การปรับปรุงรหัสลับเชิงเส้นโดยใช้ตารางสาธารณะ คู่ของมอดุลัส และกุญแจแบบเป็นคาบ

An Improvement of Linear Cipher Using Public Tables, Pairs of Moduli, and Periodic Keys

สุกัญญา โฮมวงศ์ และ ทศพร ทองจันทึก*

Sukanya Homwong and Thotsaphon Thongjunthug*

ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

Department of Mathematics, Faculty of Science, Khon Kaen University

Received : 19 February 2018

Accepted : 10 June 2018

Published online : 2 July 2018

บทคัดย่อ

บทความวิจัยนี้นำเสนอวิธีการหนึ่งในการปรับปรุงรหัสลับเชิงเส้นโดยใช้ตารางสาธารณะ ซึ่งมีเพียงผู้รับเท่านั้นที่สามารถใช้ถอดรหัสลับได้ และคู่ของมอดุลัสเพื่อป้องกันมิให้บุคคลภายนอกหากุญแจส่วนตัวได้สำเร็จ วิธีการที่นำเสนอนี้ยังได้ใช้กุญแจแบบเป็นคาบในการเข้ารหัสลับแต่ละบล็อกของข้อความปกติและในการถอดรหัสลับแต่ละบล็อกของข้อความรหัสลับ ผลการศึกษาพบว่า รหัสลับเชิงเส้นที่ปรับปรุงใหม่มีความปลอดภัยต่อการวิเคราะห์ความถี่ การโจมตีแบบทราบข้อความรหัสลับเท่านั้น และการโจมตีแบบทราบข้อความปกติ มากกว่ารหัสลับเชิงเส้นแบบดั้งเดิม

คำสำคัญ : วิทยาการเข้ารหัสลับ, รหัสลับเชิงเส้น, กุญแจแบบเป็นคาบ, คู่ของมอดุลัส, ตารางสาธารณะ

Abstract

In this paper, we propose an improvement of the linear cipher using a public table, which can be used for decryption only by the recipient, and a pair of moduli to prevent successful determination of the private keys by the opponent. Our scheme also uses a periodic key for encrypting each block of plaintext and decrypting each block of ciphertext. We find that our modified linear cipher is more secure against frequency analysis, a ciphertext-only attack, and a known-plaintext attack than the classical linear cipher.

Keywords : cryptography, linear cipher, periodic key, pair of moduli, public table

***Corresponding author. E-mail** : thotho@kku.ac.th

Introduction

The *linear cipher* (also known as the *affine cipher*) is a symmetric cipher system in which each letter in the plaintext is encrypted mathematically by the function

$$E(P) = (aP + b) \bmod n, \tag{1}$$

where

- n is the number of letters in the alphabet system;
- P is the numerical value associated to each plaintext letter; and
- a and b, the *private keys* of the cipher, are integers with $\gcd(a, n) = 1$

(Burton, 2007; Stinson, 2006). The linear cipher with $a = 1$ is simply the *shift cipher*, for the encrypting function simply reduces to a linear shift (Stinson, 2006). In particular, the *Caesar cipher*, one of the earliest cryptographic systems circa 50 BC, is simply a special case of the linear cipher where $a = 1$ and $b = 3$ (Burton, 2007).

As a monoalphabetic cipher, the primary weakness of the linear cipher is its vulnerability to a *known-plaintext attack*: if an opponent can discover the plaintext of two ciphertext letters, then the keys a, b can be recovered by solving a system of linear congruences. Moreover, since $\gcd(a, n) = 1$, one can discard many "false" keys rapidly using an automated system.

For the Caesar cipher, several modifications have been proposed. Singh *et al.* (2012) proposed a combination of the Caesar cipher and rail fence techniques with stack method for making the communication more secure. Senthil *et al.* (2013) proposed a modified version of the Caesar cipher involving a prime divisor and its primitive roots, which leads to non-uniform shifts and substitutions. Rajan and Balakumaran (2014) proposed an advancement in the Caesar cipher by changing the entire order of alphabets before re-encrypting the first ciphertext using delta formation technique. Nevertheless, an improvement of the linear cipher in general is still less satisfactory.

In this paper, we will propose a modification of the linear cipher, which involves the creation of a public conversion table, the use of a pair of different moduli in computation, and the use of a periodic key for encryption and decryption. In addition, we will discuss the security of our modified linear cipher against frequency analysis, a ciphertext-only attack, and a known-plaintext attack.

