

Analysis and Design of Affine and Hill Cipher

Mozhgan Mokhtari (Corresponding author)

Department of Mathematics, Islamic Azad University, Ashtian Branch, Iran

PO box 39618-13347, Ashtian, Iran

Tel: 98-862-722-2500 E-mail: mozhganmokhtari@yahoo.com

Hassan Naraghi

Department of Mathematics, Islamic Azad University, Ashtian Branch, Iran

PO box 39618-13347, Ashtian, Iran

Tel: 98-862-722-2500 E-mail: naraghi@mail.aiu.ac.ir

Received: August 9, 2011 Accepted: September 6, 2011 Published: February 1, 2012

doi:10.5539/jmr.v4n1p67 URL: <http://dx.doi.org/10.5539/jmr.v4n1p67>

Abstract

Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques. Cryptology is the study of cryptography and cryptanalysis. The security of information encompasses the following aspects:

- confidentiality or privacy,
- data integrity,
- authentication,
- nonrepudiation.

Each of these aspects of message security can be addressed by standard methods in cryptography. Besides exchange of messages, tools from cryptography can be applied to sharing an access key between multiple parties so that no one person can gain access to a vault by any two of them. Another role is in the design of electronic forms of cash. In this paper, we study affine and Hill cipher in cryptography.

Keywords: Affine cipher, Encryption, Cryptography, Decryption, Monoalphabetic

1. Introduction

Cryptography is the study of mathematical techniques for all aspects of information security. Cryptanalysis is the complementary science concerned with the methods to defeat these techniques. Cryptology is the study of cryptography and cryptanalysis. The security of information encompasses the following aspects:

- confidentiality or privacy,
- data integrity,
- authentication,
- nonrepudiation.

Each of these aspects of message security can be addressed by standard methods in cryptography. Besides exchange of messages, tools from cryptography can be applied to sharing an access key between multiple parties so that no one person can gain access to a vault by any two of them. Another role is in the design of electronic forms of cash.

As we have seen, shift ciphers offer very little security. The problem is that the letter substitutions, or shifts, are not mixed up enough. The idea of an affine cipher is to use multiplication combined with addition, modulo m , where m is an integer, to create a more mixed-up substitution (Barr, 2002). The affine cipher is simply a special case of the more general monoalphabetic substitution cipher. The key for the affine cipher consists of an ordered pair, say (a, b) . In selecting the key, it is important to note the following restrictions; $a \neq 0$ and b must be chosen from among the integers $0, 1, 2, 3, \dots, m-1$ and $a \neq 0$ must be relatively prime to m (i.e. a should have no factors in common with m). For example, assuming we use a 26 character alphabet (i.e. $m = 26$), 15 and 26 have no factors in common and therefore 15 is an acceptable value for a .

On the other hand, if we chose 12 for the value of a , it is obvious that 12 would be an unacceptable value since 12 and 26 have common factors, specifically 2.

In General, an affine cipher is a cipher system in which plaintext letters are enciphered mathematically by the function,

$$y = ax + b \pmod{m}$$

and using function notation, we have,

$$\epsilon(x) = ax + b \pmod{m}$$

where x is the numerical equivalent of the plaintext letter and m is the number of letters in the alphabet.

2. Preliminaries

Whenever possible we follow the notation, terminology and examples of (Barr, 2002; Castaneda, 2009; Shannon, 1949) and subjects of history of cryptology selected of (Flannery & Flannery, 2001; Singh, 1999; Wrixon, 1998).

Encryption = the process of disguising a message so as to hide the information it contains; this process can include both encoding and enciphering (see definitions below).

Protocol = an algorithm, defined by a sequence of steps, precisely specifying the actions of multiple parties in order to achieve an objective.

Plaintext = the message to be transmitted or stored.

Ciphertext = the disguised message.

Alphabet = a collection of symbols, also referred to as characters.

Character = an element of an alphabet.

Bit = a character 0 or 1 of the binary alphabet.

String = a finite sequence of characters in some alphabet.

Example 1 The following are some standard alphabets.

A, \dots, Z	26 symbols	MSDOS(less punctuation)
<i>ASCII</i>	7-bit words(128 symbols)	American standard
<i>extended</i>	8-bit words(256 symbols)	
<i>ISO – 8859 – 1</i>	8-bit words(256 symbols)	European standard
<i>Binary</i>	{0, 1}	Numerical alphabet base 2
<i>Octal</i>	{0, ..., 7}	Numerical alphabet base 8
<i>Decimal</i>	{0, ..., 9}	Numerical alphabet base 10
<i>Hexadecimal</i>	{0, ..., 9, a, b, c, d, e, f}	Numerical alphabet base 16

Encode = to convert a message into a representation in a standard alphabet, such as to the alphabet $\{A, \dots, Z\}$ or to numerical alphabet.

