Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1190 – 1196

RESEARCH ARTICLE

Comparison of Asymmetric Algorithms in Cryptography

Neha Garg
Student, CSE Department
PDMCEW
MDU Rohtak, India
nehagarg9115@gmail.com

Partibha Yadav
Assistant Professor, CSE Department
PDMCEW
Bahadurgarh, India
pratibha1007@gmail.com

ABSTRACT:- In this paper we compare asymmetric algorithm like (RSA , Elliptic curve ,OAEP) which is used for security when data is transmitting over the network. These algorithms are based on digital signature scheme. Digital signature is the technique of cryptography which is used for providing security to the users. Cryptographic technique is one of the principal means to protect information security. Not only this but it also ensures the information confidential, and also provides digital signature, authentication, secret sub-storage, system security and other functions. So encryption and decryption process is the solution of ensuring the non repudiation, confidentiality, integrity and authenticity of the data. These are the four main objectives of cryptography which is used to ensure the security of data.

Keywords: Cryptography, RSA, Elliptic curve cryptography, OAEP, Security

I. INTRODUCTION

Does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects for security purpose and there are many applications for secure commerce and payments for private communications and protecting passwords which is the basic need for user. So cryptography is necessary because it provides secure environment for communication. Main purpose of cryptography is keep information secure from unauthorized access. Cryptography is practice and study of techniques for secure communication in the presence of third parties. Cryptography is the practice and study of hiding information. it is the art and science of converting the plain text into cipher text. In cryptographic terminology, the message is called plaintext. Encoding the contents of the message in such a way that its contents cannot be unveiled by outsiders is called encryption. The encrypted message

is called the cipher text. The process of retrieving the plaintext from the cipher text is called decryption. There are four main objectives of cryptography:-

1. **Confidentiality:** It guarantees that the sensitive information can only be accessed by those users/entities authorized to unveil it.
2. **Data integrity:** It is a service which addresses the unauthorized alteration of data. This property refers to data that has not been changed, destroyed, or lost in a malicious or accidental manner.
3. **Authentication:** It is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other.
4. **Non-repudiation:** It is a service which prevents an entity from denying previous commitments or actions.

Digital signature is an electronic signature which is used to identify the identity of sender's message or signer of document, and ensure that the original content of the message or document that has not been sent is altered. Digital signatures are easily transmitted that cannot be matched by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message is authenticated means that sender cannot easily repudiate it. A digital signature can be used with any kind of message, whether it is confidential or not whether it is encrypted message or decrypted messages, so it can say that the receiver can be sure of the sender's identity and that the message arrived with its consistency that means arrived message is original or unaltered information.

II. TYPES OF CRYPTOGRAPHY

SYMMETRIC KEY CRYPTOGRAPHY is also known as single-key, secret-key, and private key or one-key encryption. In this technique sender and recover share same key for encryption and decryption process. Symmetric key algorithm is divided into two parts:- first one is **BLOCK CIPHER** which is used for blocks of data. In this technique data is divided into blocks and then these blocks is used for encryption and decryption. Example of block cipher is AES, triple DES which is popular techniques of symmetric algorithms. And second one is **STREAM CIPHER** which operates on a single bit at a time. Transmitting the secret key on insecure network is also a curse of destroy the secrecy. There are many advantages of symmetric key cryptography like Symmetric key encryption is much faster. Single-key encryption does not require a lot of computer resources when compared to public key encryption. A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

ASYMMETRIC KEY CRYPTOGRAPHY is also known as the public key cryptography. There are two types of key first one is public key which is used for encryption and second is private key which is used for decryption. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. The major drawbacks of asymmetric ciphers are their speed and security strength; they are much slower than the symmetric algorithms and more vulnerable to intruder attacks but they make key exchange easier. Asymmetric popular ciphers RSA (Rivest Shamir Adlemam), Elliptic curve, Diffie hellman key exchange algorithm, Digital signature. Advantages of asymmetric key algorithm are It solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret. Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender. The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.

III. RSA ALGORITHM

Problems with RSA algorithm

- Key generation is very slow.
- Speed of encrypting of text is slow.
- Message length should be less than the bit length otherwise algorithm will be fail.
- RSA is factorization based algorithm so that every time RSA initialization takes two large prime number p and q.

IV. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz as an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths. The security of a public key system using elliptic curves is based on difficulty of computing discrete algorithms in the group of points on an elliptic curve defined over a finite field. Elliptic curve equation over a finite field F_p is

$$y^2 = x^3 + ax + b \mod p$$

Here, y, x, a and b are all within F_p, and p is a integers modulo p. a and b is the coefficients which determine what points will be on the curve. Curve coefficients have to fulfill one condition that is:

$$4a^3 + 27b^2 \neq 0$$

This condition guarantees that the curve will not contain any singularities.

