Fall 2006
Chris Christensen
MAT/CSC 483

# The Hill cipher

The Playfair cipher is a polygraphic cipher; it enciphers more than one letter at a time. Recall that the Playfair cipher enciphers digraphs – two-letter blocks. An attack by frequency analysis would involve analyzing the frequencies of the $26 \times 26 = 676$ digraphs of plaintext. Complications also occur when digraph frequencies are considered because sometimes common plaintext digraphs are split between blocks. For example, when encrypting the phrase *another type* the digraphs are *an ot he rt yp e_*, and the common digraph *th* is split between blocks.

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

Systems that enciphered even larger blocks would make cryptanalysis even more difficult. There are $26 \times 26 \times 26 \times 26 = 456976$ blocks of length 4,
$26 \times 26 \times 26 \times 26 \times 26 = 11881376$ blocks of length 5,
$26 \times 26 \times 26 \times 26 \times 26 \times 26 = 308915776$ blocks of length 6 … .

If we had a cryptosystem that encipher blocks of length 100, there would be

3142930641582938830174357788501626427282669988762475256374173
1753989959842010402346543259906970228933096407508161171919783
5869803511992549376

plaintext blocks.

But, there is no 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-trigrapphic 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 a cryptosystem that enciphers blocks. Any block size may be selected, but it might be difficult to find good keys for enciphering large blocks.

# Block Ciphers

In [most of the ciphers that we have studied], changing one letter in the plaintext changes exactly one letter in the ciphertext. In the [Caesar], affine, and substitution ciphers, a given letter in the ciphertext always comes from exactly one letter in the plaintext. In the Vigenère system, the use of blocks of letters corresponding to the length of the key, made the frequency analysis more difficult, but still possible since there was not interaction among the various letters in each block. Block ciphers avoid these problems by encrypting blocks of several letters or numbers simultaneously. A change of one character in a plaintext block should change potentially all the characters in the corresponding ciphertext block.

The Playfair cipher … is a simple example of a block cipher, since it takes two-letter blocks and encrypts them to two-letter blocks. A change of one letter of a plaintext pair will always change at least one letter, and usually both letters of the ciphertext pair. However, blocks of two letters are too small to be secure, and frequency analysis, for example, is usually successful.

The standard way of using a block cipher is to convert blocks of plaintext to blocks of ciphertext, independently and one at a time. This is called electronic code book (ECB) mode. However, there are ways to use feedback from the blocks of ciphertext in the encryption of subsequent blocks of plaintext. This leads to the cipher block chaining (CBC) mode and cipher feedback (CFB) [and other modes] of operation. *Introduction to Cryptography and Coding Theory*, Wade Trappe and Lawrence C. Washington.

## Matrices

The Hill cipher is usually taught by means of matrices.

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

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

are all matrices.

The dimension of a matrix is given as

*number of rows* × *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 as a single number 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).

$$ax + by = u$$
$$cx + dy = v$$

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

$$\textit{square matrix} \times \textit{column matrix}$$

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

$$\begin{aligned} 3\times 8 &+ 7\times 5 &&= 59 \\ 5\times 8 &+ 12\times 5 &&= 100 \end{aligned}$$

and $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 18 \\ 2 \end{bmatrix} = \begin{bmatrix} 68 \\ 114 \end{bmatrix}$

$$\begin{aligned} 3\times 18 &+ 7\times 2 &&= 68 \\ 5\times 18 &+ 12\times 2 &&= 114 \end{aligned}$$

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

$$\begin{aligned} 1\times 5 &+ 0\times -3 &+ 7\times 12 &= 89 \\ -3\times 5 &+ 4\times -3 &+ 9\times 12 &= 81 \\ 12\times 5 &+ -7\times -3 &+ 5\times 12 &= 141 \end{aligned}$$

Etc.

To multiply two square matrices of the same dimension, we just do the multiplication one column at a time.

For example, $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 8 & 18 \\ 5 & 2 \end{bmatrix} = \begin{bmatrix} 59 & 68 \\ 100 & 114 \end{bmatrix}$.