Decode = to convert the encoded message back to its original alphabet and original form the term plaintext will apply to either the original or the encoded form. The process of encoding a message is not an obscure process, and the result that we get can be considered equivalent to the plaintext message.

Cipher = a map from a space of plaintext to a space of ciphertext.

Encipher = to convert plaintext into ciphertext.

Decipher = to convert ciphertext back to plaintext.

Stream cipher = a cipher which acts on the plaintext one symbol at a time.

Block cipher = a cipher which acts on the plaintext in blocks of symbols.

Substitution cipher = a stream cipher which acts on the plaintext by making a substitution of the characters with elements of a new alphabet or by a permutation of the characters in the plaintext alphabet.

Transposition cipher = a block cipher which acts on the plaintext by permuting the positions of the characters in the plaintext.

Example 2 The following is an example of a substitution cipher:

A	B	C	D	E	F	G	H	\dots	Z	$-$
\downarrow	\dots	\downarrow	\downarrow							
P	C	$-$	O	N	A	W	Y	\dots	L	S

which takes the plaintext BAD CAFE BED to the ciphertext CPOS ANSNO.

2.1 Cryptosystems

Given an alphabet \mathcal{A} we define \mathcal{A}^* to be the set of all strings over \mathcal{A} . In order to define a cryptosystem, we require a collection of sets:

$$\begin{array}{ll} \mathcal{A} = \text{plaintext alphabet} & \mathcal{A}' = \text{ciphertext alphabet} \\ \mathcal{M} = \text{plaintext space} & \mathcal{C} = \text{ciphertext space} \\ \mathcal{K} = (\text{plaintext}) \text{ keyspace} & \mathcal{K}' = (\text{ciphertext}) \text{ keyspace} \end{array}$$

where \mathcal{M} is a subset of \mathcal{A}^* , \mathcal{C} is a subset of \mathcal{A}'^* , and \mathcal{K} and \mathcal{K}' are sets which are generally strings of fixed finite length over some alphabets (e.g. \mathcal{A}^n or \mathcal{A}'^m). A cryptosystem or encryption scheme is a pair (E, D) of maps

$$E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}, \quad D : \mathcal{K}' \times \mathcal{C} \rightarrow \mathcal{M}$$

such that for each K in \mathcal{K} there exists a K' in \mathcal{K}' such that

$$D(K', E(K, M)) = M$$

for all M in \mathcal{M} . We write E_K for the map $E(K, \cdot) : \mathcal{M} \rightarrow \mathcal{C}$ and similarly write $D_{K'}$ for $D(K', \cdot) : \mathcal{C} \rightarrow \mathcal{M}$. With this notation the condition on E, D, K and K' is that $D_{K'} \circ E_K$ is the identity map on \mathcal{M} .

We will refer to E_K as a cipher, and note that a cipher is necessarily injective. For many cryptosystems, there will exist a unique inverse ciphertext key K' associated to each plaintext key K . A cryptosystem for which the inverse key K' is K itself (hence $K = K'$) is said to be symmetric. If the inverse key K' associated to K is neither K itself nor easily computable function of K , then we say that the cryptosystem is asymmetric or a public key cryptosystem.

A fundamental principle of cryptography is that the security of a cipher E_K (i.e. the difficulty in finding $D_{K'}$) does not rest on the lack of knowledge of the cryptosystem (E, D) . Instead, security should be based on the secrecy of K' . Recall that a (cryptographic) protocol is an algorithm, defined by a sequence of steps, precisely specifying the actions of multiple parties in order to achieve a (security) objective. An example of a cryptographic protocol, we describe the steps for message exchange using a symmetric key cryptosystem.

- Alice and Bob publicly agree on a cryptosystem (E, D) .
- For each message M Alice \rightarrow Bob:
 - a) Alice and Bob agree on a secret key K .
 - b) Alice computes $C = E_K(M)$ and sends it to Bob.
 - c) Bob computes $M = D_K(C)$ to obtain the plaintext.

The difficulty of step 2.a was one of the fundamental obstructions to cryptography before the advent of public key cryptography. Asymmetric cryptography provides an elegant solution to the problem of distribution of private keys.

