Hill Cipher Cryptography

The Playfair cipher encrypts digraphs – two-letter blocks. An attack by frequency analysis would involve analyzing the frequencies of the $26 \times 26 = 676$ digraphs of plaintext.

Frequency analysis would be more difficult if we had a cryptosystem that encrypted trigraphs – three-letter blocks. Frequency analysis would involve knowing the frequencies of the $26 \times 26 \times 26 = 17576$ trigraphs.

Systems that encrypted even larger blocks would make cryptanalysis even more difficult. There are

\[
26 \times 26 \times 26 \times 26 = 456976 \text{ blocks of length 4,}
\]
\[
26 \times 26 \times 26 \times 26 \times 26 = 11881376 \text{ blocks of length 5,}
\]
\[
26 \times 26 \times 26 \times 26 \times 26 \times 26 = 308915776 \text{ blocks of length 6} \ldots .
\]

Today many ciphers encrypt blocks of 16 letters. There are

\[
43,608,742,899,428,874,059,776
\]

16-letter blocks.

Cryptographers recognized the value of encrypting larger blocks, but they did not find an obvious way to extend the Playfair key square to three or more dimensions.

… cryptographers … tried to extend [Wheatstone’s Playfair cipher’s] geometrical technique to trigraphic substitutions. Nearly all have failed. Perhaps the best known effort was that of Count Luigi Gioppi di Tükheim, who in 1897 produced a pseudo-trigraphic system in which two letters were monoalphabetically enciphered and the third depended only on the second. Finally, about 1929, a young American mathematician. Jack Levine, used six $5 \times 5$ squares to encipher
trigraphs in an ingenious extension of the Playfair. But he did not disclose his method.

This was the situation when a 38-year-old assistant professor of mathematics at Hunter College in New York published a seven-page paper entitled “Cryptography in an Algebraic Alphabet” in *The American Mathematical Monthly* for June-July 1929. He was Lester S. Hill [1891? – 1961]. … Later in the summer in which his paper on algebraic cryptography appeared, he expanded the topic before the American Mathematical Society in Boulder, Colorado. This lecture was later published in *The American Mathematical Monthly* [March 1931] as “Concerning Certain Linear Transformation Apparatus of Cryptography.” *The Codebreakers* by David Kahn

The Hill cipher is based on theorems of linear algebra, which are independent of dimension; therefore, the method can be extended to any size block.
Matrices

The Hill cipher is usually taught by means of matrices.

A matrix is just a rectangular array of numbers. For example,

\[
\begin{bmatrix}
1 & 9 \\
-3 & 7
\end{bmatrix}, \quad \begin{bmatrix}
-1 & 2 & 17 \\
43 & 0 & 9
\end{bmatrix}, \quad \begin{bmatrix}
3
\end{bmatrix}, \quad \begin{bmatrix}
0 & 6 & -8 & 23 & 65 \\
-9 & 76 & 1 & 98 & -10 \\
11 & 7 & 34 & 72 & 1
\end{bmatrix}
\]

are all matrices.

The dimension of a matrix is given as

\[\text{number of rows} \times \text{number of columns}.\]

For the four matrices given above, the dimensions are 2\(\times\)2, 3\(\times\)3, 2\(\times\)1, and 3\(\times\)5, respectively. The dimensions are read as “2 by 2, 3 by 3, 2 by 1, and 3 by 5.”

If the number of rows equals the number of columns, the matrix is said to be a square matrix. The first two matrices above are square matrices.

If the matrix has only one column, the matrix is said to be a column matrix. The third matrix above is a column matrix.

We will deal exclusively with square and column matrices.

Matrices can be added, subtracted, multiplied, and in some cases divided just like numbers. The fact that an array of numbers can be treated in a way that is similar to the way a single number is treated (i.e., they can be added; subtracted; multiplied; and, sometimes, divided) is what permits the theory of matrices to extend cryptographic techniques to higher dimensions.
Multiplication by Square Matrices

One origin of matrices is the solution of systems of linear equations, and the multiplication of matrices reflects that use.

