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 e-mail 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:

\[ C = E_{k_3}(D_{k_2}(E_{k_1}(M))) \]

the decryption:

\[ M = D_{k_1}(E_{k_2}(D_{k_3}(C))) \]

(2) 3-DES with two different keys

the encryption:

\[ C = E_{k_2}(D_{k_1}(E_{k_1}(M))) \]

the decryption:

\[ M = D_{k_1}(E_{k_2}(D_{k_1}(C))) \]

(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 \( \mathbb{F}_p \) be a prime finite field so that \( p \) is an odd prime number, and let \( a, b \in \mathbb{F}_p \), satisfy \( 4a^3 + 27b^2 \neq 0 \mod p \).

Then an elliptic curve \( E(\mathbb{F}_p) \) over \( \mathbb{F}_p \) defined by the parameters \( a, b \in \mathbb{F}_p \) consists of the set of solutions or points \( P = (x, y) \in \mathbb{F}_p \) to the equation:

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

together with an extra point \( \mathcal{O} \) called the point at infinity. For a given point \( P = (x, y) \in E(\mathbb{F}_p) \), \( x \) is called the \( x \)-coordinate of \( P \), and \( y \) is called the \( y \)-coordinate of \( P \). The addition operation in \( E(\mathbb{F}_p) \) is specified as follows:

\begin{enumerate}
  \item For all \( P \in E(\mathbb{F}_p) \), \( P + \mathcal{O} = \mathcal{O} + P = P \).
  \item If \( P = (x, y) \in E(\mathbb{F}_p) \), then \( (x, y) + (x, -y) = \mathcal{O} \).
  \item \( \mathcal{O} \) is called the point at infinity.
  \item Let \( P = (x_1, y_1) \in E(\mathbb{F}_p) \), then \( P + Q = (x_2, y_2) \in E(\mathbb{F}_p) \), where \( x_2 = \lambda^2 - x_1 - x_3 \mod p \), \( y_2 = \lambda(x_1 - x_3) - y_1 \mod p \) and \( \lambda = \frac{y_2 - y_1}{x_2 - x_1} \).
  \item Let \( P = (x_1, y_1) \in E(\mathbb{F}_p) \), then \( P + P = (x_2, y_2) \), where \( x_2 = \lambda^2 - 2x_3 \mod p \), \( y_2 = \lambda(x_1 - x_3) - y_1 \mod p \) and \( \lambda = \frac{y_2 - y_1}{x_2 - x_1} \).
\end{enumerate}

The performance of an elliptic curve cryptosystem depends on 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 \( w \), \( u_1 = (k_{m-1}, \ldots, k_1, k_0)_2 \), \( u_2 = (l_{m-1}, \ldots, l_1, l_0)_2 \); \( P, Q \in E(\mathbb{F}_p) \).

**output:** \( u_1P + u_2Q \).

\begin{enumerate}
  \item Compute \( iP + jQ \) for all \( i, j \in [0, 2^w - 1] \).
  \item Write \( k = (k_{d-1}, \ldots, k_1, k_0) \) and \( l = (l_{d-1}, \ldots, l_1, l_0) \), where each \( k_i \) and \( l_i \) is a bitstring of length \( w \), and \( d = \lceil m/w \rceil \).
  \item Return \( \mathcal{O} \).
  \item For \( i \) from \( d - 1 \) downto 0 do
    \[
    R \leftarrow 2^wR.
    R \leftarrow R + (k^iP + l^iQ)
    \]
  \item Return \( R \).
\end{enumerate}

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

Algorithm 2. Window NAF method for point multiplication

**input:** Integers \( k \) and \( w \), and a point \( P = (x, y) \in E(\mathbb{F}_p) \).

**output:** The point \( kP \).

\begin{enumerate}
  \item \( P_0 \leftarrow P, T \leftarrow 2^wP \).
  \item For \( i \) from 1 to \( 2^w - 1 \) do
    \[
    P_t \leftarrow P_{i-1} + T.
    \]
  \item Compute \( NAF_k(k) = (u_{i-1}, u_{i-2}, \ldots, u_1, u_0) \).
  \item \( Q \leftarrow \mathcal{O} \).
  \item For \( i \) from \( 1 \) to \( 1 \) downto 0 do
    \[
    Q \leftarrow 2Q.
    \]
    If \( u_j \neq 0 \) then
    \[
    1 \leftarrow (u_j - 1)/2
    \]
    Else \( Q \leftarrow Q + P_t \).
  \item Return \( Q \).
\end{enumerate}

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 \( \text{key}_1, \text{key}_2, \text{key}_3 \). Elliptic curve domain parameters over finite field \( \mathbb{F}_p \).

\begin{enumerate}
  \item The sender A’s private key is \( K_R \). \( 1 \leq K_R \leq n - 1 \), compute \( u = K_R \cdot U_2 \cdot K_R \cdot U_1 \cdot \cdots \cdot K_R \cdot U_1 \cdot K_R \cdot U_1 \).
  \item Write \( k = (k_{d-1}, \ldots, k_1, k_0) \) and \( l = (l_{d-1}, \ldots, l_1, l_0) \), where each \( k_i \) and \( l_i \) is a bitstring of length \( w \), and \( d = \lceil m/w \rceil \).
  \item For \( i \) from \( d - 1 \) downto 0 do
    \[
    R \leftarrow 2^wR.
    R \leftarrow R + (k^iP + l^iQ)
    \]
  \item Return \( R \).
\end{enumerate}

(1) The sender A’s private key is \( K_R \).\( 1 \leq K_R \leq n - 1 \), compute \( u = K_R \cdot U_2 \cdot K_R \cdot U_1 \cdot \cdots \cdot K_R \cdot U_1 \).

(2) Get \( \text{In} \) by M, then compute the integer e;

(3) The receiver B’s private key is \( K_R \).\( 1 \leq K_R \leq n - 1 \), compute \( (x_2, y_2) \equiv K_R \cdot P \mod n \); then user A sends \( \{u, v, w, a, r_1\} \) to user B.
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 shows the process of verify:

1. Compute \((x_1, y_1) = uKR_\alpha^{-1}\);
2. Get \(key_1, key_2, key_3\) by decrypt \(v, w, \alpha\):
   \(key_1 = vx_1^{-1}, key_2 = wx_1^{-1}, key_3 = \alpha x_1^{-1}\);
3. Compute \(u_1 = s^{-1}e \mod n; u_2 = s^{-1}r_1 \mod n\);
   \(R = u_1P + u_2KU_\alpha = (x_R, y_R)\),
   \(r_2 = \frac{x_R}{\alpha} \mod n\).

If \(s\) is the signature, then \(r_2 = r_1\).

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

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


