An ElGamal-Like Cryptosystem for Enciphering Large Messages

Min-Shiang Hwang, Chin-Chen Chang, *Fellow, IEEE*, and Kuo-Feng Hwang

Abstract—In practice, we usually require two cryptosystems, an asymmetric one and a symmetric one, to encrypt a large confidential message. The asymmetric cryptosystem is used to deliver secret key SK, while the symmetric cryptosystem is used to encrypt a large confidential message with the secret key SK. In this article, we propose a simple cryptosystem which allows a large confidential message to be encrypted efficiently. Our scheme is based on the Diffie-Hellman distribution scheme, together with the ElGamal cryptosystem.

Index Terms—Cryptosystems, data security, encryption, public key.

1 Introduction

Symmetric cryptosystems, such as DES [6], [9] and FEAL-32 [5], use same secret key to encrypt plaintext and to decrypt ciphertext. This means that both the sender and the receiver must have the same secret key for the cryptosystem. This presents two difficulties. One is how to distribute the secret keys privately. The other is how to manage a large number of secret keys [1], [8]. For example, if there are 50 people communicating with each other, each person must keep his/her own secret key, as well as, 49 secret keys of the other users. The advantage of symmetric cryptosystems is good performance for enciphering and deciphering, enabling them to encrypt large confidential messages.

The asymmetric cryptosystems, such as the RSA [7] and ElGamal cryptosystems [3], use different keys for encryption and decryption, respectively. The enciphering key could be published in a public directory and any user can send a confidential message to the receiver with the receiver's public enciphering key. The receiver uses his deciphering key, which is private, to decrypt the ciphertext. Asymmetric cryptosystems can solve the difficulties of symmetric cryptosystems and they are suitable for encrypting a small confidential message. However, it is time consuming when encrypting large confidential messages with an asymmetric cryptosystem.

In practice, we usually require two cryptosystems, one asymmetric cryptosystem and one symmetric cryptosystem, to encrypt a large confidential message. The asymmetric cryptosystem is used to deliver the secret key SK, while the symmetric cryptosystem is used to encrypt a large confidential message with the secret key SK. In this article, we propose a simple cryptosystem which allows a large confidential message to be encrypted efficiently. Our scheme is based on the Diffie-Hellman distribution scheme and the ElGamal cryptosystem.

This article is organized as follows: In the next section, we review the ElGamal cryptosystem and the problems that arise when it is applied to encrypt a large confidential message. In Section 3, we present an ElGamal-like cryptosystem for efficiently enciphering a large message. In Section 4, we analyze the security of our scheme. Finally, Section 5 presents our conclusions.

2 The ElGamal Cryptosystem

The ElGamal cryptosystem [3] was originally developed in 1985 and is based on the difficulty of the discrete logarithm problem for finite fields. We briefly review this cryptosystem as follows: Let P denote a large prime; g denotes a primitive element, (i.e., $g \in Z_p$), x_i denotes a secret key of the user i (u_i); r denotes a random number; and $p_i = g^{x_i} \mathrm{mod} P$ denotes a public key of u_i. Here P, g, and p_i are public information, while x_i and r are private information. Whenever, u_i wants to deliver the message m $(0 \leq m \leq P-1)$ to u_j, u_i generates a random number r and then encrypts m as below:

$$b = \quad g^r \bmod P, \tag{1}$$

$$c = \quad m \cdot p_i^r \bmod P. \tag{2}$$

u_i sends (b, c) to u_j. When u_j receives (b, c), u_j decrypts c as follows:

$$m = c \cdot (b^{x_j})^{-1} \bmod P. \tag{3}$$

Since the ciphertext c depends on both plaintext m and the random number r, the ElGamal cryptosystem is nondeterministic. In other words, a different random number r will obtain a different ciphertext c from same plaintext m.

Breaking ElGamal cryptosystem is equivalent to breaking the Diffie-Hellman [2] distribution scheme. For the encryption, two exponentiations are required and one exponentiation for decryption is needed.