3. Affine Cipher

Another type of substitution cipher is the affine cipher (or linear cipher). Even though affine ciphers are examples of substitution ciphers, and are thus far from secure, they can be easily altered to make a system which is, in fact, secure. To set up an affine cipher, you pick two values a and b , and then set $\epsilon(m) = am + b \pmod{26}$. For example, if we take $a = 3$ and $b = 8$, then the encryption function is

$$\epsilon(m) = 3m + 8 \pmod{26}.$$

To encrypt the letter C , we first note that C corresponds to the number 02. Plugging this in for m , we get $\epsilon(02) = 3(02) + 8 = 14$, and so C is encrypted as O . To find our decryption function, we set $s = \epsilon(m)$ and solve for m in terms of s . We have:

$$\begin{aligned} s &\equiv 3m + 8 \pmod{26} \\ s - 8 &\equiv 3m \pmod{26}, \end{aligned}$$

so

$$3m \equiv s - 8 \pmod{26}$$

Definition 3.1 (Barr, 2002) A multiplicative inverse of an integer a modulo m is an integer b , in the range 1 to $m - 1$, such that $ab \equiv 1 \pmod{m}$. When a and m are relatively prime, such ab will exist and we call b the multiplicative inverse of a and label it a^{-1} .

Since $\gcd(3, 26) = 1$, we know that there will be an x with $3x \equiv 1 \pmod{26}$. We could use the Extended Euclidean Algorithm to find x , or we can simply notice that $(3)(9) = 27 \equiv 1 \pmod{26}$ and so $x = 9$ works. Now we multiply both sides by 9:

$$\begin{aligned} 27m &\equiv 9(s - 8) \pmod{26} \\ &\equiv 9s - 72 \pmod{26} \\ &\equiv 9s + 6 \pmod{26}, \end{aligned}$$

which tells us that $m = \delta(s) = 9s + 6 \pmod{26}$. In general, to construct an affine cipher, we begin by choosing a and b with $\gcd(a, 26) = 1$. Then $\epsilon(m) = am + b \pmod{26}$ and $\delta(s) = x(s - b) \pmod{26}$, where x satisfies $ax \equiv 1 \pmod{26}$.

Exercise 3.2 This exercise has two parts. Working in teams of 2,

(1) you and your partner will create an affine cipher by choosing a and b with $\gcd(a, 26) = 1$. Using your cipher, $\epsilon(m) = am + b \pmod{26}$, encode a message that is between 8 and 12 letters long. Give this encoded message, along with your values of a and b , to another team to decipher.

(2) you and your partner will decipher the message that the other team gave you. Using their values of a and b , decode their message using $\delta(s) = x(s - b) \pmod{26}$, where x satisfies $ax \equiv 1 \pmod{26}$.

As we mentioned earlier, affine ciphers are not secure because they're really just special examples of substitution ciphers and so one may use "frequency analysis" to crack them. However, we can tweak the idea a bit and consider affine block ciphers instead. The mathematics is the same, only now instead of encrypting one letter at a time, we encrypt a block of letters together. As an example, suppose we want to take our block-length to be 4. This means that we divide our message into blocks of 4 letters and encrypt each block separately. The largest number we could end up with is 456,975 (corresponding to the highly unlikely 4-letter block "ZZZZ"), and so we need to be sure that our modulus is greater than 456,975. We could use 456,976 but it's just as easy (if not easier) to use 1,000,000. Now we proceed just as before. We choose a and b and set $\epsilon(m) = am + b \pmod{1,000,000}$. As long as we've chosen a so that $\gcd(a, 1,000,000) = 1$, we can find an integer x such that $ax \equiv 1 \pmod{1,000,000}$. In this case, our decryption function is $\delta(s) = x(s - b) \pmod{1,000,000}$. Because we're now encrypting blocks of letters rather than single letters, frequency analysis will not work here. In other words, affine block ciphers are reasonably secure as long as the block size is large enough (blocks of size four will most likely be big enough). Even though affine block ciphers are secure, there's still a problem with them. The problem is that they're symmetric. This means that anyone who knows the encryption function $\epsilon(m)$ also knows (or can easily figure out) the decryption function $\delta(s)$. For example, all one needs to do to figure out the formula for $\delta(s)$ given that $\epsilon(m) = am + b \pmod{1,000,000}$ is use the Extended Euclidean Algorithm to find x such that $ax \equiv 1 \pmod{1,000,000}$. This is easy to do either by hand or with the help of a computer.