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

# Hill's Cipher

The situation with regard to the Hill cipher is much the same as that with regard to the Vigenère cipher. What is usually referred to as the Hill cipher is only one of the methods that Hill discusses, 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`, …, `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) `e` (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

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

The ciphertext is `G` (7) `V` (22).

For the next pair `r` (18) `b` (2),

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 18 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 16 \\ 10 \end{bmatrix} \bmod 26,$$

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

Do this for every pair and obtain

`GVPJKGAJYMRHHMMSCCYEGVPEKGVCWQLXXOBMEZAKKG`

Encryption is like using a multiplicative cipher except that multiplying by a matrix allows us to encipher more than one letter at a time.

## 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

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 7 \\ 22 \end{bmatrix} \bmod 26$$

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

$$\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \bmod 26$$

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

$$\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix}\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \bmod 26$$

We want $\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix}\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ to leave $\begin{bmatrix} 8 \\ 5 \end{bmatrix}$ unchanged.

## Matrix Inverse

The matrix we are looking for is called the inverse of $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ and 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 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 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 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Notice that the determinant of a $2\times 2$ 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, 15, 17, 19, 21, 23, or 25 modulo 26. To be able to undo multiplication by a matrix mod 26, the determinant of the matrix must be 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25 modulo 26. For a matrix to be a key for a Hill cipher, the determinant of the matrix must be 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25 modulo 26.

The determinant of $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ is $3\times 12 - 7\times 5 = 1 \equiv 1 \bmod 26$. So, the inverse of $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ is $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}^{-1} = \begin{bmatrix} 12 & -7 \\ -5 & 3 \end{bmatrix} \equiv \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \bmod 26$. 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 $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ is $9\times 7 - 4\times 5 = 63 - 20 = 43 \equiv 17 \bmod 26$.
Because 17 has a multiplicative inverse modulo 26, this matrix has an inverse. The inverse of the matrix is

$$\begin{bmatrix} \frac{7}{17} & \frac{-4}{17} \\ \frac{-5}{17} & \frac{9}{17} \end{bmatrix} \bmod 26.$$

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. So, the inverse of the matrix is

$$\begin{bmatrix} \frac{7}{17} & \frac{-4}{17} \\ \frac{-5}{17} & \frac{9}{17} \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 7\times 23 & -4\times 23 \\ -5\times 23 & 9\times 23 \end{bmatrix} \bmod 26$$

$$\equiv \begin{bmatrix} 161 & -92 \\ -115 & 207 \end{bmatrix} \bmod 26 \equiv \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26$$

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. Usually calculators and computer algebra systems are able to calculate determinants.

Similarly, calculating the inverse of an $n\times n$ matrix with $n > 2$ differs from calculating the inverse of a $2\times 2$ matrix. Again, usually calculators and computer algebra systems are able to calculate inverses.

## Decryption

We return to the earlier example. Encrypting

```
Herbert Yardley wrote The American Black Chamber.
```

using the key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ resulted in the ciphertext

```
GVPJKGAJYMRHHMMSCCYEGVPEKGVCWQLXXOBMEZAKKG
```

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` orresponds to 7, and v corresponds to 22.

$$\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \begin{bmatrix} 7 \\ 22 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 5 \end{bmatrix} \bmod 26$$

`h` (8) `e` (5).

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

## Hill ciphers that encipher larger blocks

Notice that the multiplicative cipher is just the $1\times1$ case of the Hill cipher; individual letters are enciphered one at a time.

$2\times2$ invertible matrices modulo 26 (an invertible matrix is a matrix that has an inverse) can be used to encipher digraphs. $3\times3$ invertible matrices modulo 26 can be used to encipher trigaphs. $4\times4$ invertible matrices modulo 26 can be used to encipher blocks of 4 letters. Etc.

Finding keys is pretty much a trial and error process. That means that it can be very difficult to find a key for encrypting large blocks.