Methods

1. The linear cipher

Before we proceed to the development of our modified cipher, we shall first explore the linear cipher in detail, particularly its encryption and decryption functions and its vulnerability to a known-plaintext attack.

The linear cipher is a *monoalphabetic cipher*, that is, an encryption scheme in which each letter of the original plaintext is replaced by the same cipher substitute (Burton, 2007). In the linear cipher, all letters of an alphabet system of size n are first mapped to the integers in the set $\{0, 1, 2, \ldots, n-1\}$. Modular arithmetic is then used to transform the integer associated to each letter in the plaintext into another integer, which in turn yields a letter in the ciphertext.

Recall the encryption function (1). Suppose that a single letter P is encrypted as a letter C, that is, $C = E(P)$. Then the decryption function of the letter C is given by

$$D(C) = a^{-1}(C - b) \mod n, \tag{2}$$

where a^{-1} is the *multiplicative inverse* of a modulo n, that is, an integer a^{-1} satisfying $1 = aa^{-1} \bmod n$. Note that the multiplicative inverse of a modulo n exists if and only if $\gcd(a, n) = 1$ (Stinson, 2006). Finally, one can see that

$$\begin{aligned} D(E(P)) &= a^{-1}(E(P) - b) \bmod n \\ &= a^{-1}(((aP + b) \bmod n) - b) \bmod n \\ &= a^{-1}(aP + b - b) \bmod n \\ &= a^{-1}aP \bmod n \\ &= P \bmod n. \end{aligned} \tag{3}$$

Thus, the decryption function (2) is indeed the inverse of the encryption function (1).

Consider an example of encrypting English messages (that is, $n = 26$). Let $\phi : \mathbb{N} \to \mathbb{N}$ be the Euler's phi-function, that is, $\phi(n)$ is the number of positive integers $x \leq n$ such that $\gcd(x, n) = 1$ (Burton, 2007). Then there are $\phi(26) = 12$ possible values of the private key a in the set $\{0, 1, 2, \ldots, 25\}$, each of which can be paired up with 26 different values of the private key b. Therefore, there are $12 \cdot 26 = 312$ possible pairs of the private keys (a, b), including 26 pairs of the form $(1, b)$ which yield trivial shift ciphers.

Despite a high number of possibilities, one may recover the pair (a, b) of private keys easily if two distinct pairs of correspondence between a plaintext letter and a ciphertext letter are known (Stinson, 2006). Let (P_1, C_1) and (P_2, C_2) be two pairs of such correspondence. From (1), we obtain the system of linear congruences

$$\begin{aligned} C_1 &\equiv aP_1 + b \pmod n, \\ C_2 &\equiv aP_2 + b \pmod n. \end{aligned} \tag{4}$$

This yields $C_1 - C_2 \equiv a(P_1 - P_2) \pmod n$. It then follows that $a \equiv (C_1 - C_2)(P_1 - P_2)^{-1} \pmod n$, and thus $b = (C_1 - aP_1) \bmod n$.

Finally, one can prove easily that the encryption function (1) is bijective on the set $\{0, 1, 2, \ldots, n-1\}$ (Stinson, 2006). This means that a plaintext letter is always encrypted as the same ciphertext letter regardless of its location in the plaintext, and thus their frequencies are preserved. Then one can use frequency analysis to determine the pairs (P_1, C_1) and (P_2, C_2).

2. Modifying the linear cipher

The development of our modified linear cipher consists of the following three main steps:

1. Create a public table which can be used for decryption only by the recipient.
2. Modify the encryption algorithm of the classical linear cipher.
3. Derive the decryption algorithm associated to our modified encryption.

2.1. Creating a public table

In the linear cipher, both sender and recipient use the same conversion table for converting letters into integers, and vice versa. The conversion table is normally made available publicly, for it does not contain any information on the private keys. Having another public conversion table, which differs from the one that was used by both sender and recipient, can therefore provide some hindrance to an opponent attempting decryption.