Example 3.3 Suppose we want to set up correspondence where a message is encrypted with the key $(7, 11)$ and using a twenty-six letter alphabet. Substituting our given key and modulus into the Affine Cipher encryption function, we have $\epsilon(x) = 7x + 11 \pmod{26}$. Then, using Table 1, the message, ATTACK, has numerical equivalent

$$0, 19, 19, 0, 2, 10,$$

and to encrypt the plaintext we substitute the integer values into the Affine Cipher encryption function as follows

$$\begin{aligned} 7 \times 0 + 11 &\pmod{26} = 11 \pmod{26} = 11 \\ 7 \times 19 + 11 &\pmod{26} = 144 \pmod{26} = 14 \\ 7 \times 19 + 11 &\pmod{26} = 144 \pmod{26} = 14 \\ 7 \times 0 + 11 &\pmod{26} = 11 \pmod{26} = 11 \\ 7 \times 2 + 11 &\pmod{26} = 25 \pmod{26} = 25 \\ 7 \times 10 + 11 &\pmod{26} = 81 \pmod{26} = 3, \end{aligned}$$

hence, the numerical equivalents of the ciphertext are

$$11, 14, 14, 11, 25, 3.$$

Finally, we translate the encrypted integers back into letters using Table 1 and get LOOLZD.

All of the examples presented thus far have been calculated modulo 26, with the numbers 0 thru 25 corresponding to letters A thru Z respectively. When we take into consideration using lower case, upper case, punctuation, and other symbols,

more numbers are required. To help us define alphabets other than the standard twenty-six letter upper case alphabet, we will employ shifted ASCII codes, which are numerical values assigned to every character on a computer keyboard, to generate three additional alphabets, specifically, the Mod 29 alphabet, which is formed from the mod 26 alphabet by adding a space, period, and question mark, the Mod 89 alphabet, which are the ASCII codes of a certain 89 characters shifted left 34 units, and the Mod 95 alphabet, which are the ASCII codes shifted left 32 units.

Note 3.4 Each of these additional alphabets are located in Appendix [2, A].

<Table 1>

Decryption of the ciphertext obtained by applying the Affine Cipher encryption function can be accomplished similar to the encryption process. However, as we seen with the Shift Cipher, we must first perform the steps, learned in algebra, to find the inverse function. As we previously stated, the Affine Cipher consists of both multiplication and addition and unlike the Shift Cipher, it is necessary to define the multiplicative inverse of an integer a modulo m .

Note 3.5 For the purposes of this project, the multiplicative inverses of invertible elements in the alphabets modulo 26, 29, 89, and 95 will be supplied in Appendix [2, B]. However, there is a process that can be used to calculate the multiplicative inverse, generally seen in Discrete Mathematics and Number Theory, known as the Euclidean Algorithm.

Example 3.6 Using the derived decryption function for the Affine Cipher, let us decipher the ciphertext, LOOLZD, from the previous example to ensure we get the correct plaintext. Our plaintext was encrypted using a key of $(7, 11)$, where $a = 7$ and $b = 11$, and therefore we must first find 7^{-1} modulo 26.

By Table 2, $7^{-1} = 15$, so our decryption formula will be

$$\delta(x) = 15(x - 11) \pmod{26}.$$

The numerical equivalents of the encrypted message are

$$11, 14, 14, 11, 25, 3.$$

Substituting these values for x in the derived decryption function we get

$$\begin{aligned} 15(11 - 11) \pmod{26} &= 0 \pmod{26} = 0 \\ 15(14 - 11) \pmod{26} &= 45 \pmod{26} = 19 \\ 15(14 - 11) \pmod{26} &= 45 \pmod{26} = 19 \\ 15(11 - 11) \pmod{26} &= 0 \pmod{26} = 0 \\ 15(25 - 11) \pmod{26} &= 210 \pmod{26} = 2 \\ 15(3 - 11) \pmod{26} &= -120 \pmod{26} = 10 \end{aligned}$$

Therefore, the numerical equivalents of our calculated plaintext are

$$0, 19, 19, 0, 2, 10.$$

Finally, the last step is to translate the decrypted integers back into letters using Table 1, and get ATTACK.

<Table 2>

Now suppose we want to encrypt a message twice. Suppose we use the mod 95 alphabet in Appendix [2, A], we would then need to select two separate keys, say $(17, 62)$ and $(9, 24)$. Substituting our two keys and the selected modulus into the Affine Cipher encryption function, we get two functions g and h as follows

$$g(x) = 17x + 62 \pmod{95}, h(x) = 9x + 24 \pmod{95}.$$

Using the same process as the previous example, let us encrypt the message, Retreat NOW!, first using function g and then h . Do note, since we are using a 95 character alphabet, we must take into account using lower and upper case letters, punctuation, and empty spaces. Using Mod 95 Alphabet, in Appendix [2, A], the numerical equivalents of Retreat NOW! are