## Ciphertext Attack

Here is a ciphertext that is known to be enciphered with a Hill cipher.

```
wbvec itxwb mphsr hytyw gmqdq egxyf yncta zdkyi eenin zkygh
yntgb pbpkl azfgy ikkru drzcp aaaci fueqg ywbuu urozm vfgmy
vkwwo zbpyn ezsbg jfynz yvmeo zctiu ghfgu aekds ayicc tkrus
xgbpz cufve lvsjg lklls vefyt onmdk
```

The first thing to be determined would be the size of the blocks. If the key were an $n\times n$ matrix, then $n$ must divide the number of letters in the ciphertext. This ciphertext has 180 letters. There are many possibilities for $n$, but let us assume that it was encrypted using a $2\times2$ key. (That's a really good assumption.)

Because such a key encrypts digraphs, we might begin by looking at digraph frequencies.

Here are the digraphs that appear more than once and their frequencies:

| Digraph | Frequency |
|---|---|
| bp | 4 |
| yn | 4 |
| ct | 3 |
| fg | 3 |
| fy | 3 |
| oz | 3 |
| ve | 3 |
| wb | 3 |
| yi | 3 |
| zc | 3 |
| aa | 2 |
| az | 2 |
| ci | 2 |
| dk | 2 |
| gb | 2 |
| gh | 2 |
| gm | 2 |
| gy | 2 |
| hy | 2 |
| kl | 2 |
| kr | 2 |
| ky | 2 |
| nz | 2 |
| ru | 2 |
| uu | 2 |
| yt | 2 |
| yv | 2 |
| yw | 2 |

If we're lucky the most common plaintext digraph `th` will correspond to (one of) the most common ciphertext digraph(s). `BP` and `YN` each appear 4 times in the ciphertext. Let's assume that ciphertext `BP` corresponds to plaintext `th`. (Another really good assumption.)

We could try to determine the key or the key inverse. Because we are trying to determine the plaintext, let's try to directly determine the key inverse. We want to find a $2\times 2$ matrix $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ that is the inverse of the key. If we are correct that `B(2)P(16)` corresponds to `t(20)h(8)`, then

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 2 \\ 16 \end{bmatrix}=\begin{bmatrix} 20 \\ 8 \end{bmatrix}$$

This corresponds to two linear equations:

$$\begin{aligned} 2e &+ 16f &&= 20 \\ 2g &+ 16h &&= 8 \end{aligned}$$

Because this Hill cipher (we assume) encrypts digraphs, the key inverse is a $2\times 2$ matrix. The key inverse has $2^2 = 4$ entries *e*, *f*, *g*, and *h* that must be determined. We would like to have four equations – two involving *e* and *f* and two involving *g* and *h*.

If we knew another plaintext/ciphertext digraph correspondence, we would have the other two equations that we need. Perhaps, the next most common ciphertext digraph `YN` corresponds to the next most common plaintext digraph `he`. (But, it doesn't.)

We could try assuming that `YN` corresponds to another common digraph, but here is another technique.

The most common letter that follows plaintext `th` is `e`. We might examine the digraphs that follow `BP` in the ciphertext and assume that the next ciphertext digraph corresponds to plaintext `e_`. We notice that we have `BP KL`, `BP BP`, `BP YN`, and `BP ZC`. If we are correct that `BP` corresponds to `th`, the second pair of digraphs corresponds to plaintext `th th`. In each of the other cases, we will assume that the two ciphertext digraphs correspond to `th e_`. Making this assumption, we should be correct more than half the time.

So, if `KL` corresponds to `e_`, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 11 \\ 12 \end{bmatrix} = \begin{bmatrix} 5 \\ * \end{bmatrix}$ which yields the equation $11e + 12f = 5$. If `YN` corresponds to `e_`, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 25 \\ 14 \end{bmatrix} = \begin{bmatrix} 5 \\ * \end{bmatrix}$ which yields the equation $25e + 14f = 5$. If `ZC` corresponds to `e_`, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 26 \\ 3 \end{bmatrix} = \begin{bmatrix} 5 \\ * \end{bmatrix}$ which yields the equation $26e + 3f = 5$.

