JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 18, 341-344 (2002)

Short Paper

Remarks on Using RSA With Low Exponent in a Public Network

WEI-HUA HE, TZONG-CHEN WU* AND CHIH-YIN LIN**
Department of Information Management
Chaoyang University of Technology
Taichung, 413 Taiwan
E-mail: whhe@mail.cyut.edu.tw
**Department of Information Management*
National Taiwan University of Science and Technology
Taipei, 106 Taiwan
E-mail: tcwu@cs.ntust.edu.tw
***Institute of Information Management*
National Chiao Tung University
Hsinchu, 300 Taiwan
E-mail: u8534502@cc.nctu.edu.tw

The authors give a counterexample to show that the RSA-based cryptosystem with low exponent proposed by Lee and Chang (*Computer Communications* 21 (1998)) is vulnerable to the low exponent attack with respect to their suggested lower boundary for the size of the public encryption key. That is, an eavesdropper can recover the plaintext from the ciphertext without knowing the secret decryption key, even though the size of the secret decryption key is large enough. The authors also suggest a new lower boundary for the size of the public encryption key for the Lee-Chang cryptosystem to enforce secrecy.

Keywords: RSA, public key system, low exponent attack, encryption key, lower boundary

1. INTRODUCTION

Consider a scenario in which a sender wants to use the well-known RSA cryptosystem [1] to secretly send the same message to a group of receivers via a public network. One simple way to achieve this goal is for the sender to use each recipient's public key to encrypt the same message using RSA, and then to send the ciphertext to that receiver. However, in 1985, Hastad [2] proposed a well-known low exponent attack against the RSA-based cryptosystem with a small-size public key. The low exponent attack is described as follows. Let (e_i, n_i) be the public key, and let d_i be the private key for user U_i defined by RSA. Consider a case in which a message m is encrypted with the same pub-

Received January 5, 2000; revised November 6, 2000; accepted February 13, 2001.
Communicated by Michael R. Lyu.

lic key $e_1 = e_2 = e_3 = 3$ (with different moduli n_1, n_2, n_3) and the corresponding ciphertext $c_i = m^{e_i} \bmod n_i$ (for $i = 1, 2, 3$) is sent to three recipients U_1, U_2, U_3. If an eavesdropper intercepts the ciphertext c_1, c_2, c_3, then he/she can easily compute $c = m^3 \bmod(n_1 \cdot n_2 \cdot n_3)$ using the Chinese remainder theorem and thereby obtain m by simply calculating the cube root of c without knowing the private keys d_1, d_2, d_3.

Recently, Lee and Chang [3] proposed an RSA-based cryptosystem with low exponent and claimed that their cryptosystem can withstand the low exponent attack. One feature of the Lee-Chang cryptosystem is that the sender of a message can dynamically change the size of the public key, i.e., the encryption key, which is determined by the lower boundary according to the number of recipients. Meanwhile, each recipient can use his/her private key to derive the corresponding decryption key to recover the message from the ciphertext. In this paper, we will first give a counterexample to show that the Lee-Chang cryptosystem is still vulnerable to the low exponent attack with respect to their suggested lower boundary for the size of the public encryption key. We will then suggest a new lower boundary for the size of the public encryption key for the Lee-Chang cryptosystem to enforce secrecy.

2. LEE-CHANG CRYPTOSYSTEM

The RSA-based cryptosystem with low exponent, proposed by Lee and Chang [3], is described in the following. For system setup, each user U_i selects two large primes p_i and q_i, and computes $n_i = p_i \cdot q_i$ and $d_i = e_i^{-1} \bmod (p_i - 1)(q_i - 1)$, where $e_i = 3$. After that, U_i publishes (e_i, n_i) as his/her public key while keeping p_i, q_i and d_i secret. Here, d_i is the secret key for U_i. Suppose that user U_0 wants to secretly send a message m to users U_1, U_2, …,U_t in a public network. For the recipients to be able to successfully recover m without message-loss, m should satisfy the following conditions: $m < n_i$ and $m^3 > n_i$ (for $i = 1, 2, \ldots, t$). Before performing the encryption operation, U_0 first determines the public encryption key $E = 3^h$, where

$$h = \left\lceil \frac{1 + \log_2 t}{2 \log_2 3} \right\rceil. \tag{1}$$

U_0 then computes the ciphertext for m as $C = m^E \bmod(n_1 \cdot n_2 \cdot \ldots \cdot n_t)$ and broadcasts C to these t recipients. Upon receiving the ciphertext C, each recipient U_i first determines h using Eq. 1 and then computes the secret decryption key $D_i = (d_i)^h \bmod(p_i - 1)(q_i - 1)$ and an intermediate ciphertext $C_i = C \bmod n_i$. After that, U_i recovers m by computing $m = (C_i)^{D_i} \bmod n_i$. From Eq. 1, it can be seen that the lower boundary for the size of the public encryption key, i.e., h, only depends on the number of recipients designated by the sender.

3. NEW LOWER BOUNDARY FOR THE PUBLIC ENCRYPTION KEY

Hastad pointed out that a user can send linearly related messages, instead of sending the same message, to many users to guard against the low exponent attack [2]. He also

obtained the corollary that sending more than $E(E + 1)/2$ linearly related messages may enable an eavesdropper to recover these messages, where $E = 3^h$ is the public encryption key and h is the low boundary determined by the number of recipients and the size of the message to be encrypted. This means that the RSA-based cryptosystem with the public encryption key E is breakable if the eavesdropper intercepts more than $E(E + 1)/2$ linearly related messages. Notice that any RSA-based cryptosystem using the public encryption key $> 3^h$ is not necessarily breakable.

