Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 932-936
doi:10.4028/www.scientific.net/AEF.6-7.932

A New Secure Communications Solution for Network Application

Xin Mao[1, a], Yang Liu[2,b] , Songfeng Lu[2,c] and You Li[3,d]

[1] Wuhan Qiaokou Power Supply Company, Wuhan 430034, China

[2]School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

[3]Meigujia Network Science Technologies (Shenzhen) Co., Shenzhen 518000, China

[a]1501318134@qq.com, [b]hustemily@gmail.com, [c]lusongfeng@hotmail.com, [d]evaleelb@126.com

Keywords: security architecture; elliptic curve cryptosystems; digital signature; digital envelope

Abstract. Data privacy and integrity will be the crucial and significant factors in recent times for network applications. To deal with these security problems related to symmetric and asymmetric key types have been framed. In this paper, we suggest a new secure communications solution for a secure channel that combines the digital envelopes and digital signatures and implements with symmetric key algorithm of AES and the asymmetric key algorithm of ECC. The experiment result shows it's a more perfect choice.

Introduction

Network applications, such as e-commerce and e-government have grown exponentially over the past years; the prime requirements for any electronic transactions are privacy, authentication, integrity maintenance and non-repudiation. All these are achieved through cryptographic techniques [1]. It is important how to ensure data security, the traditional digital envelope and digital signature has some lacks to some extent, can not achieve Privacy, Integrity, and non-Repudiation at the same time.

Digital envelope is one such mechanism to achieve the same. Most of the digital envelope employs RSA algorithm to encrypt and decrypt the secret key. However, the RSA itself is vulnerable. Therefore, in this research work we emphasize ECC asymmetric key technique as an alternative for RSA in the digital envelope. Cryptographic techniques are broadly classified into symmetric key cryptographic techniques and asymmetric key cryptographic techniques.

This paper combines the two techniques and implements with AES (Advanced Encryption Standard) and ECC (Elliptic Curve Cryptosystems), to construct a more perfect and secure encryption solution. The reason behind for the adoption of ECC in this approach is that, for the minimal key length, ECC provides more security than RSA.

In Section 2, digital envelopes and digital signature and their advantages and disadvantages are proposed. Moreover, there are some brief introductions to symmetric cryptosystem and asymmetric cryptosystem. Section 3 gives the improved scheme and the major algorithms of the scheme: key generation, encryption and decryption algorithm. Results and analysis are in Section 4. Finally, Section 5 is a conclusion.

Digital Envelopes and Digital Signature

Digital Envelope. Digital Envelope [2] is a hybrid cryptography which combines the symmetric cryptography and the asymmetric cryptography. According to RSA Labs, "the digital envelope consists of a message encrypted using secret-key cryptography and an encrypted secret key. Digital envelopes usually use public-key cryptography to encrypt the secret key." A common choice is to use DES (Data Encryption Standard) and RSA.

Digital Envelope has both the flexibility of asymmetric cryptography and the efficiency of symmetric cryptography, and overcomes asymmetric cryptography's key distribution problem and the symmetric cryptography's long time requiring problem.

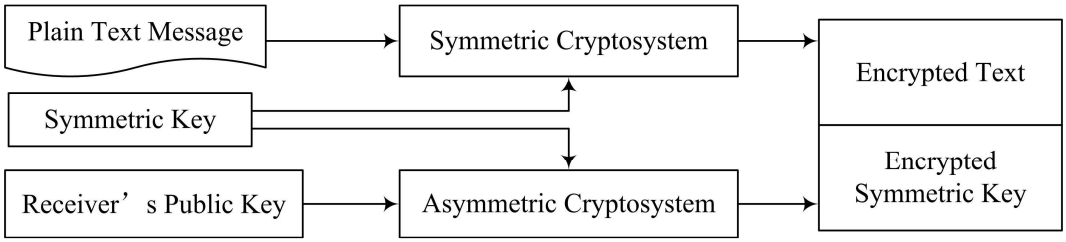

Figure 1. Encryption process of digital envelope.

Fig. 1 describes the encryption process of digital envelop. The plain data is encrypted by symmetric key at first, after that the symmetric key is encrypted by asymmetric key to get the digital envelope, that is the cipher data and the cipher key.