Each of these can be solved simultaneously with, $12e + 16f = 20$ which was obtained by assuming that `BP` corresponds to `th`. All of the solving,

however, is to be done modulo 26. We may use whatever techniques we know for solving systems of linear equations provided that we divide only when division is possible – we can divide by only 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25. We will use *Mathematica* to solve the equations.

```
Solve[23 e + 2 f == 9 && 22 e + 5 f == 13 && Modulus == 26,
 {e, f}]
{{Modulus → 26, e → 1, f → 19}}
Solve[23 g + 2 h == 14 && 22 g + 5 h == 1 && Modulus == 26,
 {g, h}]
{{Modulus → 26, g → 20, h → 11}}
Solve[2 e + 16 f == 20 && 11 e + 12 f == 5 && Modulus == 26,
 {e, f}]
Solve::svars : Equations may not
   give solutions for all "solve" variables.
{{Modulus → 26, e → 1, f → 6}, {Modulus → 26, e → 1, f → 19}}
Solve[2 e + 16 f == 20 && 25 e + 14 f == 5 && Modulus == 26,
 {e, f}]
Solve::svars : Equations may not
   give solutions for all "solve" variables.
{{Modulus → 26, e → 1, f → 6}, {Modulus → 26, e → 1, f → 19}}
Solve[2 e + 16 f == 20 && 26 e + 3 f == 5 && Modulus == 26,
 {e, f}]
Solve::svars : Equations may not
   give solutions for all "solve" variables.
{{Modulus → 26, e → 1, f → 19}, {Modulus → 26, e → 14, f → 19}}
```

Each system of congruences has two solutions modulo 26. $e = 1$ and $f = 19$ is common to all of the pairs of solutions. That would happen if in each of these three cases `th` were followed by `e_`. Let us assume that is the case. (That's another really good assumption.) We could later try the other possibilities if needed.

So, we believe that the key inverse is $\begin{bmatrix} 1 & 19 \\ g & h \end{bmatrix}$.

We have one more congruence: $2g+16h=8 \bmod 26$. It is possible to solve a congruence of the form $ax+by=c \bmod n$ provided that the greatest common divisor of $a$, $b$, and $n$ also divides $c$. In our case, the greatest common divisor of $a$=2, $b$=16, and $n$=26 is 2 which does divide $c$=8. It is necessary to reduce the modulus; remove the factor of 2 to get $g+8h=4 \bmod 13$. Then rearrange the terms to get $g=4-8h \bmod 13$. Modulo 13, the possible values of $h$ are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12. We substitute these values for $h$ one at a time and solve for $g$. It's easy, but again we show *Mathematica* output.

```
Solve[g == 4 - 8*0 && Modulus == 13, g]
{{Modulus → 13, g → 4}}
Solve[g == 4 - 8*1 && Modulus == 13, g]
{{Modulus → 13, g → 9}}
Solve[g == 4 - 8*2 && Modulus == 13, g]
{{Modulus → 13, g → 1}}
Solve[g == 4 - 8*3 && Modulus == 13, g]
{{Modulus → 13, g → 6}}
Solve[g == 4 - 8*4 && Modulus == 13, g]
{{Modulus → 13, g → 11}}
Solve[g == 4 - 8*5 && Modulus == 13, g]
{{Modulus → 13, g → 3}}
Solve[g == 4 - 8*6 && Modulus == 13, g]
{{Modulus → 13, g → 8}}
Solve[g == 4 - 8*7 && Modulus == 13, g]
{{Modulus → 13, g → 0}}
Solve[g == 4 - 8*8 && Modulus == 13, g]
{{Modulus → 13, g → 5}}
Solve[g == 4 - 8*9 && Modulus == 13, g]
{{Modulus → 13, g → 10}}
Solve[g == 4 - 8*10 && Modulus == 13, g]
{{Modulus → 13, g → 2}}
Solve[g == 4 - 8*11 && Modulus == 13, g]
{{Modulus → 13, g → 7}}
Solve[g == 4 - 8*12 && Modulus == 13, g]
{{Modulus → 13, g → 12}}
```

For example, if $h = 3$, $g = 6 \bmod 13$. But, we are ultimately interested in what happens modulo 26. 6 and 6 + 13 = 19 are congruent mod 13, but they are not congruent mod 26. So, each solution mod 13 becomes two solutions mod 26.

