

# Lecture 4: Classical Encryption Algorithms

Yuan Xue

In this lecture, we study two classical encryption forms: *substitution* and *transposition*, which serve as building blocks for many advanced encryption schemes. A *substitution* technique is one in which the letters of plaintext are replaced by other letters. In *transposition*, the order of the letters are rearranged.

## I. SUBSTITUTION

### A. Monoalphabetic Ciphers

The Caesar cipher which we introduced earlier is an example use of monoalphabetic substitution cipher, where a character is substituted for each character in the original message. In the general Caesar cipher, there are only 25 possible keys, which provides 25 possibilities in substitution. This is far from secure, as cryptanalyst can easily deduce the key by bruce-force attack. One way to increase the key space and improve the security of the cipher is to allow arbitrary substitution. In this case, the “cipher” line can be any permutation of the 26 alphabetic characters. Thus there are  $26!$  possible keys, making it harder for a bruce-force attack. However, there is another type of attack, which makes use of the regularity of the language, called *frequency analysis*. Frequency analysis studies the frequency of letters or groups of letters in a ciphertext. It is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language.

### B. Multiple-letter Ciphers

Multiple-letter encryption cipher treats consecutive letters in the plaintext as a single unit and translate the unit into ciphertext. Such ciphers lessen the extent to which the structure of the plaintext survives in the ciphertext, thus are stronger against frequency analysis.

#### **Playfair Cipher**

Playfair cipher was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher. Playfair cipher takes two-letter combinations (digrams) as single units for encryption.

The encryption algorithm takes a  $5 \times 5$  matrix of letters as a key table to translate digrams. The key table is constructed by a keyword. To generate the key table, the letters of the keyword (dropping any duplicate letters) are filled into the matrix from left to right, and from top to bottom (some other patterns, such as a spiral beginning in the upper-left-hand corner and ending in the center, are also allowed). Then the rest of the letters of the alphabet are filled into the remaining spaces of the key table. Since there are 26 letters in the alphabet, while only 25 spaces, letters “i” and “j” take the same space (or letter “q” is omitted). Table I shows an example of the key table with keyword “monarchy”.

To encrypt a message, the following four rules are applied to each digram in the plaintext:

- 1) If both letters are the same (or only one letter is left), add an “x” (any uncommon letter will do) after the first letter. For example, “balloon” would be treated as “ba lx lo on”.

m	o	n	a	r
c	h	y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

TABLE I  
EXAMPLE KEY TABLE FOR PLAYFAIR CIPHER

- 2) If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (the table wraps around). For example, ar is encrypted as RM based on Table I.
- 3) If the letters appear on the same column of the table, replace them with the letters immediately below respectively. For example, mu is encrypted as CM based on Table I.
- 4) If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. For example, hs is encrypted as BP, and ea is encrypted as IM (or JM).

To decrypt, use the inverse of these four rules and drop any extra "x"s that don't make sense in the final plaintext. The Playfair cipher is significantly harder to break in comparison with monoalphabetic cipher. But frequency analysis can still be undertaken over playfair cipher based on the  $26 \times 26 = 676$  possible digram instead of the 26 possible letters. Such frequency analysis is more difficult, as it generally requires more ciphertext.

### Hill Cipher

Hill cipher was invented by Lester Hill in 1929. In the encryption algorithm,  $n$  successive letters in plaintext are considered as a  $n$ -dimension vector  $P$ . The algorithm takes a  $n \times n$  matrix  $K$  as a key. The ciphertext  $C$  of  $P$  is also a  $n$ -dimension vector derived by multiplying  $P$  by  $K$ , modulo 26. That is  $C = (KP) \bmod(26)$ . The inverse of the matrix  $K$  is used to decrypt the ciphertext. The inverse  $K^{-1}$  of a matrix  $K$  is defined by the equation  $KK^{-1} = K^{-1}K = I$ , where  $I$  is the identity matrix<sup>1</sup>. In particular, the plaintext  $P$  is derived by multiplying ciphertext  $C$  by  $K^{-1}$ , i.e.,  $P = (K^{-1}C) \bmod(26)$ . The cryptographic system of Hill cipher can be summarized as follows.

$$C = E(K, P) = (KP) \bmod(26) \quad (1)$$

$$P = D(K, C) = (K^{-1}C) \bmod(26) = K^{-1}KP = P \quad (2)$$

Here we illustrate Hill cipher using an example. Consider the plaintext "paymoremoney", and the key

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The plaintext is decomposed into 3-letter blocks. For the first block "pay", its corresponding vector is (15, 0, 24). Then its ciphertext can be derived as

<sup>1</sup>Identity matrix is the matrix with ones on the main diagonal and zeros elsewhere.

