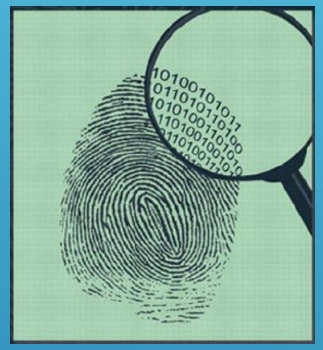
COMPUTER SECURITY



WILLIAM STALLINGS, CRYPTOGRAPHY AND NETWORK SECURITY, (PRINCIPLES AND PRACTICE), 2011

AL-MANSOUR UNIVERSITY COLLEGE
CSIS DEPARTMENT 4TH CLASS 2020
DR. MAY KAMIL

PLAYFAIR CIPHER

- The **Playfair cipher** or **Playfair square** is a manual symmetric encryption technique and was the first literal digraph substitution cipher.
- The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher.

  - The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher.

PLAYFAIR CIPHER

The 'key' for a playfair cipher is generally a word

for the sake of example we will choose 'monarchy'. This is then used to generate a ‘ 'key square', e.g.

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

Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats. Note that there is no 'j', it is combined with 'i'. We now apply the encryption rules to encrypt the plaintext.

1. Remove any punctuation or characters that are not present in the key square (this may mean spelling out numbers, punctuation etc.).
2. Identify any double letters in the plaintext and replace the second occurence with an 'x' e.g. 'hammer' -> 'hamxer'.
3. If the plaintext has an odd number of characters, append an 'x' to the end to make it even.
4. Break the plaintext into pairs of letters, e.g. 'hamxer' -> 'ha mx er'
5. The algorithm now works on each of the letter pairs.

PLAYFAIR CIPHER

6. Locate the letters in the key square, (the examples given are using the key square above)

a. If the letters are in different rows and columns, replace the pair with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter. 'ha' -> 'bo', 'es' -> 'il'

b.If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row). 'ma' -> 'or', 'lp' -> 'pq'

c.If the letters appear on the same column of the table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column). 'rk' -> 'dt', 'pv' -> 'vo'

EXAMPLE :

An example encryption, "we are discovered, save yourself" using the key square shown at the beginning of this section

`Plaintext: wearediscoveredsaveyourselfx`

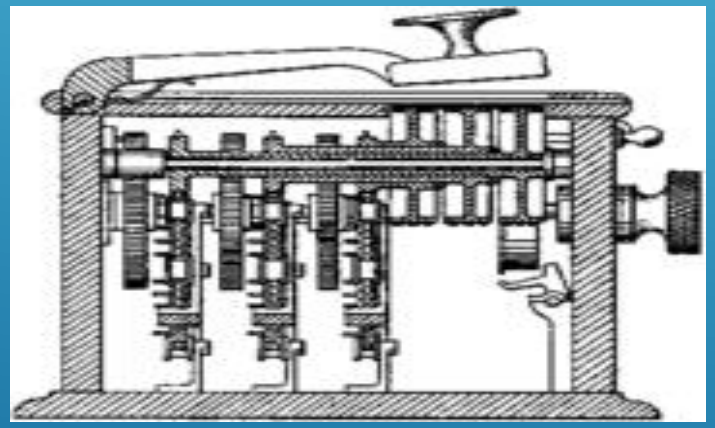
Ciphertext : `ugrmkcsxhmufmkbtoxgcmvatluiv`

ANALYSIS

- Size of diagrams: 25!
  - But the actual different diagrams are not 25!
  - Two iagrams are the same if they derive the same encryption and decryption method
  - Then what is the number of difference diagrams in playfair cipher?
    - 25!/25=24!
- Difficult using frequency analysis
  - But it still reveals the frequency information
    - Frequency of 2-gram (bi-gram, two-letters)

HILL CIPHER

The **Hill cipher** is an **example** of a block **cipher**. A block **cipher** is a **cipher** in which groups of letters are enciphered together in equal length blocks. The **Hill cipher** was developed by Lester **Hill** and introduced in an article published in 1929



HILL CIPHER ENCRYPTION

To encrypt a message using the Hill Cipher we must first turn our keyword into a key matrix (a 2 x 2 matrix for working with digraphs, a 3 x 3 matrix for working with trigraphs, etc). We also turn the plaintext into digraphs (or trigraphs) and each of these into a column vector. We then perform matrix multiplication modulo the length of the alphabet (i.e. 26) on each vector. These vectors are then converted back into letters to produce the ciphertext.

$$C = (K * P) \bmod 26$$

HILL CIPHER EXAMPLE

We shall encrypt the plaintext message "retreat now" using the keyphrase ”*back up”* and a 3 x 3 matrix. The first step is to turn the key phrase into a matrix. Notice that the key phrase is a few letters short, so we fill in the final elements with the start of the alphabet.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}$$

Now we turn the keyword matrix into the key matrix by replacing letters with their numeric values.