In the following, we will give a counterexample to show that the lower boundary for the size of the public encryption key suggested by Lee and Chang does not provide adequate security against the low exponent attack. Suppose that U_0 wants to send a message m to four recipients U_1, U_2, U_3, U_4. In this case, we have $t = 4$, $h = \left\lceil \frac{1+\log_2 t}{2\log_2 3} \right\rceil = \left\lceil \frac{1+\log_2 4}{2\log_2 3} \right\rceil = \left\lceil \frac{3}{3.17} \right\rceil = 1$ and $E = 3^h = 3$. Recall that $m < n_i$ and $m^3 > n_i$ (for $i = 1, 2, \ldots, t$), which implies that $m^3 < n_1 \cdot n_2 \cdot n_3 \cdot n_4$. Thus, an eavesdropper can easily recover m by computing the cube root of $C = m^3 \bmod (n_1 \cdot n_2 \cdot n_3 \cdot n_4)$. Therefore, the Lee-Chang cryptosystem is still vulnerable to the low exponent attack.

In order to withstand the low-exponent attack stated above, the lower boundary for the size of the public encryption key for the Lee-Chang cryptosystem should be raised. That is, the public encryption key E should satisfy the condition $m^E > n_1 \cdot n_2 \cdot \ldots \cdot n_t$, which implies that $E > \frac{\log_2 (n_1 \cdot n_2 \cdot \ldots \cdot n_t)}{\log_2 m}$. Consequently, the lower boundary for the size of E is adjusted as follows:

$$h = \left\lfloor \log_3 \left(\frac{|n_1 \cdot n_2 \cdot \ldots \cdot n_t|}{|m|} \right) \right\rfloor + 1, \tag{2}$$

where $|x|$ denotes the bit length of x. As a result, it is computationally infeasible (that is, as difficult as it is to break the RSA scheme) for the eavesdropper to find the E^{th} root of C. From Eq. 2, it can be seen that h depends not only on the number of recipients, but also on the size of the message to be encrypted. Furthermore, if we let $|m| = |n_1| = |n_2| = \ldots = |n_t|$, then Eq. 2 can be further simplified to obtain $h = \lfloor \log_3 t \rfloor + 1$, which is always greater than the lower boundary suggested by Lee and Chang when $t > 2$.

4. CONCLUDING REMARKS

We have given a counterexample to show the Lee-Chang RSA-based cryptosystem cannot withstand the low exponent attack with respect to their suggested lower boundary for the size of the public encryption key. Our suggested new lower boundary for the size of the public encryption key depends not only on the number of recipients, but also on the size of the message to be encrypted. Furthermore, our suggested new lower boundary is always larger than that suggested by Lee and Chang when the number of recipients is larger than two. It can be easily verified that our suggested new lower boundary actually minimizes the size of the public encryption key required in the RSA-based cryptosystem when a low exponent is used, while still enforcing secrecy.

REFERENCES

1. R. L. Rivest, A. Shamir, and L. Adelman, "A method for obtaining digital signature and public key cryptosystem," *Communications of the ACM*, Vol. 21, 1978, pp. 120-126.
2. J. Hastad, "On using RSA with low exponent in a public key network," *Advances in Cryptology – CRYPTO'85*, Springer-Verlag, 1985, pp. 403-408.
3. W. B. Lee and C. C. Chang, "Using RSA with low exponent in a public network," *Computer Communications*, Vol. 21, 1998, pp. 284-286.

Wei-Hua He (何煒華) received the B.S. in Applied Mathematics from Chinese Culture University, Taiwan, Republic of China, in 1992. He received the M.S. and Ph.D. degrees in Information Management from National Taiwan University of Science and Technology, Taiwan, Republic of China, in 1994 and 2000, respectively. He obtained the 2000 Acer Long Term Thesis Award. He is currently an assistant professor in the Department of Information Management, Chaoyang University of Technology, Taiwan, Republic of China, and is a member of Chinese Information Security Association. His current research interests include cryptography and information security.

Tzong-Chen Wu (吳宗成) received the B.S. degree in Information Engineering from National Taiwan University in 1983, the M.S. degree in Applied Mathematics from National Chung Hsing University in 1989, and the Ph.D. in Computer Science and Information Engineering from National Chiao Tung University in 1992. From August 1992 to January 1997, he has been the associate professor at the Department of Information Management, National Taiwan University of Science and Technology (NUTST). Since February 1997, he has been the professor at the Department of Information Management, NTUST. Professor Wu now is the chairman of the Department of Information Management, NTUST, and also the members of IEEE, ACM, and the Chinese Cryptology and Information Security Association (CCISA). His current research interests include data security, cryptography, network security, and data engineering.

Chih-Yin Lin (林之寅) received the B.S. degree in Computer Science and Information Engineering from Catholic Fu-Jen University, Taiwan, Republic of China, in 1996. He is now a Ph.D. student in the Institute of Information Management, National Chiao Tung University, Taiwan, Republic of China. His current research interests include cryptography, information security, and Internet laws.