For example, consider this system of two linear equations in two variables $x$ and $y$. $a$, $b$, $c$, $d$, $u$, and $v$ represent constants (i.e., numbers).

\[
\begin{align*}
ax + by &= u \\
(cx + dy &= v)
\end{align*}
\]

This system of equations can be represented by one matrix equation

\[
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\begin{bmatrix}
x \\ y
\end{bmatrix} =
\begin{bmatrix}
u \\ v
\end{bmatrix}.
\]

The square matrix is called the coefficient matrix ($a$, $b$, $c$, and $d$ are the coefficients of the variables $x$ and $y$). There are two column matrices – one consisting of the two variables $x$ and $y$ and the other of the two constants that appear on the right hand side of the system $u$ and $v$.

For the moment, we will only consider matrix multiplication of the form

\[\text{\textit{square matrix}} \times \text{\textit{column matrix}}\]

Such a multiplication is only defined if the number of columns of the square matrix equals the number of rows of the column matrix.

The system of equations gives us the pattern for multiplication.

\[
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\begin{bmatrix}
x \\ y
\end{bmatrix} =
\begin{bmatrix}
ax + by \\ cx + dy
\end{bmatrix}
\]

The top entry of the product is calculated by, first, taking the entries of the first row of the square matrix and multiplying them "term-by-term" with the entries of the column matrix and then adding those products.
The lower entry of the product is calculated by, first, taking the entries of the second row of the square matrix and multiplying them "term-by-term" with the entries of the column matrix and then adding those products.

For example, 
\[
\begin{bmatrix}
3 & 7 \\
5 & 12
\end{bmatrix}
\begin{bmatrix}
8 \\
5
\end{bmatrix}
= 
\begin{bmatrix}
59 \\
100
\end{bmatrix}
\]

\[3 \times 8 + 7 \times 5 = 59\]
\[5 \times 8 + 12 \times 5 = 100\]

and 
\[
\begin{bmatrix}
3 & 7
\end{bmatrix}
\begin{bmatrix}
18 \\
2
\end{bmatrix}
= 
\begin{bmatrix}
68 \\
114
\end{bmatrix}
\]

\[3 \times 18 + 7 \times 2 = 68\]
\[5 \times 18 + 12 \times 2 = 114\]

Multiplication is defined similarly for higher dimension square and column matrices. For example, for \(3 \times 3\) matrices 
\[
\begin{bmatrix}
a & b & c \\
d & e & f \\
g & h & i
\end{bmatrix}
\begin{bmatrix}
x \\
y \\
z
\end{bmatrix}
= 
\begin{bmatrix}
ax + by + cz \\
dx + ey + fz \\
gx + hy + iz
\end{bmatrix}
\]

For example, 
\[
\begin{bmatrix}
1 & 0 & 7 \\
-3 & 4 & 9 \\
12 & -7 & 5
\end{bmatrix}
\begin{bmatrix}
5 \\
-3 \\
12
\end{bmatrix}
= 
\begin{bmatrix}
89 \\
81 \\
141
\end{bmatrix}
\]

\[1 \times 5 + 0 \times -3 + 7 \times 12 = 89\]
\[-3 \times 5 + 4 \times -3 + 9 \times 12 = 81\]
\[12 \times 5 + -7 \times -3 + 5 \times 12 = 141\]

Etc.

To multiply two square matrices of the same dimension, we do the multiplication one column at a time.
For example,
\[
\begin{bmatrix}
3 & 7 \\
5 & 12
\end{bmatrix}
\begin{bmatrix}
8 & 18 \\
5 & 2
\end{bmatrix}
=\begin{bmatrix}
59 & 68 \\
100 & 114
\end{bmatrix}.
\]

\[
\begin{bmatrix}
3 & 7 \\
5 & 12
\end{bmatrix}
\begin{bmatrix}
8 \\
5
\end{bmatrix}
=\begin{bmatrix}
59 \\
100
\end{bmatrix}
\text{ and }
\begin{bmatrix}
3 & 7 \\
5 & 12
\end{bmatrix}
\begin{bmatrix}
18 \\
2
\end{bmatrix}
=\begin{bmatrix}
68 \\
114
\end{bmatrix}.
\]