$$50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1$$

and encrypting the message by first using g we get

$$17 \times 50 + 62 \pmod{95} = 912 \pmod{95} = 57$$

$$\begin{aligned}
17 \times 69 + 62 \pmod{95} &= 1235 \pmod{95} = 0 \\
17 \times 84 + 62 \pmod{95} &= 1490 \pmod{95} = 65 \\
17 \times 82 + 62 \pmod{95} &= 1456 \pmod{95} = 31 \\
17 \times 69 + 62 \pmod{95} &= 1235 \pmod{95} = 0 \\
17 \times 65 + 62 \pmod{95} &= 1167 \pmod{95} = 27 \\
17 \times 84 + 62 \pmod{95} &= 1490 \pmod{95} = 65 \\
17 \times 0 + 62 \pmod{95} &= 62 \pmod{95} = 62 \\
17 \times 46 + 62 \pmod{95} &= 844 \pmod{95} = 84 \\
17 \times 47 + 62 \pmod{95} &= 861 \pmod{95} = 6 \\
17 \times 55 + 62 \pmod{95} &= 997 \pmod{95} = 47 \\
17 \times 1 + 62 \pmod{95} &= 79 \pmod{95} = 79
\end{aligned}$$

hence, the integer values of the encrypted plaintext using g are

$$57, 0, 65, 31, 0, 27, 65, 62, 84, 6, 47, 79.$$

For the second encryption, we will use the integer values found using g and plug them into h as follows

$$\begin{aligned}
9 \times 57 + 24 \pmod{95} &= 537 \pmod{95} = 62 \\
9 \times 0 + 24 \pmod{95} &= 24 \pmod{95} = 24 \\
9 \times 65 + 24 \pmod{95} &= 609 \pmod{95} = 39 \\
9 \times 31 + 24 \pmod{95} &= 303 \pmod{95} = 18 \\
9 \times 0 + 24 \pmod{95} &= 24 \pmod{95} = 24 \\
9 \times 27 + 24 \pmod{95} &= 267 \pmod{95} = 77 \\
9 \times 65 + 24 \pmod{95} &= 609 \pmod{95} = 39 \\
9 \times 62 + 24 \pmod{95} &= 582 \pmod{95} = 12 \\
9 \times 84 + 24 \pmod{95} &= 780 \pmod{95} = 20 \\
9 \times 6 + 24 \pmod{95} &= 78 \pmod{95} = 78 \\
9 \times 47 + 24 \pmod{95} &= 447 \pmod{95} = 67 \\
9 \times 79 + 24 \pmod{95} &= 735 \pmod{95} = 70
\end{aligned}$$

After twice encrypting the plaintext with a key of $(17, 62)$ and then with $(9, 24)$ we get the integers

$$62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.$$

Finally, we translate the encrypted integers back into letters using the Mod 95 Alphabet in Appendix [2, A] and get the following ciphertext

$$\wedge 8 G 2 8 m G, 4 n c f.$$

The process of encrypting plaintext multiple times can be lengthy and time consuming. To shorten the process we can use function composition to create one function for encryption. However, before we begin it is important to note that $f(k(x)) \neq k(f(x))$, except for special cases, therefore, we must take caution when performing function composition. As a general rule, take the first encryption function and insert into the second encryption function. In our case take g and insert it into h , specifically $f(x) = h(g(x))$, as follows

$$\begin{aligned}
9(17x + 62) + 24 \pmod{95} \\
153x + 558 + 24 \pmod{95} \\
153x + 582 \pmod{95}
\end{aligned}$$

Since we are calculating modulo 95, all integer values must be reduced modulo 95. Hence, our new function composition is $f(x) = 58x + 12 \pmod{95}$.

Using our function composition, let us encrypt the same message, Retreat NOW!, to show we get the same ciphertext as the process of double encrypting. First, using Mod 95 Alphabet, in Appendix [2, A], the numerical equivalents of Retreat NOW! are 50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1 and encrypting using f we get

$$\begin{aligned} 58 \times 50 + 12 \pmod{95} &= 2912 \pmod{95} = 62 \\ 58 \times 69 + 12 \pmod{95} &= 4014 \pmod{95} = 24 \\ 58 \times 84 + 12 \pmod{95} &= 4884 \pmod{95} = 39 \\ 58 \times 82 + 12 \pmod{95} &= 4768 \pmod{95} = 18 \\ 58 \times 69 + 12 \pmod{95} &= 4014 \pmod{95} = 24 \\ 58 \times 65 + 12 \pmod{95} &= 3782 \pmod{95} = 77 \\ 58 \times 84 + 12 \pmod{95} &= 4884 \pmod{95} = 39 \\ 58 \times 0 + 12 \pmod{95} &= 12 \pmod{95} = 12 \\ 58 \times 46 + 12 \pmod{95} &= 2680 \pmod{95} = 20 \\ 58 \times 47 + 12 \pmod{95} &= 2738 \pmod{95} = 78 \\ 58 \times 55 + 12 \pmod{95} &= 3202 \pmod{95} = 67 \\ 58 \times 1 + 12 \pmod{95} &= 70 \pmod{95} = 70 \end{aligned}$$

