A New Method to Strengthen Ciphers

Min-Shiang Hwang S. Wesley Changchien Cheng-Chi Lee

Department of Information Management
Chaoyang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw

August 6, 2002

Abstract: This article discusses a known-plaintext attack on a strengthened ciphers method proposed by Georgiou. We also propose a scheme for extending strengthen ciphers so that the security will be greatly improved. Our scheme is efficient and easy to implement for mobile communications.
Key Words: Cipher, Cryptography, Security, Smart Card.

1 Introduction

In 1989, Georgiou proposed a method, called "A" cipher [3] which is a formalization of the Aryabhata cipher [7], to strengthen ciphers based on a combination of a given one-to-one enciphering transformation and a multiplication. His enciphering method is a lot easier and faster to implement than other traditional cryptosystems.

In 1991, Desmedt [2] demonstrated that if the enciphering transformation is a homomorphism and the multiplication in the domain is used in the "A" cipher and the multiplication in the range is known to the cryptanalyst, Georgiou's method does not strengthen the cipher at all. However, Desmedt did not present a method to attack Georgiou's enciphering method. In this article, we show that Georgiou's enciphering method cannot withstand a known-plaintext attack when cryptanalyst knows a few pairs of (plaintext, ciphertext). Furthermore, we propose an extended scheme which are a slight modification of the Georgious's scheme. The proposed scheme not only retains the advantages of the Georgiou's scheme, but also enhances the security.

2 The "A" Cipher

Let f be a rule (an encryption function), $f : M \longrightarrow C$, M be a message space, C be a ciphertext space, and m be a message, $m \in M$. Using the "A" cipher, m is written as

$$m = r_1 * r_2 * \cdots * r_k, \tag{1}$$

where $*$ is a simple operation such as addition modulo an integer at each digit position. Note that $*$ is elected to be public. Moreover, $r_i \in M$, $r_1, r_2, \cdots, r_{k-1}$ are chosen randomly and r_k is calculated such that Equation (1) is satisfied. The ciphertext $c \in C$ in the "A" cipher is as follows.

$$c = (f(r_1), f(r_2), \cdots, f(r_k)).$$

3 The Weakness of The "A" Cipher

Now we show the weakness in security of the "A" cipher method. Let operation $*$ be an addition modulo n at each digit position; m be a message with t digits whose range are from 0 to n; m_j, $j = 1, 2, \cdots, t$, in the range of 0 to n, be the jth position at m; r_i, $i = 1, 2, \cdots, k$, be a random; r_{ij}, $i = 1, 2, \cdots, k$, $j = 1, 2, \cdots, t$ be the jth position at r_i; and f be a secret rule of one-to-one transformation.

Using the "A" cipher, the message

$$m_j = \sum_{i=1}^{k} r_{ij} \bmod n, \quad j = 1, 2, \cdots, t.$$

The ciphertext

$$c_j = (f(r_{1j}), f(r_{2j}), \cdots, f(r_{kj})), \quad j = 1, 2 \cdots, t.$$

If enough message m are known, the secret rule f can be derived by solving the following equation simultaneously.

$$m_j = f^{-1}(r_{1j}) + f^{-1}(r_{2j}) + \cdots + f^{-1}(r_{kj}), \quad j = 1, 2 \cdots, t,$$

where f^{-1} is an inverse rule of f. Since there are at most n unknown variables $f(\cdot)$ in the above equation, we can solve the equation when we known $\lceil n/t \rceil$ messages.

We give an example to illuminate the weakness of the "A" cipher as follows. For $m = 1413$, $k = 3$, and the message space is all the 4-digit numbers. $*$ is defined as addition modulo 5 at each digit position. Rule f is given in Figure 1. Choosing $r_1 = 1030$ and $r_2 = 0143$, it follows that $r_3 = 0340$ such that Equation (1) is satisfied as follows:

$$\begin{aligned} m_1 &= r_{11} + r_{21} + r_{31} \bmod 5 \\ 1 &= 1 + 0 + r_{31} \bmod 5. \end{aligned}$$

We obtain the first digit number $r_{31} = 0$ from the above equation. In the similar method, we obtain the second digit number $r_{32} = 3$. The third and fourth digit numbers are 4 and 0, respectively. Therefore, $r_3 = r_{31}r_{32}r_{33}r_{34} = 0340$.

$$\begin{array}{ccc} 0 & \longleftrightarrow & 4 \\ 1 & \longleftrightarrow & 3 \\ 2 & \longleftrightarrow & 1 \\ 3 & \longleftrightarrow & 0 \\ 4 & \longleftrightarrow & 2 \end{array}$$

Figure 1: Rule f. Each digit of each side is transformed to its corresponding one of the other side.