POINT REPRESENTATION

Representing a point on the curve is done in affine projection. Points which are represented in affine coordinates are vectors with an x and y component. Here x and y values are also integers modulo p.

Point Operation:- There are two basic operation in elliptic curve Point Addition and Point Doubling.

1. POINT ADDITION

Adding two points is not easy in curve, adding their x- and y-components and taking them modulo p. connecting the two points via a line and then intersecting that line using curve. Point addition is works only two points which are not same.

$$R = P + Q = \begin{pmatrix} p_x \\ p_y \end{pmatrix} + \begin{pmatrix} q_x \\ q_y \end{pmatrix}, \quad P \neq Q$$

2. POINT DOUBLING

Point doubling comes into play if two points shall be added which are identical, i.e

$$R = P + P$$

These are the calculations needed to get R. Note that a, which is needed for calculating s, is one of the curve parameters:

$$r_y = s \cdot (p_x - r_x) - p_y$$

Elliptic curve cryptosystem parameters is

- p: The prime number which defines the field and curve operate on finite field F_p.
- a and b are two coefficients which define the curve.
- G: The generator or base point. it has two separate integers g_x and g_y.

- n: The order of the curve generator point G.
- h: The cofactor of the curve. It is the quotient of the number of curve-points.

Generate a key in elliptic curve:-

To get the private key, choose a random integer d_A, so that

$$0 < d_A < n$$

Then getting the accompanying public key Q_A is equally trivial, you just have to use scalar point multiplication of the private key with the generator point G:

$$Q_A = d_A \cdot G$$

In the elliptic curve public and private key are not equally exchangeable the private key d_A is a integer, but the public key Q_A is a point on the curve.

Encryption

We want to encrypt data with the public key Q_A that we just generated. Again, first choose a random number r so that

$$0 < r < n$$

Then, calculate the appropriate point R by multiplying r with the generator point of the curve:

$$R = r \cdot G$$

Also multiply the secret random number r with the public key point of the recipient of the message:

$$S = r \cdot Q_A$$

Now, R is publicly transmitted with the message and from the point S a symmetric key is derived with which the message is encrypted.

Decryption

Now, we receive a message which is encrypted with a symmetric key. With the message we receive a value of R in plain text.

$$S = d_A \cdot R$$

By just multiplying your private key with the publicly transmitted point R, we will receive the shared secret point S, from which we can then derive the symmetric key. Now substitute the values:-

$$S = d_A \cdot R = d_A \cdot r \cdot G = r \cdot (d_A \cdot G) = r \cdot Q_A$$

Elliptical curve cryptography is a method of encoding data files so that only specific individuals can decode them. ECC is based on the mathematics of elliptic curves and uses the location of points on an elliptic curve to encrypt and

decrypt information. it increases the size of the encrypted message significantly more than RSA encryption. ECC algorithm is more complex and more difficult to implement than RSA.

V. OAEP (OPTIMAL ASYMMETRIC ENCRYPTION PADDING)

OAEP was introduced by Bellare and Rogaway. Optimal Asymmetric Encryption Padding (OAEP) is a padding scheme often used together with RSA encryption. The OAEP algorithm is a form of Feistel network which uses a pair of random oracles G and H to process the plaintext prior to asymmetric encryption. When combined with any secure trapdoor one-way permutation f, this processing is proved in the random oracle model to result in a combined scheme which is semantically secure under chosen plaintext attack . When implemented with certain trapdoor permutations (e.g., RSA), OAEP is also proved secure against chosen cipher text attack. OAEP can be used to build an all-or-nothing transform.

Steps for OAEP algorithm:

In the diagram,

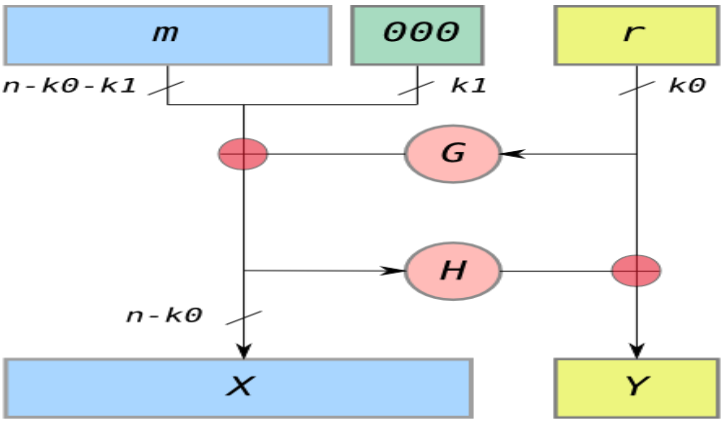
- n is the number of bits in the RSA modulus.
- k_0 and k_1 are integers fixed by the protocol.
- m is the plaintext message, an $(n - k_0 - k_1)$-bit string
- G and H are cryptographic hash functions fixed by the protocol.