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 & 0 & 24 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 375 & 819 & 486 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 11 & 13 & 18 \end{pmatrix} = LNS$$

Applying the same encryption over the rest of 3-letter blocks, we have the ciphertext of the entire plaintext LNSHDLEWMTRW. For decryption, the inverse of key matrix is used.

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

For the first 3-letter block in the ciphertext LNS, its decryption is demonstrated as follows.

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 & 13 & 18 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 431 & 494 & 570 \end{pmatrix} \text{mod}(26) = \begin{pmatrix} 15 & 0 & 24 \end{pmatrix} = pay$$

The use of a larger  $n$ -dimension vector in Hill cipher hides more frequency information, thus provides stronger protection against frequency analysis. Yet Hill cipher is easily broken with a *known plaintext attack*, because it is completely linear. An opponent who intercepts  $n^2$  plaintext/ciphertext character pairs can set up a linear system which can be solved to derive the key matrix.

### C. Polyalphabetic Ciphers

Polyalphabetic cipher uses different monoalphabetic substitution as it proceeds through the plaintext. Usually a polyalphabetic cipher defines

- A set of monoalphabetic substitution rules;
- A key that determines which particular rule is chosen for a given transformation.

#### Vigenère cipher

The Vigenère cipher uses a series of general Caesar ciphers with different values of  $K$  based on the letters of a keyword. To encrypt a message, a key is needed that is as long as the message. Given a letter  $p_i$  in the plaintext, there is a key letter  $k_i$  corresponding to  $p_i$ . The ciphertext letter  $c_i$  of  $p_i$  is determined by  $c_i = (p_i + k_i) \text{mod}(26)$  based on the general Caesar cipher with key value  $k_i$ .

To acquire a key that is as long as the message, we can pick a keyword and derive the key by repeating the keyword. For example, if the keyword is *deceptive*, then the message “we are discovered” is encrypted as follows:

key	d	e	c	e	p	t	i	v	e	d	e	c	e	p	t
plaintext	w	e	a	r	e	d	i	s	c	o	v	e	r	e	d
ciphertext	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W

TABLE II

MESSAGE ENCRYPTED BY VIGENÈRE CIPHER

Decryption is straightforward based on the key and the rule of general Caesar cipher. The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique

letter of the keyword. Thus, the letter frequency information is obscured. On the other hand, the strength of a Vigenère cipher depends on its keyword length. If the keyword is relatively short, when constantly repeated, some letter groups in plaintext (such as red in the example) will likely be encrypted using the same key letters, leading to repeated groups in the ciphertext (such as VTW in the example). The periodic nature of the key can be eliminated by an autokey system, in which a running key as long as the message is provided by concatenating the plaintext itself to the keyword. In the previous example, the running key is *deceptivewared*. But because the key and the plaintext share the same frequency distribution of the letters, a statistical technique can still be applied by a cryptanalyst.

### One-time Pad

Joseph Mauborgne suggested using a truly random key that is as long as the message with no repetitions. Such a scheme is known as *one-time pad*. Claude Shannon showed that the one-time pad has a property known as *perfect secrecy*: the ciphertext gives absolutely no additional information about the plaintext. Because the ciphertext bears no statistical relationship to the plaintext, there is no way to break the code.

However one-time pad is only a theoretically unbreakable method of encryption. It has two fundamental difficulties in practice:

- 1) Generation of large volume of perfectly random keys, which are at least as long as the messages.
- 2) Secure exchange of the key.

Because of these difficulties, the one-time pad encryption is of limited utility.

## II. TRANSPOSITION

Transposition technique changes the order of the letters in a message. We first illustrate this technique using a columnar transposition cipher.

### Columnar Transposition Cipher

To encrypt plaintext “attack postponed until two am”, columnar transposition cipher writes the message in a rectangle, row by row, and reads the message off, column by column, but permutes the order of the columns based on the key. The following table shows the encryption of the plaintext<sup>2</sup> and the ciphertext would be TTNAAPTMTSUOAODWCOIXKNLYPETZ.

key	4	3	1	2	5	6	7
plaintext	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

TABLE III  
COLUMNAR TRANSPOSITION CIPHER

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. A single columnar transposition could be attacked by guessing possible column lengths, and then looking for possible anagrams. This cipher can be made significantly more secure by performing more than one stage of transposition. The same key can be used for all transpositions, or different keys can be used.

<sup>2</sup>Filler letters are appended at the end.

### **Permutation Cipher**

A permutation cipher is a transposition cipher in which the key is a permutation. To apply a cipher, a random permutation of size  $n$  is generated (the larger the value of  $n$  the more secure the cipher). The plaintext is then broken into segments of size  $n$  and the letters within that segment are permuted according to this key. In theory, any transposition cipher can be viewed as a permutation cipher where  $n$  is equal to the length of the plaintext. However, in practice, such a generalization is too cumbersome to use.