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

Now we split the plaintext into trigraphs (we are using a 3 x 3 matrix so we need groups of 3 letters), and convert these into column vectors. However, since the plaintext does not go perfectly into the column vectors, we need to use some nulls to make the plaintext the right length. We then convert these into numeric column vectors.

$$\begin{pmatrix} r \\ e \\ t \end{pmatrix} \begin{pmatrix} r \\ e \\ a \end{pmatrix} \begin{pmatrix} t \\ n \\ o \end{pmatrix} \begin{pmatrix} w \\ x \\ x \end{pmatrix}$$

The plaintext converted into numeric column vectors.

$$\begin{pmatrix}17\\4\\19\end{pmatrix}\begin{pmatrix}17\\4\\0\end{pmatrix}\begin{pmatrix}19\\13\\14\end{pmatrix}\begin{pmatrix}22\\23\\23\end{pmatrix}$$

Now we perform matrix multiplication, multiplying the key matrix by each column vector in turn.

The first matrix multiplication.

$$\begin{pmatrix}1&0&2\\10&20&15\\0&1&2\end{pmatrix}\begin{pmatrix}17\\4\\19\end{pmatrix}$$

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} r \\ e \\ t \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 19 \\ 10 \times 17 + 20 \times 4 + 15 \times 19 \\ 0 \times 17 + 1 \times 4 + 2 \times 19 \end{pmatrix}$$

$$= \begin{pmatrix} 55 \\ 535 \\ 42 \end{pmatrix}$$

$$= \begin{pmatrix} 3 \\ 15 \\ 16 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} D \\ P \\ Q \end{pmatrix}$$

Encryption of the first trigraph.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix} \begin{pmatrix} r \\ e \\ a \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 0 \\ 10 \times 17 + 20 \times 4 + 15 \times 0 \\ 0 \times 17 + 1 \times 4 + 2 \times 0 \end{pmatrix}$$

$$= \begin{pmatrix} 17 \\ 250 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 17 \\ 16 \\ 4 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} R \\ Q \\ E \end{pmatrix}$$

Encryption of the second trigraph.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} t \\ n \\ o \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 19 + 0 \times 13 + 2 \times 14 \\ 10 \times 19 + 20 \times 13 + 15 \times 14 \\ 0 \times 19 + 1 \times 13 + 2 \times 14 \end{pmatrix}$$

$$= \begin{pmatrix} 47 \\ 660 \\ 41 \end{pmatrix}$$

$$= \begin{pmatrix} 21 \\ 10 \\ 15 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} V \\ K \\ P \end{pmatrix}$$

Encryption of the third trigraph.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} w \\ x \\ x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 22 + 0 \times 23 + 2 \times 23 \\ 10 \times 22 + 20 \times 23 + 15 \times 23 \\ 0 \times 22 + 1 \times 23 + 2 \times 23 \end{pmatrix}$$

$$= \begin{pmatrix} 68 \\ 1025 \\ 69 \end{pmatrix}$$

$$= \begin{pmatrix} 16 \\ 11 \\ 17 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} Q \\ L \\ R \end{pmatrix}$$

Encryption of the fourth trigraph.

This gives us a final ciphertext of "DPQRQ EVKPQ LR".

Decryption

To decrypt a ciphertext encoded using the Hill Cipher, we must find the inverse matrix. Once we have the inverse matrix, the process is the same as encrypting. That is we multiply the inverse key matrix by the column vectors that the ciphertext is split into, take the results modulo the length of the alphabet, and finally convert the numbers back to letters.

$P= (K^{-1} * C) \bmod 26$

In general, to find the inverse of the key matrix, we perform the calculation below, where *K* is the key matrix, *d* is the determinant of the key matrix and *adj*(*K*) is the adjugate matrix of K.

$$K^{-1} = d^{-1} \times adj(K)$$

2 x 2 Example

We shall decrypt the example above, so we are using the keyword *hill* and our ciphertext is "APADJ TFTWLFJ". We start by writing out the keyword as a matrix and converting this into a key matrix as for encryption. Now we must convert this to the inverse key matrix, for which there are several steps.

The keyword written as a matrix.

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix}$$

The key matrix (each letter of the keyword is converted to a number).

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

Step 1 - Find the Multiplicative Inverse of the Determinant

The determinant is a number that relates directly to the entries of the matrix. It is found by multiplying the top left number by the bottom right number and subtracting from this the product of the top right number and the bottom left number. This is shown algebraically below. Note that the notation for determinant has straight lines instead of brackets around our matrix.

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

Once we have found this value, we need to take the number modulo 26. Below is the way to calculate the determinant for our example.

$$\begin{vmatrix} 7 & 8 \\ 11 & 11 \end{vmatrix} = 7 \times 11 - 8 \times 11 = -11 = 15 \ mod \ 26$$

Calculating the determinant of our 2 x 2 key matrix.