To encode,

1. messages are padded with k_1 zeros to be $n - k_0$ bits in length.
2. r is a random k_0-bit string
3. G expands the k_0 bits of r to $n - k_0$ bits.
4. $X = m00..0 \oplus G(r)$
5. H reduces the $n - k_0$ bits of X to k_0 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 $m00..0 = X \oplus G(r)$



Two main goals of OAEP:-

1. Add an element of randomness which can be used to convert a deterministic encryption scheme (e.g., traditional RSA) into a probabilistic scheme.
2. Prevent partial decryption of cipher texts (or other information leakage) by ensuring that an adversary cannot recover any portion of the plaintext without being able to invert the trapdoor one-way permutation f.

VI. CONCLUSION AND FUTURE WORK

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 its provide better security for users. RSA algorithm is providing much overhead in encrypting the text. When we compare the elliptic curve cryptography with RSA then we identify that ECC provides less overhead compare to the RSA. In case of encrypting the text ECC is better than RSA. OAEP is a padding scheme which is used by RSA algorithm. OAEP provides the better security compared to RSA. In RSA algorithm, message length should be less than the bit length so unauthorized person can easily crack it but in case of OAEP there is no problem with the message length because it takes large bit length. In OAEP speed of encryption process is better than RSA. RSA provides highest security to the business application so this scheme can be used for encryption of long messages without employing the hybrid and symmetric encryption. RSA key generation is significantly slower than ECC key generation for RSA key of sizes 1024 bits and greater. Purpose of this paper is to find out the best algorithm which provides the security to users .

REFERENCES

[1]. Jiezhao Peng, Qi Wu, Research and Implementation of RSA Algorithm in Java, 978-0-7695-3366-7/08 $25.00 © 2008 IEEE

[2]. Xin Zhou, Xiaofei Tang, Research and Implementation of RSA Algorithm for Encryption and Decryption, 978-1-4577-0399-7/111$26.00 ©20111EEE

[3]. Li Dongjiang, Wang Yandan and Chen Hong, The research on key generation in RSA public- key cryptosystem, 2012 Fourth International Conference on Computational and Information Sciences, 978-0-7695-4789-3/12 $26.00 © 2012 IEEE

[4]. Shilpi Gupta, Jaya Sharma, A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman, 978-1-4673-1344-5/12/$31.00 ©2012 IEEE

[5]. Alese, B. K., Philemon E. D., Falaki and S. O., Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology Volume 2 No. 9, September, 2012

[6]. Aqeel Khalique, Kuldip Singh and Sandeep Sood, Implementation of Elliptic Curve Digital Signature Algorithm, International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[7]. Ram Ratan Ahirwal and Manoj Ahke, Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network, International Journal of Computer Science and Information Technologies, Vol. 4 (2) , 2013, 363 – 368

[8]. Vishal Garg and Rishu, Improved Diffie-Hellman Algorithm for Network Security Enhancement, Int.J.Computer Technology & Applications,Vol 3 (4), 1327-1331, July-August 2012

[9]. Rounak Sinha, Hemant Kumar Srivastava and Sumita Gupta, Performance Based Comparison Study of RSA and Elliptic Curve Cryptography, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 ,ISSN 2229-5518

[10]. M. Preetha, M. Nithya, A STUDY AND PERFORMANCE
ANALYSIS OF RSA ALGORITHM, IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139

[11]. Ashish Vijay,Priyanka Trikhaand Kapil Madhur, A New Variant of RSA Digital Signature, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012

[12]. Botes, J.J., Penzhorn, W.T., 1994. An implementation of an elliptic curve cryptosystem. Communications and Signal Processing. COMSIG-94. In Proceedings of the 1994 IEEE South African Symposium, 85 -90.

[13]. Mohsen Machhout eat.al., "coupled FPGA/ASIC Implementation of elliptic curve crypto-processor," International Journal of Network Security & its Applications Vol. 2 No. 2 April 2010

[14]. Certicom Corp., (2004). An elliptic curve cryptography (ecc) primer. White paper, Certicom

[15]. Williams Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006