Representation of a matrix in Mathematica: \{\{3, 7\}, \{5, 12\}\}

In matrix form:

\[
\text{In}[11]= \text{MatrixForm}[\{\{3, 7\}, \{5, 12\}\}]
\]

\[
\text{Out}[11]//\text{MatrixForm}=
\begin{pmatrix}
3 & 7 \\
5 & 12
\end{pmatrix}
\]

Representation of a column matrix in Mathematica: \{\{8\}, \{5\}\}

In matrix form:

\[
\text{In}[12]= \text{MatrixForm}[\{\{8\}, \{5\}\}]
\]

\[
\text{Out}[12]//\text{MatrixForm}=
\begin{pmatrix}
8 \\
5
\end{pmatrix}
\]
Multiplication of square matrices:

\[
\text{In}[13] := \{\{3, 5\}, \{5, 12\}\} \cdot \{\{8, 18\}, \{5, 2\}\}
\]

\[
\text{Out}[13] := \{\{49, 64\}, \{100, 114\}\}
\]

\[
\text{In}[14] := \text{MatrixForm}[[\{\{3, 5\}, \{5, 12\}\} \cdot \{\{8, 18\}, \{5, 2\}\}]]
\]

\[
\text{Out}[14]/\text{MatrixForm} = \\
\begin{pmatrix}
49 & 64 \\
100 & 114
\end{pmatrix}
\]

Multiplication of column matrix by square matrix:

\[
\text{In}[15] := \{\{3, 7\}, \{5, 12\}\} \cdot \{\{8\}, \{5\}\}
\]

\[
\text{Out}[15] := \{\{59\}, \{100\}\}
\]
Hill's Cipher

What is usually referred to as the Hill cipher is only one of the methods that Hill discusses in his 1929 and 1931 papers, and even then it is a weakened version. We will comment more about this later, but first we will consider what is usually called the Hill cipher.

The Hill cipher uses matrices to transform blocks of plaintext letters into blocks of ciphertext. Here is an example that encrypts digraphs.

Consider the following message:

Herbert Yardley wrote The American Black Chamber.

Break the message into digraphs:

he rb er ty ar dl ey wr ot et he am er ic an bl ac kc
ha mb er

(If the message did not consist of an even number of letters, we would place a null at the end.)

Now convert each pair of letters to its number-pair equivalent. We will use our usual $a = 01, \ldots, z = 26$.

```
8 5   18 2   5 18   20 25   1 18   4 12   5 25   23 18   15 20   5 20   8 5
1 13   5 18   9 3   1 14   2 12   1 3   11 3   8 1   13 2   5 18
```

Now we encrypt each pair using the key which is the matrix $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$.

Make the first pair of numbers into a column vector $(h\ (8) \in (5))$, and multiply that matrix by the key.

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} = \begin{bmatrix} 59 \\ 100 \end{bmatrix}$$

Of course, we need our result to be mod 26
The ciphertext is $G(7) \lor (22)$.

For the next pair $r(18) \lor (2)$,

$$\begin{bmatrix} 59 \\ 100 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 22 \end{bmatrix} \mod 26$$

and 16 corresponds to $P$ and 10 corresponds to $J$. Etc.

Do this for every pair and obtain

GVPJKGAGYJMRRHMMCCYEGVPEKGVCWQLXXOBMEZAKKG

Encryption is like using a multiplicative cipher except that multiplying by a matrix allows us to encrypt more than one letter at a time.
Using Mathematica to do the matrix multiplications:

\[
\text{In}[20]:= \text{Mod}[[\{3, 7\}, \{5, 12\}] . [[8], \{5\}], 26]
\]
\[
\text{Out}[20]= \{\{7\}, \{22\}\}
\]

\[
\text{In}[21]:= \text{MatrixForm}[\text{Mod}[[\{3, 7\}, \{5, 12\}] . [[8], \{5\}], 26]]
\]
\[
\text{Out}[21]/\text{MatrixForm}=
\begin{pmatrix}
7 \\
22
\end{pmatrix}
\]

\[
\text{In}[24]:= \text{MatrixForm}[\text{Mod}[[\{3, 7\}, \{5, 12\}] . [[18], \{2\}], 26]]
\]
\[
\text{Out}[24]/\text{MatrixForm}=
\begin{pmatrix}
16 \\
10
\end{pmatrix}
\]
Decryption