Rather than using a common conversion table as in the linear cipher, we introduce the concept of using two different conversion tables: while the sender uses a *private table* for encryption, he also creates a *public table*, which will be the only information made available publicly. Using the private keys, the recipient can easily retrieve the private table from the public one (and thus can decrypt the ciphertext), whereas an opponent will encounter considerable difficulty in order to do the same. Our process for creating both conversion tables consists of the following steps:

1. A sender and a recipient choose the following integers as their private keys:

   (a) a positive integer l;

   (b) integers $a, b \in \{0, 1, \ldots, n^l - 1\}$ (where n is the number of letters in the alphabet system) such that a^{-1} modulo n^l exists. Here, we require that n has a primitive root. It is well known that a primitive root modulo n exists if and only if $n = 2, 4, p^k$, or $2p^k$ for some odd prime p and $k \in \mathbb{N}$ (Burton, 2007).

2. The sender calculates $A = a^b \bmod n$.
3. The sender chooses a primitive root modulo n, say, r.
4. Create the private table by assigning the numerical value $r^{i-1}A$ to the i^{th} letter in the alphabet system (for $i = 1, 2, \ldots, n$) and exchanging the numerical value of the n^{th} letter with the A^{th} letter.

5. Create the public table by letting the numerical value of its i^{th} letter (for $i = 1, 2, \ldots, n$) be that of the j^{th} letter of the private table, where

$$j = \begin{cases} (a + bi) \bmod n & \text{if } a + bi \not\equiv 0 \pmod{n}, \\ n & \text{if } a + bi \equiv 0 \pmod{n}. \end{cases} \tag{5}$$

For an illustrative example of how to create a private table and a public table for our modified linear cipher, see Example 1.

2.2. The encryption algorithm

Recall the encryption function (1) of the linear cipher. Unlike the linear cipher which is monoalphabetic, our modified linear cipher allows encrypting a block of at least two letters at a time. On encrypting each block of plaintext, we also use a periodic key and perform modular arithmetic with different modulus in order to disguise the monoalphabetic property originally existing in the linear cipher. To be precise, our encryption algorithm consists of the following steps:

1. The sender divides the plaintext into blocks of l letters. For simplicity, here we shall assume that the length of plaintext is divisible by l.

2. In each block, the sender converts every letter into its corresponding numerical value using the private table.

3. Let N be the number of blocks of plaintext. For $j = 1, 2, \ldots, N$, the sender encrypts the j^{th} block of plaintext using the following steps:

(a) Let P_j be the numerical value obtained by viewing the number associated to each letter as a digit in base n and then converting the entire block to base 10.

(b) Calculate

$$C_j = (aP_j + b_j) \bmod n^l, \tag{6}$$

where $b_j = b + j$.

(c) Convert C_j to base n and pad it with leading zeros if necessary so that it contains l integers. Then convert the result into letters.

4. Combine all blocks of letters to form the ciphertext.

For an illustrative example of how encryption is done using our modified linear cipher, see Example 2.

2.3. The decryption algorithm

Our decryption algorithm, which is a slight modification of the one of the classical linear cipher, consists of the following steps:

1. The recipient recalls the private keys a, b, and l.
2. The recipient derives the private table from the public one using the private keys.
3. The recipient converts each letter in the ciphertext into its numerical value using the private table.
4. The recipient divides the ciphertext into N blocks of l letters.
5. For $j = 1, 2, \ldots, N$, the recipient decrypts the j^{th} block of ciphertext using the following steps:

(a) Let C_j be the numerical value obtained by viewing the number associated to each letter as a digit in base n and then converting the entire block to base 10.

(b) Calculate

$$P_j = a^{-1}(C_j - b_j) \bmod n^l, \tag{7}$$

where a^{-1} is the multiplicative inverse of a modulo n^l and $b_j = b + j$.

(c) Convert P_j to base n and pad it with leading zeros if necessary so that it contains l integers. Then convert the result into letters.

6. Combine all blocks of letters to obtain the plaintext.

For an illustrative example of how decryption is done using our modified linear cipher, see Example 3.

Results and Discussion

In this section, first we will illustrate the use of our modified linear cipher via some examples. Then we will discuss some cryptanalytic aspects of our modified cipher compared with those of the classical linear cipher.

1. Examples

Example 1. For purpose of illustration, we shall use an alphabet system of 53 letters, consisting of all uppercase and lowercase English letters, and the underscore. Hence $n = 53$, which has a primitive root.

Suppose that a sender and a recipient choose the integers $l = 2$, $a = 253$, and $b = 131$ as their private keys. The sender calculates $A = a^b \bmod n = 12$ and chooses a primitive root r modulo 53; here we choose $r = 2$.

