Cryptanalysis of an ElGamal-Like Cryptosystem for Enciphering Large Messages

YUH-DAUH LYUU
Dept. of Computer Science & Information Engineering and Dept. of Finance
National Taiwan University
No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan

MING-LUEN WU
Dept. of Computer Science & Information Engineering
National Taiwan University
No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan
and
Dept. of Information Management
Chung-Yu Institute of Technology
No. 40, Yi-7th Rd, Keelung, Taiwan

Abstract: - In 2002, Hwang et al. propose an asymmetric cryptosystem in which a large message is broken into smaller plaintexts which are then encrypted efficiently. They claim that based on the assumption of the intractability of the discrete logarithm problem, their cryptosystem is secure in the sense that even knowing some pairs of plaintext-ciphertext does not allow an intruder to acquire other plaintexts easily. This paper disproves this claim.

Key-Words: - Asymmetric cryptosystem, ElGamal cryptosystem, Cryptanalysis, Discrete logarithm, Order of element.

1 Introduction

Asymmetric cryptosystems solve the key-exchange problem associated with symmetric cryptosystems. However, asymmetric cryptosystems such as the RSA [6] and ElGamal cryptosystems [2] are less efficient than symmetric cryptosystems such as DES [3] and Rijndael [1]. When a large message is segmented into many smaller plaintexts which are then encrypted individually, the performance penalty is multiplied. Segmentation is needed because the size of a plaintext to be encrypted must be smaller than the modulus of the cryptosystem to have any hope of being uniquely decrypted.

In 2002, Hwang et al. propose an ElGamal-like asymmetric cryptosystem that allows a large message to be enciphered efficiently [4]. They claim that based on the assumption of the intractability of the discrete logarithm problem, their cryptosystem is secure because even know-

ing some pairs of plaintext-ciphertext does not allow an intruder to acquire other plaintexts easily. This paper shows that their claim does not hold over several popular finite fields if the message is long enough.

2 The Cryptosystem of Hwang et al.

Assume the sender $\mathcal{S}$ wants to send a message M to the receiver $\mathcal{R}$. Their scheme works as follows.

1. **Key generation:** $\mathcal{R}$ picks a large prime p and a primitive root g modulo p. He also chooses a random exponent $\alpha \in \mathbb{Z}_p$ and computes $\beta = g^\alpha \bmod p$. $\mathcal{R}$'s public key is (g, p, β) and the secret key is α.

2. **Encryption:** $\mathcal{S}$ breaks message M into n plaintexts $M_1, M_2, \ldots, M_n$, each $\lfloor \log_2 p \rfloor$ bits long. Note $0 \le M_i < p$. $\mathcal{S}$ then chooses two random exponents r_1 and r_2 with $1 < r_1, r_2 \le p-1$ and computes $R_1, R_2, C_1, C_2, \ldots, C_n$ according as

$$\begin{aligned} R_1 &= g^{r_1} \bmod p, \\ R_2 &= g^{r_2} \bmod p, \\ C_i &= M_i \cdot (\beta^{r_1} \oplus (\beta^{r_2})^{2^i}) \bmod p. \end{aligned}$$

   Above, β^{r_1} and $(\beta^{r_2})^{2^i}$ are calculated in modulo p, and $\oplus$ is the bit exclusive-OR operation. The whole encrypted message is $(R_1, R_2, C_1, C_2, \ldots, C_n)$. $\mathcal{S}$ sends it to $\mathcal{R}$ through a public network.

3. **Decryption:** After receiving

$$(R_1, R_2, C_1, C_2, \ldots, C_n),$$

   $\mathcal{R}$ reconstructs the plaintexts M_i as

$$M_i = C_i \cdot (R_1^\alpha \oplus (R_2^\alpha)^{2^i})^{-1} \bmod p.$$

   Above, R_1^α and $(R_2^\alpha)^{2^i}$ are calculated in modulo p.

3 Our Cryptanalysis

We will show that the cryptosystem of Hwang et al. is insecure if (1) n exceeds the order of 2 modulo q and (2) p is of the form $2^e q+1$, where q is a large prime and e is a positive integer. Note that the discrete logarithm problem over $\mathbb{Z}_p$ is generally regarded as difficult because $p-1$ has at least one large prime factor q [7]. In the following we demonstrate that if an intruder knows one pair of plaintext-ciphertext, he can acquire certain other plaintexts.

Let the order of 2 modulo q be d. An intruder can solve for d using, e.g., the efficient Algorithm 4.79 of [5]. By definition, $2^d - 1 \equiv 0 \pmod q$. Then $2^e(2^d - 1) \equiv 0 \pmod{2^e q}$. So $2^{e+d} \equiv 2^e \pmod{2^e q}$. This implies that the period of the sequence $2^e, 2^{e+1}, 2^{e+2}, \ldots$ modulo $2^e q$ is d.

Next we show that given a plaintext-ciphertext pair (M_{e+a}, C_{e+a}) where $0 \le a \le n-e$, the intruder can reconstruct all M_{e+i} where $0 \le i \le n-e$ and $i \equiv a \pmod d$. As $C_{e+a} = M_{e+a} \cdot (\beta^{r_1} \oplus (\beta^{r_2})^{2^{e+a}}) \bmod p$, the intruder can calculate

$$(\beta^{r_1} \oplus (\beta^{r_2})^{2^{e+a}}) \equiv C_{e+a} M_{e+a}^{-1} \pmod p.$$

As $2^{e+a} \equiv 2^{e+i} \pmod{2^e q}$, we have

$$\begin{aligned} (\beta^{r_1} \oplus (\beta^{r_2})^{2^{e+i}}) &\equiv (\beta^{r_1} \oplus (\beta^{r_2})^{2^{e+a}}) \\ &\equiv C_{e+a} M_{e+a}^{-1} \pmod p. \end{aligned}$$

Recall that $C_{e+i} = M_{e+i} \cdot (\beta^{r_1} \oplus (\beta^{r_2})^{2^{e+i}}) \bmod p$. Hence, the intruder is able to decrypt C_{e+i} as $M_{e+i} = C_{e+i}(C_{e+a} M_{e+a}^{-1})^{-1} \bmod p$.

Note in particular that if $p = 2q+1$ and if the intruder knows (M_1, C_1), (M_2, C_2), …, (M_d, C_d), then he is capable of finding all plaintexts M_1, M_2, …, M_n, thus the original message M.

4 Conclusions

In this paper, we have shown that the cryptosystem of Hwang et al. is insecure if the number of plaintexts n exceeds the order of 2 modulo q and the prime modulus p is chosen to be of the form $2^e q$, where e is a positive integer and q is a prime. This implies that the security claim in their paper does not hold in general.

References

[1] J. Daemen and V. Rijmen, "Rijndael, the advanced encryption standard," *Dr. Dobb's Journal*, vol. 26, no. 3, pp. 137–139, 2001.

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

[3] FIPS 46, "Data encryption standard." Federal Information Processing Standard Publication 46, US department of commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977.

[4] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

[5] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1997.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *CACM*, vol. 21, pp. 120–126, Feb. 1978.

[7] V. Shoup, "Lower bounds for discrete logarithms and related problems," in *Advances in Cryptology—EUROCRYPT '97*, vol. 1233 of *LNCS*, pp. 256–266, Springer-Verlag, 1997.