However, there are two limits in the ElGamal cryptosystem. One is that the plaintext m must be less than $P-1$. The other is that the random number r cannot be used repeatedly. Otherwise, the system is not secure against the known-plaintext attack. As long as we know one pair (m, b) of (2), p_i^r is obtained. Then, the same random number r is used to encrypt other pieces of plaintext m_1 as follows:

$$c_1 = m_1 \cdot p_i^r \bmod P, \tag{4}$$

then the plaintext m_1 can be obtained by computing

$$c_1 \cdot (p_i^r)^{-1} \bmod P. \tag{5}$$

Therefore, the ElGamal cryptosystem needs to break a large plaintext into smaller pieces before enciphering, with the length of each piece being less than that of P. The ElGamal cryptosystem also needs to generate a random number r for each piece. It is obvious that the ElGamal cryptosystem is time-consuming for encrypting a large plaintext. In next section, we propose an ElGamal-like cryptosystem for enciphering a large plaintext more efficiently.

3 Our Scheme

In this section, we propose an efficient scheme for enciphering a large plaintext. Our proposed scheme is based on both the Diffie-Hellman distribution scheme [2] and the ElGamal cryptosystem [3].

The Diffie-Hellman key distribution scheme is used in our proposed scheme to generate the key pair of public and secret keys for all users u_is, for $i = 1, 2 \cdots, n$. Each user u_i randomly selects a secret key $x_i \in Z_p$ and computes the corresponding public key $p_i = g^{x_i} \mathrm{mod} P$. Here P is a large prime of length being 513 bits and g is a primitive element of $GF(P)$.

P, g, and p_i are all published information. Any user who wants to deliver a confidential message M to u_i performs the following steps:

- *M.-S. Hwang is with the Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C. E-mail: mshwang@mail.cyut.edu.tw.*
- *C.-C. Chang and K.-F. Hwang are with the Department of Computer Science and Information Engineering, National Chung Cheng University, Chaiyi, Taiwan, R.O.C. E-mail: {ccc, luda}@cs.ccu.edu.tw.*

Manuscript received 16 Oct. 1998; revised 21 Dec. 1999; accepted 16 Oct. 2000.
For information on obtaining reprints of this article, please send e-mail to: tkde@computer.org, and reference IEEECS Log Number 106778.

1. Break plaintext M into t pieces M_1, M_2, $\cdots$, M_t, each piece of length being 512 bits.
2. Generate two random numbers r_1 and r_2, where $1 < r_1, r_2 \leq P - 1$, and compute b_1 and b_2 as follows:

$$b_1 = \quad g^{r_1} \bmod P, \tag{6}$$

$$b_2 = \quad g^{r_2} \bmod P. \tag{7}$$

3. Compute $C_j, j = 1, 2, \cdots, t$, as follows:

$$C_j = M_j \cdot (p_i^{r_1} \oplus (p_i^{r_2})^{2^j}) \bmod P. \tag{8}$$

4. Send $\{b_1, b_2, C_j, j = 1, 2, \cdots, t\}$ to the receiver through a public network.

After receiving $\{b_1, b_2, C_j, j = 1, 2, \cdots, t\}$ from the sender, the receiver recovers the plaintext M by computing as follows:

$$M_j = C_j \cdot (b_1^{x_i} \oplus (b_2^{x_i})^{2^j})^{-1} \bmod P. \tag{9}$$

It should be noted that the sender generates only two random numbers r_1 and r_2 in our scheme, although the ElGamal cryptosystem requires t random numbers for t pieces of plaintext.

In addition, the computational complexity of our scheme required to encrypt t pieces of plaintext is only that required to compute four times exponentiation operations (b_1, b_2, $p_i^{r_1}$, and $p_i^{r_2}$), t times exclusive-OR operations, t times multiplication operations, and t times square operations. However, the ElGamal cryptosystem requires the computation of $2t$ times exponentiation operations (t times b and t times p_i^r) and t times multiplication operations. Since the computational complexity of computing exponentiation operations is larger than that of computing exclusive-OR and square operations, our scheme is thus preferable to the ElGamal cryptosystem for enciphering a large plaintext.