To create the private table, we assign the numerical value $2^{i-1} \cdot 12$ to the i^{th} letter in the alphabet system (for $i = 1, 2, \ldots, 53$) and then exchange the numerical value of the 53^{th} letter with the 12^{th} letter. The result is shown in Table 1.

Table 1 A private table of 53 letters.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
12	24	48	43	33	13	26	52	51	49	45	0	21	42	31	9	18	36	19	38
U	V	W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
23	46	39	25	50	47	41	29	5	10	20	40	27	1	2	4	8	16	32	11
o	p	q	r	s	t	u	v	w	x	y	z	_							
22	44	35	17	34	15	30	7	14	28	3	6	37							

Next, we obtain the public table by letting the numerical value of its i^{th} letter (for $i = 1, 2, \ldots, 53$) be that of the j^{th} letter of the private table, where

$$j = \begin{cases} (253 + 131i) \bmod 53 & \text{if } 253 + 131i \not\equiv 0 \pmod{53}, \\ 53 & \text{if } 253 + 131i \equiv 0 \pmod{53}. \end{cases} \tag{8}$$

The result is shown in Table 2.

Table 2 The corresponding public table of 53 letters.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	16	49	2	26	40	43	5	12	47	3	39	7	38	34	18	44	42	32	45
U	V	W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
4	52	27	33	10	24	41	6	25	14	23	15	36	35	31	11	0	8	51	1
o	p	q	r	s	t	u	v	w	x	y	z	_							
13	20	48	29	37	50	28	46	30	19	17	9	22							

Example 2. Suppose that the sender and the recipient use the alphabet system of 53 letters and the private keys $l = 2$, $a = 253$, and $b = 131$ as in Example 1. To encrypt the plaintext “Linear”, the sender divides the plaintext into blocks of two letters, that is, “Li”, “ne”, and “ar”. For each block, after converting each letter into its numerical value using the private table (Table 1), the sender obtains $(00, 02)_{53}$, $(11, 20)_{53}$, and $(41, 17)_{53}$. It follows that

$$\begin{aligned} P_1 &= 0(53) + 2 = 2, \\ P_2 &= 11(53) + 20 = 603, \\ P_3 &= 41(53) + 17 = 2190. \end{aligned} \tag{9}$$

Using our encryption function (6), the sender encrypts P_1, P_2, P_3 by calculating

$$\begin{aligned} C_1 &= (aP_1 + b_1) \bmod n^l = \big(253(2) + (131 + 1)\big) \bmod 53^2 = 638, \\ C_2 &= (aP_2 + b_2) \bmod n^l = \big(253(603) + (131 + 2)\big) \bmod 53^2 = 1006, \\ C_3 &= (aP_3 + b_3) \bmod n^l = \big(253(2190) + (131 + 3)\big) \bmod 53^2 = 831. \end{aligned} \tag{10}$$

Converting C_1, C_2, C_3 to base 53, the sender finally obtains

$$C_1 = (12, 02)_{53}, \ C_2 = (18, 52)_{53}, \ C_3 = (15, 36)_{53}, \tag{11}$$

each of which, after being converted using the private table (Table 1), yields “Ai”, “QH”, and “tR”, respectively. Therefore, the ciphertext is “AiQHtR”.

Example 3. To decrypt the ciphertext “AiQHtR” obtained in Example 2, the recipient must first derive the private table (Table 1) from the public one (Table 2) using the private keys $l = 2$, $a = 253$, and $b = 131$ as in Example 1. Then the recipient divides the ciphertext into blocks of two letters, that is, “Ai”, “QH”, and “tR”. For each block, after converting each letter into its numerical value using the private table (Table 1), the recipient obtains $(12, 02)_{53}$, $(18, 52)_{53}$, and $(15, 36)_{53}$. It follows that

$$\begin{aligned} C_1 &= 12(53) + 2 = 638, \\ C_2 &= 18(53) + 52 = 1006, \\ C_3 &= 15(53) + 36 = 831. \end{aligned} \tag{12}$$