| $h$ | $g$ mod 13 | $g$ mod 26 |
|---|---|---|
| 0 | 4 | 4, 17 |
| 1 | 9 | 9, 22 |
| 2 | 1 | 1, 10 |
| 3 | 6 | 6, 19 |
| 4 | 11 | 11, 24 |
| 5 | 3 | 3, 22 |
| 6 | 8 | 8, 21 |
| 7 | 0 | 0, 13 |
| 8 | 5 | 5, 18 |
| 9 | 10 | 10, 23 |
| 10 | 2 | 2, 15 |
| 11 | 7 | 7, 20 |
| 12 | 12 | 12, 25 |

The determinant of the key inverse must be one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25 mod 26. So, try each of these pairs of $g$ and $h$ in $\begin{bmatrix} 1 & 19 \\ g & h \end{bmatrix}$ and calculate the determinant mod 26. Again, we use *Mathematica*.

```
Mod[Det[{{1, 19}, {0, 4}}], 26]
4
Mod[Det[{{1, 19}, {0, 17}}], 26]
17
Mod[Det[{{1, 19}, {1, 9}}], 26]
16
Mod[Det[{{1, 19}, {1, 22}}], 26]
3
Mod[Det[{{1, 19}, {2, 1}}], 26]
15
Mod[Det[{{1, 19}, {2, 10}}], 26]
24
Mod[Det[{{1, 19}, {3, 6}}], 26]
1
```

```
Mod[Det[{{1, 19}, {3, 19}}], 26]
14
Mod[Det[{{1, 19}, {4, 11}}], 26]
13
Mod[Det[{{1, 19}, {4, 24}}], 26]
0
Mod[Det[{{1, 19}, {5, 3}}], 26]
12
Mod[Det[{{1, 19}, {5, 22}}], 26]
5
Mod[Det[{{1, 19}, {6, 8}}], 26]
24
Mod[Det[{{1, 19}, {6, 21}}], 26]
11
Mod[Det[{{1, 19}, {7, 0}}], 26]
23
Mod[Det[{{1, 19}, {7, 13}}], 26]
10
Mod[Det[{{1, 19}, {8, 5}}], 26]
9
Mod[Det[{{1, 19}, {8, 18}}], 26]
22
Mod[Det[{{1, 19}, {9, 10}}], 26]
21
Mod[Det[{{1, 19}, {9, 23}}], 26]
8
Mod[Det[{{1, 19}, {10, 2}}], 26]
20
Mod[Det[{{1, 19}, {10, 15}}], 26]
7
Mod[Det[{{1, 19}, {11, 7}}], 26]
6
Mod[Det[{{1, 19}, {11, 20}}], 26]
19
Mod[Det[{{1, 19}, {12, 12}}], 26]
18
Mod[Det[{{1, 19}, {12, 25}}], 26]
5
```

The possible key inverses are $\begin{bmatrix} 1 & 19 \\ 17 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 22 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 1 & 2 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 6 & 3 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 3 & 5 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 22 & 5 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 21 & 6 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 0 & 7 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 5 & 8 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 10 & 9 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 15 & 10 \end{bmatrix}$, $\begin{bmatrix} 1 & 19 \\ 20 & 11 \end{bmatrix}$, and $\begin{bmatrix} 1 & 19 \\ 25 & 12 \end{bmatrix}$.

We have reduced the problem to checking 13 possible key inverses. We try to decrypt the ciphertext with each possible inverse. $\begin{bmatrix} 1 & 19 \\ 20 & 11 \end{bmatrix}$ is the correct key inverse.

## Known plaintext attack

The cryptanalysis that was done above is a **ciphertext only attack** – only ciphertext was known. It can be difficult to cryptanalyze a Hill cipher using a ciphertext only attack, but it is easy to break using a **known plaintext attack**. A known plaintext attack means that we know a bit of ciphertext and the corresponding plaintext – a crib. This is not an unusual situation. Often messages have stereotypical beginnings (e.g., *to …*, *dear …*) or stereotypical endings (e.g, *stop*) or sometimes it is possible (knowing the sender and receiver or knowing what is likely to be the content of the message) to guess a portion of a message.