Of course, we need a procedure for decrypting this. However, just like for the multiplicative ciphers, we cannot use all matrices as keys because we cannot undo the multiplication for all matrices.

To go from plaintext to ciphertext in the first example above we did

\[
\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 22 \end{bmatrix} \mod 26
\]

Now we want to undo this; we want to find a matrix so that

\[
\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \mod 26
\]

i.e, we want to find a matrix \( \begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \) so that

\[
\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \mod 26
\]

We want \( \begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \) to leave \( \begin{bmatrix} 8 \\ 5 \end{bmatrix} \) unchanged. Just like for multiplicative ciphers, we need the inverse of the key.
Matrix Inverse

We are looking for the inverse of $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$. It is denoted $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}^{-1}$.

It is easy to verify that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{b}{ad-bc} \\ -\frac{c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$.

The product $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ ad-bc & ad-bc \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is called the identity matrix because the effect of multiplying a matrix by it is to leave the other matrix unchanged. (It is like multiplying a number by 1.)

Notice that to calculate the inverse of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ we must be able to divide by $ad-bc$; i.e., we must have a multiplicative inverse for $ad-bc$. Because we are working modulo 26, that means that $ad-bc$ must be one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25. Otherwise, the multiplication cannot be undone; encryption cannot be undone.
Determinant

$ad - bc$ is called the **determinant** of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Notice that the determinant of a $2 \times 2$ matrix is just the product down the upper left to lower right diagonal minus the product down the upper right to lower left diagonal.

**For a matrix to have an inverse modulo 26, the determinant of the matrix must be 1, 3, 5, 7, 9, 11, 17, 19, 21, 23, or 25 modulo 26.**

Therefore, a matrix can be a key for a Hill cipher, only if the determinant of the matrix is one of 1, 3, 5, 7, 9, 11, 17, 19, 21, 23, or 25 modulo 26.

The determinant of $\begin{pmatrix} 3 & 7 \\ 5 & 12 \end{pmatrix}$ is $3 \times 12 - 7 \times 5 = 1 \equiv 1 \mod 26$; therefore, $\begin{pmatrix} 3 & 7 \\ 5 & 12 \end{pmatrix}$ is a valid Hill cipher key, and the key inverse is $\begin{pmatrix} 3 & 7 \\ 5 & 12 \end{pmatrix}$.

$$\begin{pmatrix} 3 & 7 \\ 5 & 12 \end{pmatrix}^{-1} = \begin{pmatrix} 12 & -7 \\ -5 & 3 \end{pmatrix} \equiv \begin{pmatrix} 12 & 19 \\ 21 & 3 \end{pmatrix} \mod 26.$$  
This is a special case because the determinant is 1.

Here is an example of finding the inverse of a $2 \times 2$ matrix when the determinant is not 1.

The determinant of $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ is $9 \times 7 - 4 \times 5 = 63 - 20 = 43 \equiv 17 \mod 26$.

Mathematica calculation of determinant modulo 26:

\begin{verbatim}
In[26]:= Det[\{\{9, 4\}, \{5, 7\}\}, Modulus \to 26]
Out[26]= 17
\end{verbatim}
Because 17 has a multiplicative inverse modulo 26, this matrix has an inverse. The inverse of the matrix is

$$\begin{bmatrix} 7 & -4 \\ 17^2 & 17 \\ -5 & 9 \\ 17 & 17 \end{bmatrix} \mod 26.$$ 

Dividing by 17 modulo 26 is the same as multiplying by the multiplicative inverse of 17 modulo 26. Recall that the multiplicative inverse of 17 is 23 modulo 26.

