key is dA.
Bob encrypts a short message M (M < pA) and sends it to Alice like this:
i) Bob chooses a random integer k (which he keeps secret).
ii) Bob computes r ≡ αAk (mod pA) and t ≡ βAkM (mod pA), and then discards k. Bob sends his encrypted message (r, t) to Alice.

When Alice receives the encrypted message (r, t), she decrypts (using her private key dA) by computing tr−dA.

Even if Eve intercepts the ciphertext (r, t), she cannot perform the calculation above because she doesn't know dA.
βA ≡ αA dA (mod pA), so dA ≡ LαA(βA) Eve can find dA if she can compute a discrete log in the large prime modulus pA, presumably a computation that is too difficult to be practical.

VII. Conclusion

The various asymmetric algorithms were discussed with their advantages and disadvantages. Each algorithm has its own characteristics and functionalities. The efficiency of these algorithms were calculated and compared and a comparison has been made based on the efficiency factor. Asymmetric algorithm can be used to eliminate the problem of user, when a users transmit the data over the network there is no guaranteed that data is original data or not. It means any unauthorized person can easily access that data and also they can alter that data. Asymmetric key is used for providing security to the users when they transmit data over the network. Public key cryptography uses two keys one for encryption and other for decryption so it provides better security for users. RSA algorithm is providing much overhead in encrypting the text.

References

[1] A. J. Amalraj and J. J. Raybin Jose, "A survey paper on cryptography techniques," *International Journal of Computer Science and Mobile Computing*, vol. 5, issue 8, pp. 55-59, 2016

[2] T. V. Satya Vivek, D. Anandam, G. Anil, B. Sreenivasulu, V. Lakshma Reddy, and M. R. Batchnaboyina, "Modified RSA algorithm for security protocol," *International Journal of Computer Science and Information Technologies(IJCSIT)*, vol. 6, issue 3, pp. 2097-2098, 2015.

[3] Saranya, Vinothini, and Vasumathi, "A study on RSA Algorithm for Cryptography," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 5, issue 4, pp. 5708-5709, 2014.

[4] P. M Durai Raj Vincent, "RSA encryption algorithm-A survey on its various forms and its security level," *International Journal of Pharmacy and Technology*, vol. 8, issue 2, pp. 12230- 12240, 2016.

[5] D. B. Khairnar and S. Kadam, "Secure RSA: Pair wise key distribution using modified RSA algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, issue 4, pp. 383-387, 2016.

[6] G. Gupta and R. Chawla "Review on encryption cipher of cryptography in network security," *International Journal of Advanced Research in Computer Science and Software Engineering*, volume 2, issue7, pp. 211-213, 2012.

[7] R. Tripathi and S. Agrawal, “Comparative study of symmetric and asymmetric cryptography techniques,” *International Journal of Advance Foundation and Research in Computer (IJAFRC)*, vol. 1, issue 6, pp. 68-76, 2014.

[8] S. N. Chalurkari, N. Khochare, and B. B. Mashram, “Survey on modular attack on RSA algorithm,” *International Journal of Computational Engineering & Management*, vol. 14, pp. 106-110, 2011.

[9] Cryptography and Network Security, Express Learning, ITL Education Solution ltd.

[10] B. D. Allen, “Implementing several attacks on plain ElGamal encryption,” A thesis submitted to the graduate faculty in partial fullment of the requirements for the degree of Master of Science, Iowa State University, Ames, Iowa, 2008.

[11] B. Padmavathi and S. RanjithaKumari, “A survey on performance analysis of DES, AES and RSA algorithm along with LSB substitution technique,” *International Journal of Science and Research (IJSR)*, vol. 2, issue 4, pp. 170-174, 2013.

[12] L. Qing, L. Yunfei, L. Tong, and H. Lin, “The research of the batch RSA decryption performance,” *Journal of Computational Information Systems*, vol. 7, issue 3, pp. 948-955, 2011.

[13] L. Singh and R. K. Bharti, “Comparison among different cryptographic algorithms using neighbourhood-Generated keys,” *International Journal of Computer Applications*, vol. 73, issue 5, pp. 39-42, 2013.

[14] R. S. Jamgekar and G. S. Joshi, “File encryption and decryption using secure RSA,” *International Journal of Emerging Science and Engineering (IJESE)*, vol. 1, issue 4, pp. 11-14, 2013.