Next, we use the rule f in Figure 1 for transforming r_1, r_2, and r_3 to ciphertext c_1, c_2, and c_3, respectively. The ciphertext is as follows: $c_1 = 3404$, $c_2 = 4320$, $c_3 = 4024$. For convenience, we let a_i be $f^{-1}(i)$, an inverse rule of f, for $i = 0, 1, \cdots, 4$. Whenever we know the message $m = 1413$ and the ciphertext $(3404, 4320, 4024)$, the rule f in Figure 1 can be revealed by solving the following equations simultaneously.

$$\begin{cases} 1 & \equiv a_3 + a_4 + a_4 (\mathrm{mod} 5), \\ 4 & \equiv a_4 + a_3 + a_0 (\mathrm{mod} 5), \\ 1 & \equiv a_0 + a_2 + a_2 (\mathrm{mod} 5), \\ 3 & \equiv a_4 + a_0 + a_4 (\mathrm{mod} 5). \end{cases}$$

We obtain $a_0 = 3$, $a_2 = 4$, $a_3 = 1$, and $a_4 = 0$ from the above equations. Since, the rule f is a one-to-one mapping function, we obtain $a_1 = 2$. Therefore, the rule f in Figure 1 can be revealed.

4 Our Scheme

Shannon proposed two encryption techniques to strengthen ciphers: confusion and diffusion [1, 4]. Since Georgiou only diffuses the plaintext and does not include any process of confusion, his approach is not secure when the cryptanalyst has knowledge of the pairs of plaintext and corresponding ciphertext.

To enhance the security, we propose an extended scheme which improves of the Georgiou's cipher scheme for withstanding this type of attack as follows. The main idea is that the secret key (rule; f) is a variable for each session. The secret key is embedded in smart card or SIM (Subscriber Identity Module) for mobile communications [5, 6, 8, 9]. The secret key, $f : M * S \longrightarrow C$, where f is a one-to-one and onto function; M is a message space with 64-bit in length; S is a session parameter (session key); C is a ciphertext space with 64-bit in length; $*$ is a simple operation such as exclusion-OR. We assume that Alice wants to send a confidential message M to Bob. We let the message $M = m_1 \| m_2 \| \cdots \| m_t$, where $m_i, i = 1, 2, \cdots, t$, is a 64-bit string; $\|$ denotes a concatenation. Alice encrypts the message M as follows.

1. Encrypt the pieces of plaintext (m_i), $m_i \in M$. Using the "A" cipher, m_i is written as

$$m_i = r_{i1} \oplus r_{i2} \oplus \cdots \oplus r_{ik}, \tag{2}$$

   where $\oplus$ is an exclusive-OR operation; $r_{ij} \in M$, $r_{i1}, r_{i2}, \cdots, r_{i(k-1)}$ are chosen randomly and r_{ik} is calculated such that Equation (2) is satisfied.

2. Generate ciphertext (c_i), $c_i \in C$ in the "A" cipher is as follows.

$$c_i = (f(r_{i1}, S), f(r_{i2}, S), \cdots, f(r_{ik}, S)),$$

   where S is a session key between Alice and Bob.

3. Repeat Steps 1 and 2 to generate block of ciphertext c_2, c_3, $\cdots$, and the last block of ciphertext (c_t).

After receiving these ciphertexts $c_i, i = 1, 2, \cdots, t$, from Alice, Bob decrypts c_i as follows. First, Bob obtains $r_{ij}, j = 1, 2, \cdots, t$ by computing $f^{-1}(c_i)$. Next, Bob obtains the piece of the message m_i using Equation (2). Therefore, the confidential message M can be derived by concatenating $m_i, i = 1, 2, \cdots, t$.

5 Conclusion

We have shown Georgiou's scheme cannot withstand a known-plaintext attack when an attacker knows a few pairs of (plaintext, ciphertext). We also have proposed an extended scheme which are a slight modification of the Georgiou's scheme. The proposed scheme not only retains the advantages of the Georgiou's scheme, but also enhances the security. Our improved scheme is efficient and easy to implement for mobile communications.

References

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

[2] Y. G. Desmedt. The 'a' cipher does not necessarily strengthen security. *Cryptologia*, 15:203–206, 1991.

[3] G. Georgiou. A method to strengthen ciphers. *Cryptologia*, 13:151–160, 1989.

[4] M. S. Hwang. A new redundancy reducing cipher. *International Journal of Informatica*, 11:435–440, 2000.

[5] M. S. Hwang and C. H. Lee. Authenticated key-exchange in a mobile radio network. *European Transactions on Telecommunications*, 8:265–269, 1997.

[6] M. S. Hwang and W. P. Yang. Conference key distribution protocols for digital mobile communication systems. *IEEE Journal on Selected Areas in Communications*, 13:416–420, 1995.

[7] S. Kak. The aryabhata cipher. *Cryptologia*, 12:113–117, 1988.

[8] C. H. Lee, M. S. Hwang, and W. P. Yang. Enhance privacy and authentication for the global system of mobile communications. *Wireless Networks*, 5:231–243, 1999.

[9] C. H. Lee, M. S. Hwang, and W. P. Yang. A novel application of phone card and its authentication in mobile communications. *Journal of Information Science and Engineering*, 15:471–484, 1999.