The Application of Elliptic Curve Cryptography in Secure E-mail System

Xia Lin
School of Informatics, Linyi University, Linyi, 276000, China

***Abstract*—E-mail is one of the most popular services on Internet, but traditional e-mail system is transmitted in plain text, which brings a lot of security risks. In order to ensure the security of e-mail, this paper analyses the integrity, confidentiality and repudiation of information. It introduces the protocol of e-mail transmission and encryption algorithms. Through the comparison of the algorithms, it presents an encryption and signature scheme based on triple DES and Elliptic Curve Cryptography, and designs a fast algorithm of ECC. Finally, it sets up a secure and efficient e-mail system, which implements message encryption, digital signature and identification effectively in the process of electronic mail transmission.**

Keywords-electronic mail; elliptic curve cryptography; encryption; digital signature

I. Introduction

With the rapid development of Internet, E-mail becomes one of the most popular services in Internet with its convenient. At the same time, a lot of secret information as a part of the electronic mail transferred on Internet, which attracts significant coverage from people who often use electronic mail. In order to ensure the security of e-mail in the transmission process, the mail system should provide the following secure service:

Integrity: The message can be found quickly without unauthorized tampering or tampering in the process of transmission.

Confidentiality: Only the sender and the receiver know the real content.

Repudiation: The receiver can confirm the sender by verify the signature of mail.

SMTP(Simple Mail Transfer Protocol) is an application layer protocol which provides reliable and effective e-mail transmission, but SMTP does not provide encryption services. Therefore the attackers can intercept the message content in the mail transfer process, and can easily restore the text format, non-text format of the binary data. In order to make the email confidentiality, and only the recipient can read the message, the e-mail system must provide encryption, digital signature.

Most secure e-mail products use RSA algorithm as the signature of the public key algorithm, but with the continuous development and application of information technology, the security requirements of information has becoming more and more high. At the same time, with the rapid development of network technology, people's computing power is also more and more strong, the large integer factorization is also becoming more and more easy. So we should design a secure E-mail system with higher security.

II. Encryption Algorithm

A. 3-DES

DES(Data Encryption Standard) is a block cipher which transform data from 64 bit plain-data blocks into 64 bit cipher-data blocks. The key length of DES is 64 bits, 8 bits are used for parity checking and 56 bits are actual key data for encryption or decryption. The encryption speed of DES is fast, but the key space of it is too small to prevent exhaust attack. In this paper, we use triple DES, the implementation of it is:

(1) 3-DES with three deferent keys

the encryption:

$$C = E_{k3}(D_{k2}(E_{k1}(M)))$$

the decryption:

$$M = D_{k1}(E_{k2}(D_{k3}(C)))$$

(2) 3-DES with two different keys

the encryption:

$$C = E_{k1}(D_{k2}(E_{k1}(M)))$$

the decryption:

$$M = D_{k1}(E_{k2}(D_{k1}(\mathrm{M})))$$

(3) 3-DES with the same key

this mode is equal to DES

In order to improve the security, we select the first mode.

B. ECC

Elliptic curve cryptography (ECC) was developed by Koblitz and Miller[1], which is a cryptographic approach based on the algebraic structure of elliptic curves over finite field. The primary benefits of ECC are smaller key sizes, less storage, and faster implementations than RSA.

Let F_p be a prime finite field so that p is an odd prime number, and let $a, b \in F_p$, satisfy $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ p)$. Then an elliptic curve $E(F_p)$ over F_p defined by the parameters $a, b \in F_p$ consists of the set of solutions or points $P = (x, y)$ for $x, y \in F_p$ to the equation:

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

together with an extra point O called the point at infinity. For a given point $P = (x_p, y_p)$, x_p is called the x -coordinate of P, and y_p is called the y -coordinate of P. The addition operation in $E(F_p)$ is specified as follows:

(1) $P + O = O + P = P$ for all $P \in E(F_p)$.

(2) If $P = (x, y) \in E(F_p)$, then $(x, y) + (x, -y) = O$.

(3) Let $P = (x_1, y_1) \in E(F_p)$ and $Q = (x_2, y_2) \in E(F_p)$, where $P \neq \pm Q$ .Then $P + Q = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2 (\mathrm{mod}\ p)$, $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p)$ and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.

(4) Let $P = (x_1, y_1) \in E(F_p)$, then $P + P = 2P = (x_3, y_3)$,where $x_3 = \lambda^2 - 2x_1 (\mathrm{mod}\ p)$, $y_3 = \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\ p)$ and $\lambda = \frac{3x_1^2 + a}{2y_1}$.

The performance of an elliptic curve cryptosystem depends of the efficient implementation of the scalar point multiplication kP , which is an operation of successive additions of a point, called base point, along an elliptic curve[2].