We now have to find the multiplicative inverse of the determinant working modulo 26. That is, the number between 1 and 25 that gives an answer of 1 when we multiply it by the determinant. So, in this case, we are looking for the number that we need to multiply 15 by to get an answer of 1 modulo 26.
If d is the determinant, then we are looking for the inverse of d.

$$d d^{-1} = 1 \ mod \ 26$$

The multiplicative inverse is the number we multiply 15 by to get 1 modulo 26. $15 \times x = 1 \, mod \, 26$

This calculation gives us an answer of 1 modulo 26.
So the multiplicative inverse of the determinant
modulo 26 is 7. We shall need this number later.

$$15 \times 7 = 105 = 1 \, mod \, 26$$

Step 2 - Find the Adjugate Matrix

The adjugate matrix is a matrix of the same size as the original. For a 2 x 2 matrix, this is fairly straightforward as it is just moving the elements to different positions and changing a couple of signs. That is, we swap the top left and bottom right numbers in the key matrix, and change the sign of the top right and bottom left numbers. Algebraically this is given below.

$$adj \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Again, once we have these values we will need to take each of them modulo 26 (in particular, we need to add 26 to the negative values to get a number between 0 and 25. For our example we get the matrix below

$$adj\begin{pmatrix}7 & 8\\11 & 11\end{pmatrix} = \begin{pmatrix}11 & -8\\-11 & 7\end{pmatrix} = \begin{pmatrix}11 & 18\\15 & 7\end{pmatrix}$$

Step 3 - Multiply the Multiplicative Inverse of the Determinant by the Adjugate Matrix

To get the inverse key matrix, we now multiply the inverse determinant (that was 7 in our case) from step 1 by each of the elements of the adjacent matrix from step 2. Then we take each of these answers modulo 26.

$$7 \times \begin{pmatrix}11 & 18\\15 & 7\end{pmatrix} = \begin{pmatrix}77 & 126\\165 & 49\end{pmatrix} = \begin{pmatrix}25 & 22\\1 & 23\end{pmatrix} \ mod\ 26$$

Multiplying the multiplicative inverse of the determinant by the adjugate to get the inverse key matrix. NB - note that the 165 should read 105, That is:

Now we have the inverse key matrix, we have to convert the ciphertext into column vectors and multiply the inverse matrix by each column vector in turn, take the results modulo 26 and convert these back into letters to get the plaintext.

$$if\ K = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}, then\ K^{-1} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}$$

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ P \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 15 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix}$$

$$= \begin{pmatrix} 330 \\ 345 \end{pmatrix}$$

$$= \begin{pmatrix} 18 \\ 7 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} s \\ h \end{pmatrix}$$

The decryption of the first digraph.

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} A \\ D \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 0 + 22 \times 3 \\ 1 \times 0 + 23 \times 3 \end{pmatrix}$$

$$= \begin{pmatrix} 66 \\ 69 \end{pmatrix}$$

$$= \begin{pmatrix} 14 \\ 17 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} o \\ r \end{pmatrix}$$

The decryption of the second digraph.

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} J \\ T \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 9 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 9 + 22 \times 19 \\ 1 \times 9 + 23 \times 19 \end{pmatrix}$$

$$= \begin{pmatrix} 643 \\ 446 \end{pmatrix}$$

$$= \begin{pmatrix} 19 \\ 4 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} t \\ e \end{pmatrix}$$

The decryption of the third digraph.

$$\begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} F \\ T \end{pmatrix} = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix}\begin{pmatrix} 5 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 25 \times 5 + 22 \times 19 \\ 1 \times 5 + 23 \times 19 \end{pmatrix}$$

$$= \begin{pmatrix} 543 \\ 442 \end{pmatrix}$$

$$= \begin{pmatrix} 23 \\ 0 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} x \\ a \end{pmatrix}$$

The decryption of the fourth digraph.

$$\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}W\\ L\end{pmatrix}=\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}22\\ 11\end{pmatrix}$$

$$=\begin{pmatrix}25\times 22+22\times 11\\ 1\times 22+23\times 11\end{pmatrix}$$

$$=\begin{pmatrix}792\\ 275\end{pmatrix}$$

$$=\begin{pmatrix}12\\ 15\end{pmatrix}\ mod\ 26$$

$$=\begin{pmatrix}m\\ p\end{pmatrix}$$

The decryption of the fifth digraph.

$$\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}F\\ J\end{pmatrix}=\begin{pmatrix}25 & 22\\ 1 & 23\end{pmatrix}\begin{pmatrix}5\\ 9\end{pmatrix}$$

$$=\begin{pmatrix}25\times 5+22\times 9\\ 1\times 5+23\times 9\end{pmatrix}$$

$$=\begin{pmatrix}323\\ 212\end{pmatrix}$$

$$=\begin{pmatrix}11\\ 4\end{pmatrix}\ mod\ 26$$

$$=\begin{pmatrix}l\\ e\end{pmatrix}$$

The decryption of the sixth digraph.

We get back our plaintext of "short example".