For a $2 \times 2$ Hill cipher, if we know two ciphertext digraphs and the corresponding plaintext digraphs, we can easily determine the key or the key inverse. Assume that we know that the plaintext of our ciphertext message that begins `WBVE` is `inma`. Because `WB` corresponds to `in` $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 23 \\ 2 \end{bmatrix} = \begin{bmatrix} 9 \\ 14 \end{bmatrix}$, and because `VE` corresponds to `ma` $\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 22 \\ 5 \end{bmatrix} = \begin{bmatrix} 13 \\ 1 \end{bmatrix}$. This results in two sets of linear congruences modulo 26:

$$\begin{aligned} 23e + 2f &= 9 \\ 22e + 5f &= 13 \end{aligned}$$

and

$$\begin{aligned} 23g &+ 2h = 14 \\ 22g &+ 5h = 1 \end{aligned}$$

We solve the systems modulo 26 using *Mathematica*.

```
Solve[23 e + 2 f == 9 && 22 e + 5 f == 13 && Modulus == 26,
 {e, f}]
{{Modulus → 26, e → 1, f → 19}}
Solve[23 g + 2 h == 14 && 22 g + 5 h == 1 && Modulus == 26,
 {g, h}]
{{Modulus → 26, g → 20, h → 11}}
```

Again (with a lot less assuming) we find that the key inverse is $\begin{bmatrix} 1 & 19 \\ 20 & 11 \end{bmatrix}$.

## Two More Examples of a Known Plaintext Attack

Here are two examples of cryptanalyzing a Hill cipher with a known plaintext attack. Each example is done by hand – without using *Mathematica*. In example one, there is no need to reduce the modulus; in example two the modulus must be reduced.

**Example one:**

Ciphertext: `FAGQQ ILABQ VLJCY QULAU STYTO JSDJJ PODFS ZNLUH KMOW`

We are assuming that this message was encrypted using a $2 \times 2$ Hill cipher and that we have a crib. We believe that the message begins "`a crib.`"

| ac | ri |
|---|---|
| [1, 3] | [18, 9] |
| [6, 1] | [7, 17] |
| FA | GQ |

We could either solve for the key or the key inverse. To solve for the key, we would solve

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix}=\begin{bmatrix} 6 \\ 1 \end{bmatrix}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 18 \\ 9 \end{bmatrix}=\begin{bmatrix} 7 \\ 17 \end{bmatrix}$$

To solve for the key inverse, we would solve

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 6 \\ 1 \end{bmatrix}=\begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

and

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} 7 \\ 17 \end{bmatrix}=\begin{bmatrix} 18 \\ 9 \end{bmatrix}$$

We will solve for the key.

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 \\ 3 \end{bmatrix}=\begin{bmatrix} 6 \\ 1 \end{bmatrix}$ represents two linear equations:

$$\begin{aligned} a \quad +3b \quad &= \quad 6 \\ c \quad +3d \quad &= \quad 1 \end{aligned}$$

and $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 18 \\ 9 \end{bmatrix}=\begin{bmatrix} 7 \\ 17 \end{bmatrix}$ represents

$$\begin{aligned} 18a \quad +9b \quad &= \quad 7 \\ 18c \quad +9d \quad &= \quad 17 \end{aligned}$$

Now we solve the following linear congruences mod 26.

$$\begin{cases} a & +3b & = & 6 \\ 18a & +9b & = & 7 \end{cases} \text{ and } \begin{cases} c & +3d & = & 1 \\ 18c & +9d & = & 17 \end{cases}$$

We will solve the pair of congruences $\begin{cases} a & +3b & = & 6 \\ 18a & +9b & = & 7 \end{cases}$ first.