The central operation of cryptographic schemes based on ECC is the elliptic scalar multiplication. It dominates the execution time of elliptic curve cryptographic schemes. The calculation of kP can be carried out by *Algorithm 1*.

Algorithm 1. Simultaneous multiple point multiplication

```
input: Window width $w, u_1 = (k_{m-1}, \cdots, k_1, k_0)_2$ , $u_2 = (l_{m-1}, \cdots, l_1, l_0)_2$, $P, Q \in E(F_p)$.
output: $u_1 P + u_2 Q$.
(1) Compute $iP + jQ$ for all $i, j \in [0, 2^w - 1]$.
(2) Write $k = (k^{d-1}, \cdots k^1, k^0)$ and $l = (l^{d-1}, \cdots l^1, l^0)$. where each $k^i$ and $l^i$ is a bitstring of length $w$, and $d = \lceil m/w \rceil$.
(3) $R \leftarrow O$.
(4) For $i$ from $d - 1$ d-1 downto 0 do
        $R \leftarrow 2^w R$.
        $R \leftarrow R + (k^i P + l^i Q)$
(5) Return ($R$).
```

Algorithm 1 requires storage for 2^{2w} points.

Algorithm 2. Window NAF method for point multiplication

```
input: Integers $k$ and $w$ , and a point $P = (x, y) \in E(F_p)$
output: The point $kP$
(1)$P_0 \leftarrow P, T \leftarrow 2P$.
(2) For $i$ from 1 to $2^{w-2} - 1$ do
        $P_i \leftarrow P_{i-1} + T$.
(3) Compute $NAF_w(k) = (u_{t-1}, u_{t-2}, \cdots u_1, u_0)$.
(4) $Q \leftarrow O$.
(5) For $j$ from $l - 1$ downto 0 do
        $Q \leftarrow 2Q$.
        If $u_j \neq 0$ then
            $i \leftarrow (|u_j| - 1)/2$
            If $u_j > 0$ then $Q \leftarrow Q + P_i$;
            Else $Q \leftarrow Q + P_i$.
(6) return($Q$).
```

If some extra memory is available, the running time of *Algorithm 2* can be decreased by using a window method which processes w digits of k at a time.

III. DESIGN OF SECURE E-MAIL SYSTEM

Let the keys of 3-DES are key_1, key_2, key_3, Elliptic curve domain parameters over finite field F_p .

(1)The sender A's private key is KR_a , $1 \leq KR_a \leq n - 1$, compute $u = KU_b \cdot KR_a$, $(x_1, y_1) = KR_a \cdot P$, $v = x_1 \cdot key_1$,$w = x_1 \cdot key_2$, $\alpha = x_1 \cdot key_3$;

(2) Get $h(M)$ by M, then compute the integer e;

(3) The receiver B's private key is KR_b,$1 \leq KR_b \leq n - 1$, compute $(x_2, y_2) = KR_b \cdot P$, $s = KR_b^{-1}(e + r_1 \cdot KR_a)$ mod n , $r_1 = \overline{x_2}$ mod n ;

Then user A sends (u, v, w, α, r_1) to user B.

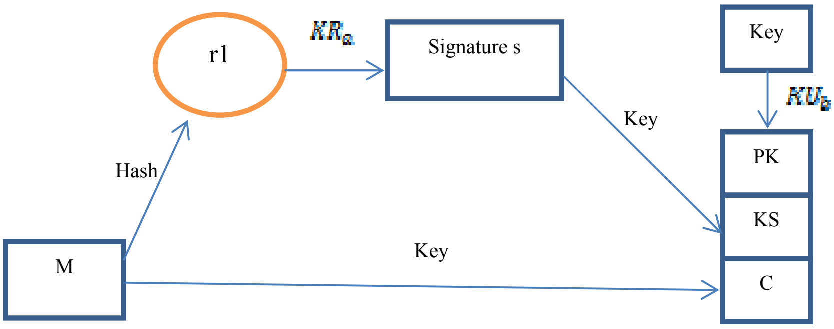

FIGURE I. FIGURE1 ENCRYPTION AND SIGNATURE PROCESS

Figure I shows the approach of packing body before sending mail:

(1) Generate random keys for symmetric encryption algorithm;

(2) Encrypt the session key with receivers' public key;

(3) Encapsulate the data, including the senders' public key and the session key;

(4) Encrypt the message with the session key.