Digital Signature. Digital signature [3] uses asymmetric cryptography to ensure data integrity and gives the receiver reason to believe the message was sent by the claimed sender. At the same time, the sender can't deny having sending the message.

There is a pair of key: the key to sign is private, the key to verify is public. The sender uses the private key to encrypt the data while the receiver uses the public key to decrypt the data.

The asymmetric cryptography is slow in calculating, to reduce the cost; a secure one-way hash function is often called to process the message before it is signed.

Fig. 2 describes the formation of digital signature. Fig. 3 describes the verification of digital signature.

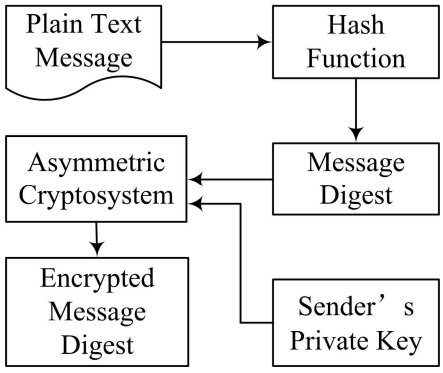

Figure 2. Formation of digital signature.

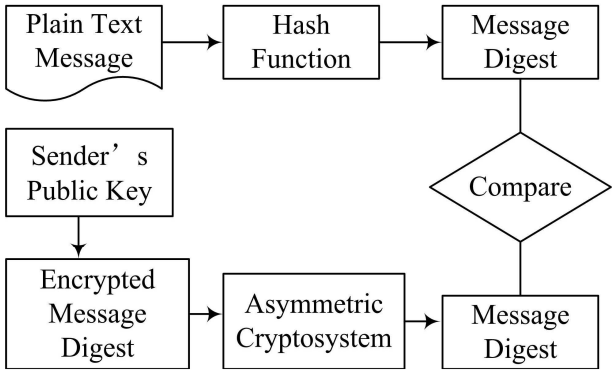

Figure 3. Verification of digital signature.

Combination. While digital envelope ensures data confidentiality, the public-key cryptography it uses makes it possible for malicious user who can't decrypt the data to destroy the data, so it is hard to ensure data's integrity and non-repudiation. At the same time, digital signature just keeps these two features because of the private-key cryptography it uses. So, the combination of digital envelope and digital signature will makes a better solution.

Cryptosystem. At present, cryptosystem used in software encryption and decryption technology is divided into symmetric cryptosystem and asymmetric cryptosystem. Symmetric cryptosystem has a key to encrypt and decrypt, the algorithm is easy to understand and implement, and has a high speed in encrypt and decrypt. But the security depends entirely on the key, if the key is lost, the system will completely not work. Asymmetric cryptosystem is also known as public-key cryptosystem, it has an encrypt key and a decrypt key, and neither the encrypt key nor the decrypt key can be deduced from the other, thus enhancing the strength of data protection. Based on the key pair, it is easy to implement digital envelope and digital signature.

Symmetric cryptosystem. DES has three parameters: key to encrypt and decrypt, data to be processed, mode to describe encrypt or decrypt. When it is encrypt mode, the data or plaintext is divided into blocks every 64-bit, the key is used for data encryption; when it is decrypt mode, the key is used for

data decryption. Brute-force method or exhaustive-key-search is often used to attack DES, which is to test a variety of keys until finally get one. With the development of computer system capabilities, DES is much weaker now. So a new encryption standard appears increasingly necessary.

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. AES has been analyzed and multi-used widely around the world and replaced DES as the most popular symmetric algorithms.

Asymmetric cryptosystem. RSA [4] is based on the big integer factorization Problem and widely used in public key encryption standard and e-commerce. Its principle is simple thus easy to implement. But with the improvement of method to decompose the big integer and computer's computing speed, the key's length has to increase to ensure the algorithm's security. It is thought that the key has to be more than 1024 bit to ensure security. At the same time, long length key causes greatly reduce of encryption and decryption speed, more complicated implement in hardware as well, it is also a burden to e-commerce who has large transactions.

ECC [5] provides the highest encryption intensity for each bit of all the known public key cryptosystem. ECC uses shorter keys to achieve the same encryption intensity with RSA. In other words, to achieve the same encryption intensity, ECC key's size is much shorter than the RSA's. ECC can achieve the same level of security with smaller key sizes and higher computational efficiency. This can effectively solve the problem of having to increase the key size to ensure encryption intensity and the implement in practice.