The resulting integers after applying our composition function are

$$62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70,$$

and using Mod 95 Alphabet in Appendix [2, A] we can look up the ciphertext, which is

$$\wedge 8 G 2 8 m G, 4 n c f$$

Finally, we can see that we can use function composition in place of using multiple encryption functions which will save time and tedious computations. Decrypting the previous example can be accomplished by finding and applying $f^{-1}(x)$ to the ciphertext or by finding and applying $h^{-1}(x)$ then $g^{-1}(x)$ to the ciphertext. We will show both processes. First, we will apply $f^{-1}(x)$ to the ciphertext. Since our plaintext was encrypted using the key $(58, 12)$, where $a = 58$ and $b = 12$, we must find 58^{-1} modulo 95. Using the Multiplicative Inverses modulo 95 table in Appendix [2, B], $58^{-1} = 77$. Substituting 58^{-1} and $b = 12$ into the Affine Cipher decryption function, we get

$$f^{-1}(x) = 77(x - 12) \pmod{95}.$$

Now, using the Mod 95 Alphabet in Appendix [2, A], the numerical equivalents of the encrypted message are

$$62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.$$

Substituting these values for x in the derived decryption function we get

$$\begin{aligned} 77(62 - 12) \pmod{95} &= 3850 \pmod{95} = 50 \\ 77(24 - 12) \pmod{95} &= 924 \pmod{95} = 69 \\ 77(39 - 12) \pmod{95} &= 2079 \pmod{95} = 84 \\ 77(18 - 12) \pmod{95} &= 462 \pmod{95} = 82 \\ 77(24 - 12) \pmod{95} &= 924 \pmod{95} = 69 \\ 77(77 - 12) \pmod{95} &= 5005 \pmod{95} = 65 \\ 77(39 - 12) \pmod{95} &= 2079 \pmod{95} = 84 \\ 77(12 - 12) \pmod{95} &= 0 \pmod{95} = 0 \end{aligned}$$

$$\begin{aligned}
77(20 - 12) \pmod{95} &= 616 \pmod{95} = 46 \\
77(78 - 12) \pmod{95} &= 5082 \pmod{95} = 47 \\
77(67 - 12) \pmod{95} &= 4235 \pmod{95} = 55 \\
77(70 - 12) \pmod{95} &= 4466 \pmod{95} = 1
\end{aligned}$$

Therefore, the numerical equivalents of our calculated plaintext are

$$50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1.$$

Finally, the last step is to translate the decrypted integers back into characters using the Mod 95 Alphabet in Appendix [2, A], and get Retreat NOW! For our second option, we need to find and apply $h^{-1}(x)$ then $g^{-1}(x)$. For h , our key was (9, 24), where $a = 9$ and $b = 24$, and we must therefore find 9^{-1} modulo 95. Using the Multiplicative Inverses modulo 95 table in Appendix [2, B], $9^{-1} = 74$. Substituting 9^{-1} and $b = 24$ into the Affine Cipher decryption function we get $h^{-1}(x) = 74(x - 24) \pmod{95}$. For g , our key was (17, 62), where $a = 17$ and $b = 62$, and we must therefore find 17^{-1} modulo 95. Using the Multiplicative Inverses modulo 95 table in Appendix [2, B], $17^{-1} = 28$. Substituting 17^{-1} and $b = 62$ into the Affine Cipher decryption function we get

$$g^{-1}(x) = 28(x - 62) \pmod{95}$$

Now, using the Mod 95 Alphabet in Appendix [2, A], the numerical equivalents of the encrypted message, $\wedge 8 G 2 8 m G, 4 n c f$, are