Here, one can verify that the multiplicative inverse of 253 modulo 53^2 is 1188. Using our decryption function (7), the recipient decrypts C_1, C_2, C_3 by calculating

$$\begin{aligned} P_1 &= a^{-1}(C_1 - b_1) \bmod n^l = 253^{-1}\big(638 - (131 + 1)\big) \bmod 53^2 = 2, \\ P_2 &= a^{-1}(C_2 - b_2) \bmod n^l = 253^{-1}\big(1006 - (131 + 2)\big) \bmod 53^2 = 603, \\ P_3 &= a^{-1}(C_3 - b_3) \bmod n^l = 253^{-1}\big(831 - (131 + 3)\big) \bmod 53^2 = 2190. \end{aligned} \tag{13}$$

Converting P_1, P_2, P_3 to base 53, the recipient finally obtains

$$P_1 = (00, 02)_{53}, \ P_2 = (11, 20)_{53}, \ P_3 = (41, 17)_{53}, \tag{14}$$

each of which, after being converted using the private table (Table 1), yields “Li”, “ne”, and “ar”, respectively. Therefore, the plaintext “Linear” is finally recovered.

2. Frequency analysis

The main weakness of the linear cipher is that the frequency of a letter in the plaintext and the one of its corresponding letter in the ciphertext are identical (Stallings, 2011). This therefore allows the opponent to determine the private keys a, b using frequency analysis of a particular language.

In this paper, to make the linear cipher more secure against frequency analysis, we encrypt blocks of plaintext instead of single letters, and use a periodic key when encrypting each block of plaintext and decrypting each block of ciphertext. For example, consider the plaintext

> “Moderncryptographyisheavilybasedonmathematicaltheoryandcomputersciencepracticecryptog raphicalgorithm”.

Encrypting using our modified linear cipher with private keys $a = 253$, $b = 131$, and $l = 2$, we obtain the ciphertext

> “wguHdiULrmEmBfTqjIsIEkMzicHPpyogylGxWmMmzXifntWLGIXtfGAVYaNFBxwecsgETmElAip WTRBeQtstXUWQ_VEyVFmxI_TP”.

The frequencies of each letter, sorted in decreasing order, in the plaintext and in the ciphertext are illustrated in Figure 1.

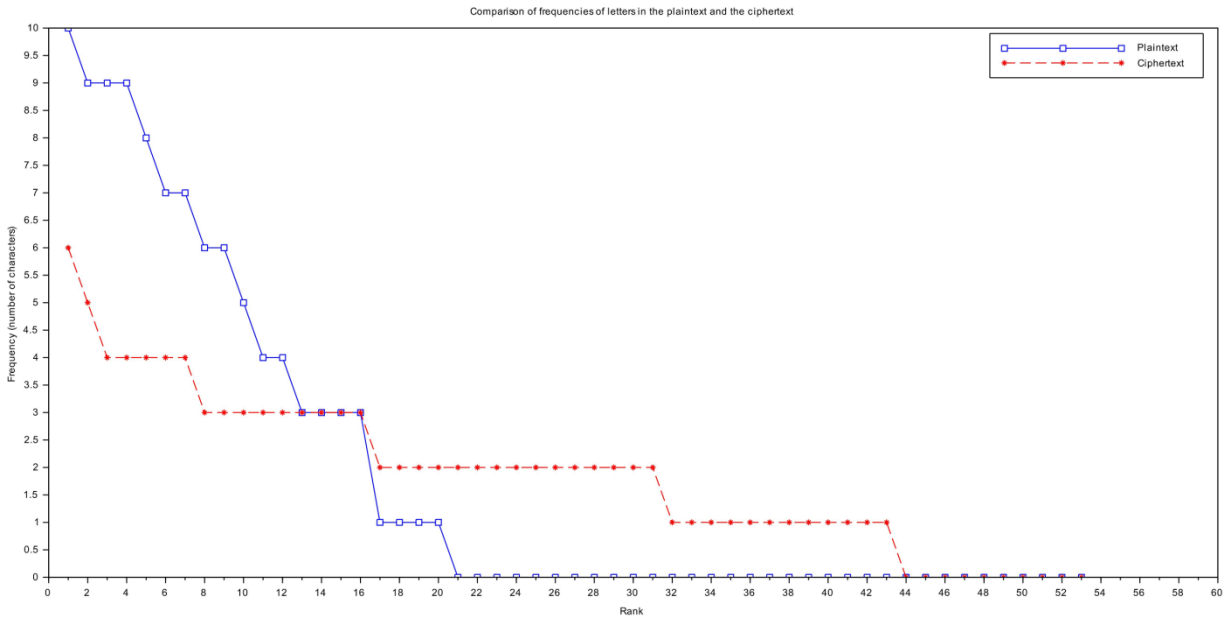

Figure 1 Frequencies of letters in the plaintext and the ciphertext.