4 Security Analysis

Since our scheme is based on both the Diffie-Hellman distribution scheme [2] and the ElGamal cryptosystem [3], it is very difficult for an illegal user to compute the secret key x_i of the user u_i from the equation $p_i = g^{x_i} \bmod P$. It is also difficult for an intruder to obtain the system-generated random numbers r_1 and r_2 directly from the equations $b_1 = g^{r_1} \bmod P$ and $b_2 = g^{r_2} \bmod P$ in Step 2 of the enciphering algorithm in Section 3. The difficulty relies on the complexity of computing discrete logarithms over finite fields [3].

If an intruder knows some pairs of the plaintext and ciphertext, (M_j, C_j), the intruder can obtain $(p_i^{r_1} \oplus (p_i^{r_2})^{2^j}) \bmod P$ by solving (8) in Section 3. However, it is difficult for the intruder to obtain $p_i^{r_1}$ and $(p_i^{r_2})^{2^j}$ from the equation $(p_i^{r_1} \oplus (p_i^{r_2})^{2^j}) \bmod P$. In addition, since the intruder cannot obtain $(p_i^{r_2})^{2^j} \bmod P$, she/he cannot obtain $p_i^{r_2} \bmod P$. The security of our scheme is based on the difficulty of finding the composite exclusive-OR operation. In addition, since $(p_i^{r_1} \oplus (p_i^{r_2})^{2^j})$ is nonlinear, an illegal user will have difficulty acquiring the pieces of plaintext even though he/she can find some pairs of (M_j, C_j)s by solving (8) in Section 3. Our scheme is thus secure against the chosen-plaintext attacks.

5 Conclusions

We have proposed an ElGamal-like cryptosystem which allows a large confidential message to be encrypted efficiently. Our scheme requires the generation of only two random numbers r_1 and r_2. However, an ElGamal cryptosystem requires the generation of more random numbers for a large plaintext. We have also shown that our proposed scheme is computationally less complex than that of the ElGamal cryptosystem for enciphering a large plaintext.

Acknowledgments

The authors would like to thank the anonymous referees for their suggestions to improve this paper. Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC89-2213-E-324-001.

References

[1] D.E.R. Denning, *Cryptography and Data Security.* Mass.: Addison-Wesley, 1982.

[2] W. Diffie and Y. Hellman, “New Directions in Cryptography,” *IEEE Trans. Information Theory,* vol. 22, pp. 644-654, 1976.

[3] T. ElGamal, ”A Public-Key Cryptosystem and a Singnature Scheme Based on Discrete Logarithms,” *IEEE Trans. Information Theory,* vol. 31, no. 4, pp. 469-472, 1985.

[4] R.C. Merkle and M.E. Hellman, ”Hiding Information and Signatures in Knapdoor Knapsacks,” *IEEE Trans. Information Theory,* vol. 24, pp. 525-530, 1978.

[5] S. Miyaguchi, ”The FEAL Cipher Family,” *Proc. CRYPTO '90,* vol. 435, pp. 727-638 Aug. 1990.

[6] National Bureau of Standard. “Data Encryption Standard,” *Federal Information Processing Standards,* NBS, 1977.

[7] R.L. Rivest, A. Shamir, and L. Adleman, ”A Method for Obtaining Digital Signatures and Public Key Cryptosystems,” *Comm. ACM,* vol. 21, no. 2, pp. 120-126, Feb. 1978.

[8] B. Schneier, *Applied Cryptography.* New York: John Wiley, 1994.

[9] M.E. Smid and D.K. Branstad, ”The Data Encryption Standard: Past and Future,” *Proc. IEEE,* vol. 76, no. 5, pp. 550-559, May 1988.