$$62, 24, 39, 18, 24, 77, 39, 12, 20, 78, 67, 70.$$

Substituting these values for x into h^{-1} first we get

$$\begin{aligned}
74(62 - 24) \pmod{95} &= 2812 \pmod{95} = 57 \\
74(24 - 24) \pmod{95} &= 0 \pmod{95} = 0 \\
74(39 - 24) \pmod{95} &= 1110 \pmod{95} = 65 \\
74(18 - 24) \pmod{95} &= -444 \pmod{95} = 31 \\
74(24 - 24) \pmod{95} &= 0 \pmod{95} = 0 \\
74(77 - 24) \pmod{95} &= 3922 \pmod{95} = 27 \\
74(39 - 24) \pmod{95} &= 1110 \pmod{95} = 65 \\
74(12 - 24) \pmod{95} &= -888 \pmod{95} = 62 \\
74(20 - 24) \pmod{95} &= -296 \pmod{95} = 84 \\
74(78 - 24) \pmod{95} &= 3996 \pmod{95} = 6 \\
74(67 - 24) \pmod{95} &= 3182 \pmod{95} = 47 \\
74(70 - 24) \pmod{95} &= 3404 \pmod{95} = 79
\end{aligned}$$

hence, the integer values from first applying h^{-1} to the ciphertext are

$$57, 0, 65, 31, 0, 2765, 62, 84, 6, 47, 79.$$

Next, we will use the integer values found using h^{-1} and substitute them into g^{-1} as follows

$$\begin{aligned}
28(57 - 62) \pmod{95} &= -140 \pmod{95} = 50 \\
28(0 - 62) \pmod{95} &= -1736 \pmod{95} = 69 \\
28(65 - 62) \pmod{95} &= 84 \pmod{95} = 84 \\
28(31 - 62) \pmod{95} &= -868 \pmod{95} = 82 \\
28(0 - 62) \pmod{95} &= -1736 \pmod{95} = 69 \\
28(27 - 62) \pmod{95} &= -980 \pmod{95} = 65
\end{aligned}$$

$$\begin{aligned}
28(65 - 62) \pmod{95} &= 84 \pmod{95} = 84 \\
28(62 - 62) \pmod{95} &= 0 \pmod{95} = 0 \\
28(84 - 62) \pmod{95} &= 616 \pmod{95} = 46 \\
28(6 - 62) \pmod{95} &= -1568 \pmod{95} = 47 \\
28(47 - 62) \pmod{95} &= -420 \pmod{95} = 55 \\
28(79 - 62) \pmod{95} &= 476 \pmod{95} = 1
\end{aligned}$$

Therefore, the numerical equivalents, after apply h^{-1} and g^{-1} , of our calculated plaintext are

$$50, 69, 84, 82, 69, 65, 84, 0, 46, 47, 55, 1.$$

Finally, the last step is to translate the decrypted integers back into characters using the Mod 95 Alphabet in Appendix [2, A], and get

Retreat NOW!

We have shown that text encrypted by the composition, $f = hog$, can be decrypted in two ways: first, by finding f^{-1} and applying it to the ciphertext or second, by applying h^{-1} to the ciphertext and then applying g^{-1} to the result. Thus illustrating

$$f^{-1} = (hog)^{-1} = (g^{-1}oh^{-1}).$$

4. Hill Cipher

In this section, whenever possible we follow the notation, terminology and examples of (Castaneda, 2009, chapter 4).

Introduced in 1929 by Lester Hill, the Hill cipher is a poly-alphabetic cipher that uses matrices to encode plaintext messages. The key for this cipher system consist of an $n \times n$ square invertible matrix A , where the larger the dimensions the more secure the encryption will be. To ensure the key matrix A is invertible it is important to note that the determinant of A , $\det(A)$, must be relatively prime to the modulus m . The basic idea of the Hill cipher is to put the letters of the plaintext into blocks of length n , assuming an $n \times n$ key matrix, and then each block of plaintext letters is then converted into a column matrix of integers according to the alphabet chosen and then pre-multiplied by the $n \times n$ key matrix. The results are then converted back to letters and the ciphertext message is produced. Due to the complexity of working with large matrices, we will stick with using a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ that is invertible modulo 26 and where $\det(A) = (ad - bc) \pmod{26}$.

Example 4.1 Suppose we want to encrypt the message *TROJAN* using the key matrix $\begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix}$ modulo 26. The first step is to assign each letter of the plaintext its numerical equivalent, using Table 1, which are

$$19, 17, 14, 9, 0, 13.$$

In the event that the length of the plaintext is not a multiple of the size of the key matrix, random letters can be added to the end of the plaintext. We then perform matrix multiplication as follows

$$\begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 19 \\ 17 \end{bmatrix} = \begin{bmatrix} 176 \\ 341 \end{bmatrix} = \begin{bmatrix} 20 \\ 30 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 14 \\ 9 \end{bmatrix} = \begin{bmatrix} 105 \\ 216 \end{bmatrix} = \begin{bmatrix} 1 \\ 8 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 3 & 7 \\ 9 & 10 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 91 \\ 130 \end{bmatrix} = \begin{bmatrix} 13 \\ 0 \end{bmatrix} \pmod{26}$$

So the numerical equivalents of the ciphertext are

$$20, 3, 1, 8, 13, 0.$$

This corresponds to the letter sequence

UDBINA.