From Figure 1, it is clear that our modified linear cipher can provide security against frequency analysis, which has never existed in the classical linear cipher, to the above ciphertext. Moreover, one can verify that every pair of two letters (digrams) occurring in the plaintext appears at most twice, whereas every digram occurring in the ciphertext appears only once.

Finally, we will show that our modified linear cipher can prevent an opponent from determining the length of the plaintext (that is, $l = 2$) from the index of coincidence. Suppose that $\mathbf{x} = x_1 x_2 \ldots x_L$ is a string of L letters. The *index of coincidence*, denoted by $I_c(\mathbf{x})$, is the probability that two random letters of $\mathbf{x}$ are identical, that is,

$$I_c(\mathbf{x}) = \frac{\sum_{i=1}^{n} \binom{f_i}{2}}{\binom{L}{2}} = \frac{\sum_{i=1}^{n} f_i(f_i-1)}{L(L-1)}, \tag{15}$$

where f_i denotes the frequency of the i^{th} letter in the alphabet system of size n, for $i = 1, 2, \ldots, n$ (Stinson, 2006). Let C_o and C_e be the strings formed by all the letters of the ciphertext at odd indices and at even indices, respectively. Then one can verified easily that $I_c(C_o) = 0.021$ and $I_c(C_e) = 0.026$, both of which are far less than 0.065, the index of coincidence of a string of English language text (Stinson, 2006). Therefore, the opponent cannot deduce that $l = 2$ by considering both $I_c(C_o)$ and $I_c(C_e)$.

3. Attacking via the public table

Let n be a prime representing the number of letters in the alphabet system and l be the number of letters in each block. Let $a, b \in \{0, 1, 2, \ldots, n^l - 1\}$ be such that a^{-1} modulo n^l exists. In this case, it is assumed that the length of the plaintext is divisible by l.

In our method, the numerical value of the i^{th} letter in the public table is identical to that of the $(a + bi)^{\text{th}}$ letter in the private table. If both positions coincide, then $a + bi \equiv i \pmod{n}$ and so $a \equiv i(1 - b) \pmod{n}$. If $b \equiv 1 \pmod{n}$, then we have $a \equiv 0 \pmod{n}$. This is clearly impossible since 0 is not invertible modulo n^l. In other words, every position in the public table changes from the private table.

On the other hand, if $b \not\equiv 1 \pmod{n}$, then it follows that $i \equiv a(1 - b)^{-1} \pmod{n}$. Hence, there is only one position in the public table that does not change from the private table. In this case, the number of a in modulo n^l that can be used as a key is $\phi(n^l)$. Each value of a can have n^l different addition shifts b in modulo n^l. Hence, the number of keys (a, b) that can be used as a key in modulo n^l is

$$\phi(n^l)n^l = (n^l - n^{l-1})n^l = n^{l-1}(n-1)n^l = n^{2l-1}(n-1). \tag{16}$$

From the public table, the opponent knows the position of 0 in that table (say, the i^{th} position), which in turn comes from the A^{th} letter in the private table. Thus, we have $A = (a + bi) \bmod n$. This leads to

$$\begin{aligned} A &\equiv a + bi \pmod{n} \\ a^b &\equiv a + bi \pmod{n} \\ a(a^{b-1} - 1) &\equiv bi \pmod{n}. \end{aligned} \tag{17}$$

Let g be a primitive root modulo n. For all integers x with $\gcd(x, n) = 1$, we define $\text{ind}_g x$ to be the smallest positive integer k such that $g^k \equiv x \pmod{n}$ (Burton, 2007). Provided that $\text{ind}_g a$, $\text{ind}_g(a^{b-1} - 1)$, $\text{ind}_g b$, and $\text{ind}_g i$ exist, the congruence (4) becomes

$$\begin{aligned} \text{ind}_g a + \text{ind}_g(a^{b-1} - 1) &\equiv \text{ind}_g b + \text{ind}_g i \pmod{\phi(n)} \\ \text{ind}_g a + \text{ind}_g(a^{b-1} - 1) - \text{ind}_g b &\equiv \text{ind}_g i \pmod{\phi(n)}. \end{aligned} \tag{18}$$

Let

$$X = \text{ind}_g a, \qquad Y = \text{ind}_g(a^{b-1} - 1), \qquad Z = \text{ind}_g b, \qquad C = \text{ind}_g i. \tag{19}$$

Note that i is known, and so is C. Then (18) becomes $X + Y - Z \equiv C \pmod{\phi(n)}$. One can see easily that there are $(\phi(n))^2$ distinct ordered triples (X, Y, Z) which satisfy this congruence in modulo $\phi(n)$.