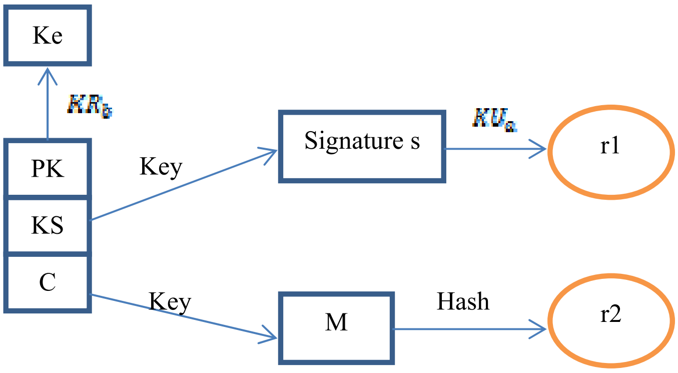

FIGURE II. DECRYPTION AND VERIFY PROCESS

(1) Compute $(x_1,y_1) = uKR_b^{-1}$;

(2) Get key_1,key_2,key_3 by decrypt v ,w, α :

$key_1 = vx_1^{-1}, key_2 = wx_1^{-1}, key_3 = \alpha x_1^{-1}$;

(3) Compute $u_1 = s^{-1}e \ mod\ n$; $u_2 = s^{-1}r_1 \ mod\ n$; $R = u_1P + u_2KU_a = (x_R, y_R)$,

$r_2 = \overline{x_R} \ mod\ n$.

If s is the signature, then $r_2 = r_1$.

Figure II shows the process of verify:

(1) Get the session key with his private key, then obtain the message digest by decrypting the data;

(2) Decrypt the message digest with the senders' public key;

(3) Finally, compare these two message digest, if they are equal, the mail is correct.

IV. Security Analysis

The encryption process of 3-DES is using different key to encryption, decryption, and then encryption, which is equivalent to the use of three keys of 56 bit to encrypt the 64 bit. If we increase one bit to the key length, the number of keys is double, so 3-DES can effectively prevent the brute force attack on the key.

The elliptic curve cryptosystem is based on ECDLP(elliptic curve discrete logarithm problem) in finite field. The finite field size m of the elliptic curve determines the computational complexity of the above problem. There is no mathematical proof that verifies the ECDLP is intractable. However, no one has proven that exist an efficient algorithm for solving the ECDLP.

V. Conclusion

E-mail has become an indispensable means of online communication, in order to make the content of mail more secure, we must take certain methods to ensure the confidentiality and integrity of the mail content. This paper uses ECC as public key algorithm of secure e-mail system, which ensures integrity, confidentiality and undeniable recognition in mail transmission.

References

[1] Certicom Research, SEC1: Elliptic Curve Cryptography Version 1.0, (2000)

[2] Yanqin Zhu, Xia Lin,Gang Wang, "Design of elliptic curve cryptography in GSI,"Current Trends in High Performance Computing and Its Applications, Part II,(2005)623-628.

[3] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., Moeller, B.: Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS). RFC 4492 (2006).

[4] Dimitrov, V. S., Jarvinen, K. U., Jacobson, M. J., Chan, W. F., &Huang, Z.. Provably sublinear point multiplication on Koblitz curves and its hardware implementation. IEEE Transaction on Computer, 57,(2008)1469–1481.

[5] Certicom Research, Standards for efficient cryptography 2: Recommended elliptic curve domain parameters. Standard SEC2, Certicom (2000)

[6] Microsoft Research.: MSR Elliptic Curve Cryptography Library (MSR ECCLib) (2014). http://research.microsoft.com/en-us/projects/nums

[7] Gueron, S., Krasnov, V.: Fast and side channel protected implementation of the NIST P-256 elliptic curve, for x86–64 platforms. OpenSSL patch

(2013). http://rt.openssl.org/Ticket/Display.html?id=3149&user=guest&pass=guest

[8] S. Brlek,S. Hamadou,J. Mullins, “Anonymous and secure electronic transaction protocol,”Annals of Telecommunications,vol.60, (2005)530-557

[9] Microsoft Research.: MSR Elliptic Curve Cryptography Library (MSR ECCLib) (2014). http://research.microsoft.com/en-us/projects/nums

[10] Yuanling Hao, Shiwei Ma, Guanghua Chen, Xiaoli Zhang, Hui Chen, and Weimin Zeng, “Optimization algorithm for scalar multiplication in the elliptic curve cryptography over prime field,” Lecture Notes in Computer Science,vol.5226, (2008)904-911,

[11] Koblitz, N.: Elliptic Curve Cryptosystems. Mathematics of Computation 48(177), (1987) 203–209.

[12] R.M.Avanzi, C.Heuberge, and H.Prodinger,“Minimality of the hamming weight of the τ-NAF for Koblitz Curves and improved combination with point halving,” Lecture Notes in Computer Science,vol.3897, Selected Areas in Cryptography, (2006)332-344.

[13] Paterson, K.G.: ID-based Signatures from Pairings on Elliptic Curves. Electronics Letters 38(18), (2002)1025–1026.

[14] Käsper, E.: Fast Elliptic Curve Cryptography in OpenSSL. In: Danezis, G., Dietrich, S., Sako, K. (eds.) Financial Cryptography and Data Security. LNCS, vol. 7126, (2012) 27–39.