To eliminate an unknown, multiply congruence 1 by 3

$$\begin{cases} 3a & +9b & = & 18 \\ 18a & +9b & = & 7 \end{cases}$$

and subtract congruence 2 from congruence 1.

$$-15a \quad = \quad 11$$

Modulo 26, -15 is 11.

$$11a \quad = \quad 11$$

Divide by 11 to obtain $a$.

$$a = 1$$

Now substitute this in congruence 1.

$$1 + 3b = 6$$

$$3b = 5$$

The multiplicative inverse of 3 is 9 modulo 26.

$$b = 9 \times 3b = 9 \times 5 = 45 = 19 \bmod 26$$

So, the key looks like

$$\begin{bmatrix} 1 & 19 \\ c & d \end{bmatrix}$$

Now solve the system $\begin{cases} c & +3d & = & 1 \\ 18c & +9d & = & 17 \end{cases}$

$$\begin{cases} 3c & +9d & = & 3 \\ 18c & +9d & = & 17 \end{cases}$$

$$15c = 14$$

$$c = 7 \times 15c = 7 \times 14 = 98 = 20 \bmod 26$$

$$20 + 3d = 1$$

$$3d = -19 = 7 \bmod 26$$

$$d = 9 \times 3d = 9 \times 7 = 63 = 11 \bmod 26$$

The key is $\begin{bmatrix} 1 & 19 \\ 20 & 11 \end{bmatrix}$.

**Example two:**

We are assuming that we have a ciphertext message was that encrypted using a $2 \times 2$ Hill cipher and that we have a crib. We believe that ciphertext `UKJN` corresponds to plaintext `word`.

| wo | rd |
|---|---|
| [23, 15] | [18, 4] |
| [21, 11] | [10, 14] |
| UK | JN |

The two systems of congruences are:

$$\begin{cases} 23a & +15b & = & 21 \\ 18a & +4b & = & 10 \end{cases} \text{ and } \begin{cases} 23c & +15d & = & 11 \\ 18c & +4d & = & 14 \end{cases}$$

We will solve the system on the left.

To eliminate an unknown, multiply congruence number 1 by 4 and congruence number 2 by 15 both modulo 26.

$$\begin{cases} 14a + 8b = 6 \\ 10a + 8b = 20 \end{cases}$$

Subtract the second congruence from the first.

$$4a = -14 = 12 \bmod 26$$

This congruence corresponds to the equation $4a = 12 + 26k$, $4a$ is 12 plus a multiple of 26. Notice that 2 divides the coefficient of $a$, the constant 12, and the modulus 26. We reduce the modulus by dividing by 2.

$$2a = 6 + 13k$$

and we have a congruence modulo 13.

$$2a = 6 \bmod 13$$

This congruence does not have a common factor among the coefficient, the constant, and the modulus.

Here are the multiplicative inverses of the integers modulo 13:

| Number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Multiplicative inverse | 1 | 7 | 9 | 10 | 8 | 11 | 2 | 5 | 3 | 4 | 6 | 12 |

To find $a$, multiply $2a = 6 \bmod 13$ by the multiplicative inverse of 2, which is 7.

$$a = 7 \times 2a = 7 \times 6 = 42 = 3 \bmod 13$$

So, $a$ is 3 modulo 13. But, there are two integers mod 26 that are 3 mod 13, namely, 3 and 3 + 13 = 16. So, there are two possible values for $a$.

If $a$ = 3,

$$18\times 3 = 4b = 10$$

$$54 + 4b = 10$$

$$2 + 4b = 10$$

$$4b = 8 \bmod 26$$

$$2b = 4 \bmod 13$$

$$b = 7\times 2b = 7\times 4 = 26 = 2 \bmod 13$$

So, $b$=2 or $b$ = 2+13 = 15 modulo 16.

If $a$ = 16,

$$18\times 16 + 4b = 10$$

$$288 + 4b = 10$$

$$2 + 4b = 10$$

which yields the same solutions for $b$.

Here are the 4 possible solutions for $a$ and $b$.

$$\begin{array}{ll} a = 3 & b = 2 \\ a = 3 & b = 15 \\ a = 16 & b = 2 \\ a = 16 & b = 15 \end{array}$$

Now solve $\begin{cases} 23c & +15d & = & 11 \\ 18c & +4d & = & 14 \end{cases}$.

$$\begin{cases} 14a & +8b & = & 18 \\ 10a & +8b & = & 2 \end{cases}$$

$$4c = 16 \bmod 26$$

$$2c = 8 \bmod 13$$

$$c = 7 \times 2c = 14c = 7 \times 8 = 56 = 4 \bmod 13$$

So, $c = 4$ or $c = 4 + 13 = 17$ modulo 26.