Suppose that the opponent knows the values of X and Z modulo $\phi(n)$. Since $X = \text{ind}_g a$ is known, that is, $a \equiv g^X \pmod{n}$, we have $a \bmod n^l = (g^X \bmod n) + ni$ for some non-negative integer i such that $(g^X \bmod n) + ni < n^l$. Then $i \in \left\{0, 1, 2, \ldots, \left\lfloor \frac{n^l - g^X \bmod n}{n} \right\rfloor\right\}$. Since $0 \le g^X \bmod n < n$, we have $0 \le \frac{g^X \bmod n}{n} < 1$. Therefore,

$$\left\lfloor \frac{n^l - g^X \bmod n}{n} \right\rfloor = \begin{cases} n^{l-1} - 1 & \text{if } g^X \bmod n \neq 0, \\ n^{l-1} & \text{if } g^X \bmod n = 0. \end{cases} \tag{20}$$

Similarly, we have $b \bmod n^l = (g^Z \bmod n) + ni$ for some $i \in \left\{0, 1, 2, \ldots, \left\lfloor \frac{n^l - g^Z \bmod n}{n} \right\rfloor\right\}$. Since $0 \le g^Z \bmod n < n$, we have $0 \le \frac{g^Z \bmod n}{n} < 1$. Therefore,

$$\left\lfloor \frac{n^l - g^Z \bmod n}{n} \right\rfloor = \begin{cases} n^{l-1} - 1 & \text{if } g^Z \bmod n \neq 0, \\ n^{l-1} & \text{if } g^Z \bmod n = 0. \end{cases} \tag{21}$$

Hence, the number of keys (a, b) that can be used as a key in modulo n^l is between $\big(\phi(n)\big)^2 (n^{l-1})^2$ and $\big(\phi(n)\big)^2 (n^{l-1} + 1)^2$.

In the next sections, we shall assume that the opponent knows the private table, which is used for encryption and decryption.

4. A ciphertext-only attack

A *ciphertext-only attack* is an attack where an opponent possesses only the encryption algorithm and a ciphertext (Stallings, 2011). Suppose that the entire ciphertext is known to the opponent. Since the length of the ciphertext is divisible by l, the opponent may have some knowledge on the exact value of l. If the exact value of l is unknown, then a ciphertext-only attack is clearly impossible.

Now assume that the exact value of l is known to the opponent, and so the ciphertext can be split into blocks of length l, say, $C_1, C_2, \ldots, C_N$. From our encryption function (6), we have

$$\begin{aligned} C_1 &\equiv aP_1 + b_1 \pmod{n^l}, \\ C_2 &\equiv aP_2 + b_2 \pmod{n^l}, \\ &\vdots \\ C_N &\equiv aP_N + b_N \pmod{n^l}. \end{aligned} \tag{22}$$

Suppose that the opponent knows two blocks of ciphertext, say C_i and C_j with $i, j \in \{1, 2, \ldots, N\}$ and $i \neq j$. This leads to the system of congruences

$$\begin{aligned} C_i &\equiv aP_i + b_i \pmod{n^l}, \\ C_j &\equiv aP_j + b_j \pmod{n^l}. \end{aligned} \tag{23}$$

Solving the system (23), we have

$$\begin{aligned} C_i - C_j &\equiv a(P_i - P_j) + (i - j) \pmod{n^l} \\ (C_i - C_j) - (i - j) &\equiv a(P_i - P_j) \pmod{n^l}. \end{aligned} \tag{24}$$

Provided that i and j are known, the number of ordered triples (a, P_i, P_j) satisfying (24) is

$$\phi(n^l)n^l = (n^l - n^{l-1})n^l = n^{l-1}(n-1)n^l = n^{2l-1}(n-1). \tag{25}$$

From this, one can see that, even if the entire ciphertext is known to the opponent, the plaintext and the private key a cannot be determined exactly due to the high number of possibilities for the ordered triples (a, P_i, P_j).