As previously stated, when selecting a key matrix A it is imperative that it be invertible. To determine if the key matrix A is invertible, the $\det(A)$ must be relatively prime to the modulus m . By definition of an inverse matrix, the inverse of a matrix must be a matrix such that when multiplied by the original matrix, or key matrix in our case, the product yields the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

There are at least a couple techniques for finding the inverse of an invertible matrix, whose entries come from a ring $\langle \mathbb{Z}, +, \cdot \rangle$, where $+$ denotes addition modulo m and \cdot denotes multiplication modulo m . It is possible to use a modified Gauss-Jordan method for finding inverses of 2×2 invertible matrices. For a 2×2 invertible matrix, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we will use the following rule $A^{-1} = [\det(A)]^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{m}$, where $[\det(A)]^{-1}$ is the multiplicative inverse of $\det(A)$ modulo m , provided it exists. To decipher the previous encrypted message, *UDBINA*, which was encrypted with the key matrix, we need to find A^{-1} . First, since the $\det(A) = 30 - 63 = -33 = 19 \pmod{26}$, we have

$$A^{-1} = 19^{-1} \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} \pmod{26}.$$

Using the multiplicative inverse modulo 26 table in Appendix [2, B], $19^{-1} = 11$. Hence we have

$$A^{-1} = 11 \begin{bmatrix} 10 & -7 \\ -9 & 3 \end{bmatrix} = \begin{bmatrix} 110 & -77 \\ -99 & 33 \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \pmod{26}.$$

Now, the numerical equivalents of the ciphertext are

$$20, 3, 1, 8, 13, 0,$$

and we calculate

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 20 \\ 3 \end{bmatrix} = \begin{bmatrix} 123 \\ 121 \end{bmatrix} = \begin{bmatrix} 19 \\ 17 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 8 \end{bmatrix} = \begin{bmatrix} 14 \\ 61 \end{bmatrix} = \begin{bmatrix} 14 \\ 9 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 6 & 1 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 78 \\ 65 \end{bmatrix} = \begin{bmatrix} 0 \\ 13 \end{bmatrix} \pmod{26}$$

The numerical equivalents of the calculated plaintext is

$$19, 17, 14, 9, 0, 13,$$

and converting each calculated integer to its respective letter using Table 1 we obtain

TROJAN.

The Hill cipher is an excellent application that enables students to practice matrix operations in an interesting and exciting way. As with the previous examples of classical ciphers, it is assumed that the student is familiar with each classical cipher's respective mathematical process.

5. Conclusion and Further Research

All our previous results show that the concepts of affine and Hill cipher in this paper can constitute a significant aspect of computer and information science. It is clear that its study started here can successfully be extended to cipher systems in which plaintext letters are enciphered mathematically by a linear function. This will surely be subject of some further research.

Finally, we mention an open problems concerning to this topic.

Problem 5.1 How can be generalized the affine cipher in which plaintext letters are enciphered mathematically by the function,

$$f(X) = AX + B \pmod{m}$$

where X, B are column matrixes and A is a $n \times n$ square matrix and m is the number of letters in the alphabet?

Acknowledgment

The authors are grateful to the reviewers for their comments and suggestions which improve the previous version of the paper. The research of the authors is supported by Islamic Azad University, Ashtian Branch. Also our proposal entitled “**Analysis and design of affine ciphers in cryptography**” is completed by this paper.

References

- Barr, Thomas. H. (2002). *Invitation to Cryptology*. Upper Saddle River, NJ: Prentice Hall, Inc.
- Castaneda, Rigoberto. G. (2009). Using Classical Ciphers in Secondary Mathematics. THESIS, Presented to the Honors Committee of McMurry University.
- Flannery, Sarah., & Flannery, David. (2001). *In Code: A Mathematical Journey*. Chapel Hill, NC: Algonquin Books of Chapel Hill.
- Shannon, Claude. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28, 657-715.
- Singh, Simon. (1999). *The Code Book*. Anchor Books, New York.
- Wrixon, Fred. B. (1998). *Codes, Ciphers, Secrets and Cryptic Communication*. Black Dog and Leventhal Publishers, Inc, New York.

Table 1. The integers corresponding to the twenty-six letter

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2. Multiplicative Inverses modulo 26

x	1	3	5	7	9	11	15	17	19	21	23	25
$x - 1 \pmod{26}$	1	9	21	15	3	19	7	23	11	5	17	25