<table>
<thead>
<tr>
<th>Number</th>
<th>1 3 5 7 9 11 15 17 19 21 23 25</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplicative inverse</td>
<td>1 9 21 15 3 19 7 23 11 5 17 25</td>
</tr>
</tbody>
</table>

So, the inverse of the matrix is

$$\begin{bmatrix} 7 & -4 \\ 17 & 17 \\ -5 & 9 \\ 17 & 17 \end{bmatrix} \mod 26 \equiv \begin{bmatrix} 7 \times 23 & -4 \times 23 \\ -5 \times 23 & 9 \times 23 \end{bmatrix} \mod 26 \equiv \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} \mod 26 \equiv \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \mod 26$$

Mathematica calculation of inverse modulo 26:

```
In[29]:= Inverse[{{9, 4}, {5, 7}}, Modulus -> 26]
Out[29]= {{5, 12}, {15, 25}}
```
Calculating the determinant of an \( n \times n \) matrix with \( n > 2 \) is more difficult. The pattern used for a \( 2 \times 2 \) matrix is a very special case. Similarly, calculating the inverse of an \( n \times n \) matrix with \( n > 2 \) differs from calculating the inverse of a \( 2 \times 2 \) matrix. Of course, the Mathematica commands do not change.

Decryption

We return to the earlier example. Encrypting

\[
\text{Herbert Yardley wrote The American Black Chamber.}
\]

using the key

\[
\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}
\]

resulted in the ciphertext

\[
\text{GVPJKGAJYMRHMMSCCYEGVPEKGVQWLXXOBMEZAKKG}
\]

We use the inverse of the key

\[
\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}
\]

to decrypt GV, which is the first digraph of the ciphertext.

\( G \) corresponds to 7, and \( V \) corresponds to 22.

\[
\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \mod 26
\]

\( h(8) = 5 \).

In a similar manner, we can decrypt the remainder of the ciphertext.
Size of the Keypspace

Multiplicative ciphers have a very small keyspace; the key must be one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. How large is the keyspace for a Hill cipher?

There are $26^4 = 456976$ $2 \times 2$ matrices having entries modulo 26; i.e., each entry must be 0, 1, ..., 25. But, recall that for a matrix to be usable as a key for a Hill cipher the matrix must have an inverse. How many of these $2 \times 2$ matrices are invertible? This is answered for $n \times n$ matrices in “On the Keypspace of the Hill Cipher” by Overby, Traves, and Wojdylo in Cryptologia, January 2005; there are 157248 possible $2 \times 2$ keys.

So the probability that a random $2 \times 2$ matrix is invertible is 0.344.

Key generation

The fact that a little more than one-third of the $2 \times 2$ matrices are invertible suggests that a reasonable way to generate a key is to generate a random $2 \times 2$ matrix and check whether the determinant is invertible. It should not take many tries before a usable key is obtained.

Here is an example during which a valid key was obtained on the first try.

\begin{verbatim}
RandomInteger[{1, 26}, {2,2}]
\end{verbatim}

\begin{verbatim}
{{8,3},{23,22}}
\end{verbatim}

\begin{verbatim}
Det[%, Modulus -> 26]
\end{verbatim}

\begin{verbatim}
3
\end{verbatim}

Hill ciphers have two keys – an encryption key and a decryption key – (although each can be determined from the other). Anyone who knows some elementary linear algebra can construct the key inverse from the key. Except in certain cases the encryption and decryption keys are not the same. Hill, in his second paper, discusses using involutory matrices (matrices that are self-inverse; i.e., the encryption and the decryption key at the same matrix) as keys. For example,
\[
\begin{bmatrix}
0 & 1 & 25 \\
4 & 22 & 4 \\
3 & 22 & 4
\end{bmatrix}
\] is an involutory matrix.

Using involutory keys would make key generation easier, but it would significantly restrict the size of the key space. (See the previously cited article in *Cryptologia*.)

Random Keys

Ideally we would generate a new random key for the encryption of each message; however, then how keys would be exchanged prior to every message becomes a problem.