5. A known-plaintext attack

A *known-plaintext attack* is an attack where an opponent possesses one or more plaintext-ciphertext pairs in addition to the encryption algorithm and the ciphertext (Stallings, 2011). Recall from (6) that our encryption function is defined by

$$C_k = (aP_k + b_k) \bmod n^l, \tag{26}$$

where P_k is the k^{th} block of plaintext, C_k is the k^{th} block of ciphertext, and $b_k = b + k$. Suppose that the opponent can discover two distinct ciphertext-plaintext pairs, say, (C_i, P_i) and (C_j, P_j). Then the value of l, the number of letters in each block, is known. This leads to the system of congruences

$$\begin{aligned} C_i &\equiv aP_i + b_i \pmod{n^l}, \\ C_j &\equiv aP_j + b_j \pmod{n^l}. \end{aligned} \tag{27}$$

Solving the system (27), we obtain

$$\begin{aligned} C_i - C_j &\equiv a(P_i - P_j) + (i - j) \pmod{n^l} \\ a &\equiv \left[(C_i - C_j) - (i - j)\right](P_i - P_j)^{-1} \pmod{n^l}. \end{aligned} \tag{28}$$

Although the opponent can discover P_i and P_j, calculating the value of the keys (a, b) is still impossible unless the positions i and j are known. This provides an additional security compared with the classical linear cipher.

Conclusions

In this paper, we propose a modification of the linear cipher using public tables, pairs of moduli, and periodic keys. In our modified linear cipher, the sender first creates the private table using the private keys a, b and a primitive root modulo n. Using the private keys a, b, the sender can also create the public table, which can be converted later into the private table and used for decryption only by the recipient.

For encryption and decryption, we introduce the use of different moduli, that is, n and n^l, as well as a periodic key derived from the private key b. Unlike the classical linear cipher, our method allows block encryption, while the true length of each block remains unknown to the opponent. Using different moduli also causes a great deal of difficulty to the opponent in determining the correct private keys a, b.

Finally, we analyze our modified linear cipher in three categories, namely, frequency analysis, a ciphertext-only attack, and a known-plaintext attack. In our analysis, we find the following:

1. Our modified linear cipher is secure against frequency analysis, which has never existed in the classical linear cipher.

2. For a ciphertext-only attack, our modified linear cipher yields more possibilities of the correct ordered triple (a, P_i, P_j), where a is a private key and P_i, P_j are the plaintext blocks which correspond to the known ciphertext blocks C_i, C_j, respectively. This provides more security against a ciphertext-only attack than the classical linear cipher.

3. For a known-plaintext attack, our modified linear cipher can prevent the opponent from deducing the private keys a, b when two distinct ciphertext-plaintext pairs are known, which is the main drawback of the classical linear cipher.

Therefore, our modified linear cipher can provide more security in the above categories than the classical linear cipher. Finally, we remark that cryptography is one of many fields that are growing rapidly nowadays. Although our modified linear cipher is secure against certain classical attacks, the question whether it remains secure against some attacks developed in modern time is worth further investigation.

Acknowledgements

The authors would like to thank the Department of Mathematics, Faculty of Science, Khon Kaen University for its support towards this research.

References

Burton, D.M. (2007). *Elementary Number Theory*. (6th ed.). New York: McGraw-Hill.

Rajan, A., & Balakumaran, D. (2014). Advancement in Caesar cipher by randomization and delta formation. In *Proceedings of the 2014 IEEE International Conference on Information Communication and Embedded Systems*. (pp. 1-4). Piscataway: Institute of Electrical and Electronics Engineers.

Senthil, K., Prasanthi, K., & Rajaram, R. (2013). A modern avatar of Julius Caesar and Vigenère cipher. In *Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research*. (pp. 1-3). Piscataway: Institute of Electrical and Electronics Engineers.

Singh, A., Nandal, A., & Malik, S. (2012). Implementation of Caesar cipher with rail fence for enhancing data security. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(12), 78-82.

Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice*. (5th ed.). Upper Saddle River: Pearson Education.

Stinson, D.R. (2006). *Cryptography: Theory and Practice*. (3rd ed.). Boca Raton: Chapman & Hall/CRC.