The Improved Scheme

The algorithm we present here combines the advantages of both symmetric and asymmetric encryption techniques.

The Improved Scheme. The data, or plaintext, is encrypted using the AES algorithm. The AES key which is used to encrypt the data is encrypted using ECC. To ensure the integrity of the data to be transmitted, the data is processed using SHA-1, a hashing algorithm, to get a message digest. Sign the digest using sender's private key, the signed digest is also encrypted using ECC.

The sender sends: a) *Ciphertext of the message M;* b) *Ciphertext of the AES key, and* c) *Ciphertext of the digest message.*

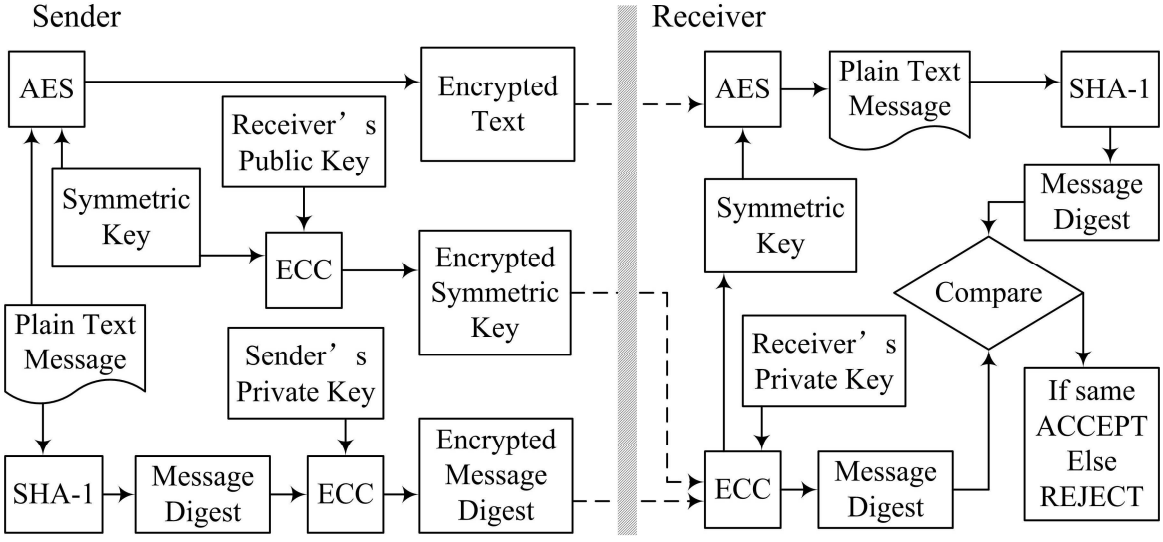

Figure 4. The improved scheme.

The receiver receives a), b) and c), first decrypts the ciphertext of the AES key to obtain the AES key. The key is then used to decrypt the ciphertext of the message to obtain the data or plaintext. The plaintext is subjected to SHA-1 hash algorithm and this gets a new message digest. The ciphertext of

the message digest is decrypted using ECC technique to obtain the message digest sent by the sender. The two message digest are compared to test whether the values are equal. If both of them are equal, the message can be accepted, else rejected. Fig. 4 shows the whole process.

Algorithm for Key Generation. The algorithm takes a security parameter x as input and outputs the public key k_a and private key k_s. Its process is as bellow:

1) Generates two cyclic groups G_{c1}, G_{c2} of prime order d and an admissible bilinear pairing $\hat{e}: G_{c1} \times G_{c1} \to G_{c2}$.
2) Picks a random generator g of G_{c1} and two hash functions $H_1 : \{0,1\}^* \to \{0,1\}^{\log_2^d}$ and $H_2 : G_{c2} \to \{0,1\}^{\log_2^d}$, where $\hat{e}$, H_1, H_2 and g are open to the public.
3) Chooses 2n + 3 random numbers $\alpha_0, \alpha_1, ..., \alpha_n, \ \beta_0, \beta_1, \ ..., \beta_n, \theta \in Z_d^*$.
4) Outputs the public key $k_a = \{g^{\alpha_0}, g^{\alpha_1}, ..., g^{\alpha_n}, g^{\beta_0}, g^{\beta_1}, ..., g^{\beta_n}, g^{\theta}, \hat{e}(g,g)\}$, where k_a is open to the public.
5) Outputs private key $k_s = \{\alpha_0, \alpha_1, ..., \alpha_n, \ \beta_0, \beta_1, \ ..., \beta_n, \theta \in Z_d^*\}$.

