An ElGamal-like Cryptosystem For Enciphering Large Messages *

Min-Shiang Hwang † Chin-Chen Chang ‡$_{IEEE\ Fellow}$ Kuo-Feng Hwang ‡

Department of Information Management †
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, TAIWAN 413 , R.O.C.
Email: mshwang@mail.cyut.edu.tw
Fax: 886-4-3742337

Department of Computer Science and Information Engineering ‡
National Chung Cheng University,
Chaiyi, Taiwan, R. O. C.
Email: ccc@cs.ccu.edu.tw

December 19, 2000

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC89-2213-E-324-001.

An ElGamal-like Cryptosystem For Enciphering Large Messages

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 fifty people communicating with each other, each person must keep his/her own secret key, as well as fourty nine 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 (ie., $g \in Z_p$); x_i denotes a secret key of the user i (u_i); r denotes a random number; and $p_i = g^{x_i} \bmod P$ 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:

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

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

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 non-deterministic. 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 Equation (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_i's, 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 $p_i = g^{x_i} \bmod P$. 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:

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.

$$\begin{aligned} b_1 &= g^{r_1} \bmod P, & (6) \\ b_2 &= g^{r_2} \bmod P. & (7) \end{aligned}$$

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, 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 4 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. S-ince 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 Equation (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 non-linear, 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 Equation (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.

Acknowledgements

The author wish to thank many 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*, Massachusetts: Addison-Wesley, 1982.

[2] W. Diffie, Y. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol.IT-22, pp. 644-654, 1976.

[3] T. ElGamal, "A public-key cryptosystem and a singnature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol.IT-31, no.4 pp. 469-472, 1985.

[4] R. C. Merkle and M. E. Hellman, "Hiding information and signatures in knapdoor knapsacks," *IEEE Transactions on Information Theory*, vol.IT-24, pp. 525-530, 1978.

[5] S. Miyaguchi, "The FEAL cipher family," in *proc. CRYPTO'90*, Lecture Notes in Computer Science, vol. 435, pp. 727–638, Aug. 1990.

[6] National Bureau of Standard, "Data encryption standard," *FIPS,* NBS, 1977.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] Bruce Schneier, *Applied Cryptography*, New York: John Wiley & Sons, 1994.

[9] M.E. Smid and D.K. Branstad, "The data encryption standard: past and future," *Proc. of the IEEE*, vol. 76, no. 5, pp. 550–559, May 1988.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He is currently the Head and Associate Professor of the Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. Dr. Hwang's current research interests include database and data security, cryptography, image compression, and mobile communications.

Chin-Chen Chang was born in Taichung, Taiwan, Republic of China, on November 12, 1954. He received his B.S. degree in applied mathematics in 1977 and his M.S. degree in computer and decision sciences in 1979 from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in Computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. During the academic years 1980-83, he was on the faculty at the Department of Computer Engineering at National Chiao Tung University. From 1983-1989, he was on the faulty at the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head and professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. Since August 1995, he has been the dean of Academic Affairs at National Chung Cheng University. In addition, he was served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, coding theory, and data structures. Dr. Chang is the associate editor of Computer Quarterly, Journal of Computers, Journal of the Chinese Institute of Engineers, Journal of Electrical Engineering, International Journal on Policy and Information, Journal of Information and Management Science, Journal of Information Science and Engineering, and is the regional editor of Information Sciences Applications and Editor-in-Chief of Journal of Information and Education. He was elected as an outstanding youth of the Republic of China in 1984. In the same year, he was also elected as an Outstanding Talent in Information Science of the Republic of China. He obtained the 1986-1987, 1988-1989, 1990-1991, 1992-1994, 1995-1996 Distinguished Research Awards of the National Science Council of the Republic of China. He also obtained from the Chung-Shan Academic Foundation of the Republic of China the 1987 Chung-Shan Academic Publication Award. He was the winner of the 1990, 1991, and 1992 AceR Long Term Award for Outstanding M.S. Thesis Supervision, the 1991 AceR Long Term Award for Outstanding Ph.D. Dissertation Study Supervision. He was the winner of the Best Paper Award at the Second International Conference on CISNA sponsored by the British Council. He was also the winner of the 1992 Outstanding Teaching Materials Award of the Ministry of Education of the Republic of China. Dr. Chang has published more than one hundred papers in well-known journals and ten books in the fields of

Databases Design, Data Structures, Information Security and Cryptography in Chinese. Dr. Chang is a senior member of the IEEE, and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Cryptologic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Society of the Republic of China and he is also the Chairman of the Executive Committee in the Information Security Society of the Republic of China.

Kuo-Feng Hwang received the B.S. in Construction Engineering from National Lien-Ho College of Technology and Commerce, Taiwan, Republic of China, in 1991; the M.S. in Information Management from Chaoyang University of Technology, Taiwan, in 1999; He is currently pursuing his Ph.D. degree in Department of Computer Science and Information Engineering, at Nation Chung Cheng University. His research interests include cryptography, image Processing, and Information Management.