Encryption and Decryption Algorithm. *Encryption.* The algorithm takes the plain text message M and public key k_a as input and outputs the cipher C_M corresponds to M. The process is as bellow:

1) Chooses a generator P from G_{c1}.
2) Chooses randomly $s \in Z_d^*$, calculates $P_{\text{pub}} = s_P$.
3) Calculates $g_p = \hat{e}(k_a, P_{pub}) \in G_{c2}$.
4) Chooses randomly $r \in Z_d^*$.
5) Calculates $U = rP, V = M \oplus H_2(g_p^r)$, and then outputs cipher $C_M = <U, V>$.

Decryption. The algorithm takes the cipher C_M and private key k_s as input and outputs the plain text message M. The process is as bellow:

1) Checks whether U is belong to G_{c1}. If it is not then rejects the cipher C_M.
2) Decrypts the cipher C_M using the private key k_s: $M = V \oplus H_2(\hat{e}(k_s, U))$.

The consistency of encryption and decryption is holds, the reason is as bellow: $V \oplus H_2(\hat{e}(k_s, U)) = V \oplus H_2(\hat{e}(sk_a, rP)) = V \oplus H_2(\hat{e}(k_a, P)^{sr}) = V \oplus H_2(\hat{e}(k_a, sP)^r) = V \oplus H_2(\hat{e}(k_a, P_{pub})^r) = V \oplus H_2(g_p^r) = M$.

Experimental Results and Analysis

Experiments are conducted on a ThinkPad R400 PC with dual Intel(R) Core™2 Duo CPU @2.40GHz processor with 4GB RAM. Software components used are Windows XP operating system and Microsoft Visual 2005 compiler. The texts used in the experiments are selected randomly.

The scheme is tested with file data of sizes 1KB, 100KB, 1000KB respectively. The results of execution time are shown in Table 1 (The results of each group is the average of multiple samples).

Table 1. Execution time of the related algorithms.

File Size (KB).	AES(ms)	DES(ms)	ECC(ms)	RSA(ms)
1	246	287	31	624
100	254	280	44	6989
1000	327	652	155	59334

From the Table 1, it is clear that the performance of AES is better than DES, and ECC is superior to RSA. So the scheme combining AES and ECC is the better alternative security mechanism for the secure e-commerce channel to achieve privacy, authentication, integrity and non-repudiation.

Conclusions

In this paper, an improved scheme was proposed. The scheme combines the traditional digital envelope techniques and digital signature techniques, uses AES to replace DES in symmetric cryptosystem and uses ECC to replace RSA in asymmetric cryptosystem, so as to get a more perfect and secure encryption communication solution for network application. The experimental results show this scheme's efficiency and ensure data privacy, authentication, integrity and non-repudiation.

Acknowledgments

The authors gratefully acknowledge the support of the National Natural Science Foundation of China under Grant No. 61173050, NSAF of China under Grant No. 10876012, and the 2011 Science and Technology Project of Wuhan Power Supply Company.

References

[1] M. S. Hwang, and C. Y. Liu, Authenticated encryption schemes: current status and key issues. International Journal of Network Security, 1(2)(2005) 61-73.

[2] R. Ganesan1, M. Gobi, and K. Vivekanandan. A novel digital envelope approach for a secure e-commerce channel. International Journal of Network Security, 11(3)(2010) 121-127.

[3] R. C. Merkle. A digital signature based on a conventional encryption function, in: C. Dwork Ed., Proceedings of the 26th Annual International Cryptology Conference, Lecture Notes in Computer Science 4117, Springer, Berlin, 2006, pp. 369-378.

[4] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. in: M. Joye, J. J. Quisquater (Eds.), the 6th International Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science 3156, Springer, Berlin, 2004, pp. 925-843.

[5] I. Blake, G. Seroussi, N. Smart, Elliptic curves in cryptography, Cambridge University Press, Cambridge, 1999.