If $c = 4$,

$$18 \times 4 + 4d = 14$$

$$20 + 4d = 14$$

$$4d = -6 = 20 \bmod 26$$

$$2d = 10 \bmod 13$$

$$d = 7 \times 2d = 7 \times 10 = 5 \bmod 13$$

So, $d = 5$ or $d = 5 + 13 = 18$ modulo 26.

If $c = 17$,

$$18 \times 17 + 4d = 14$$

$$20 + 4d = 14$$

and we are led to the same solutions for $d$.

$$\begin{array}{ll} c = 4 & d = 5 \\ c = 4 & d = 18 \\ c = 17 & d = 5 \\ c = 17 & d = 18 \end{array}$$

There are 16 possible $2 \times 2$ matrices that could be the key.

$$\begin{bmatrix} 3 & 2 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 2 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 3 & 15 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 3 & 15 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 16 & 2 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 2 \\ 17 & 18 \end{bmatrix}$$
$$\begin{bmatrix} 16 & 15 \\ 4 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 4 & 18 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 17 & 5 \end{bmatrix} \quad \begin{bmatrix} 16 & 15 \\ 17 & 18 \end{bmatrix}$$

First, calculate the determinant of each. Any matrix that does not have an invertible determinant modulo 26 (i.e., the determinant is not one of 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 modulo 26) can be eliminated. Then try to decipher the messages with each of the remaining messages. The matrix that yields plaintext is the key.

Two more examples appear in an appendix.

To break a Hill cipher with a $2 \times 2$ key requires determining four entries – the four entries of the key or the four entries of the key inverse. We can do that if we know the correspondence between plaintext and ciphertext for two digraphs because the correspondences will permit us to set up two systems of congruences – each system has two congruences of two unknowns.

To break a Hill cipher with a $n \times n$ key requires determining $n^2$ entries – the $n^2$ entries of the key or the $n^2$ entries of the key inverse. We can do that if we know the correspondence between plaintext and ciphertext for *n* *n*-graphs because the correspondences will permit us to set up *n* systems of congruences – each system has *n* congruences of *n* unknowns.

The reason that we can solve these systems of congruences is because they are linear. The solutions of linear systems of equations of congruences is well-understood.

## Linear Transformations

What do we mean by linear?

First, there are two more operations on matrices that we will briefly consider.

Adding two matrices of the same size means to add their corresponding entries; e.g., $\begin{bmatrix} 3 & -9 \\ 5 & 2 \end{bmatrix} + \begin{bmatrix} 5 & 6 \\ -3 & 0 \end{bmatrix} = \begin{bmatrix} 8 & -3 \\ 2 & 2 \end{bmatrix}$. In particular, for a column matrix, $\begin{bmatrix} 2 \\ 9 \end{bmatrix} + \begin{bmatrix} -5 \\ 12 \end{bmatrix} = \begin{bmatrix} -3 \\ 21 \end{bmatrix}$.

Multiplying a matrix by a number means to multiply each entry of the matrix by that number; e.g., $3\begin{bmatrix} 5 & -2 \\ 7 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -6 \\ 21 & 6 \end{bmatrix}$. In particular, for a column matrix, $-4\begin{bmatrix} 5 \\ -7 \end{bmatrix} = \begin{bmatrix} -20 \\ 28 \end{bmatrix}$. This multiplication is called scalar multiplication because the entries of the matrix are scaled.

A transformation *T* is said to be a **linear transformation** if it satisfies the following two properties:

$$\begin{aligned} T(x+y) &= T(x)+T(y) \\ T(ax) &= aT(x) \end{aligned}$$

where *a* is a number.

Multiplication of a column matrix by a square matrix is seen to be a linear transformation. For example,

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\left(\begin{bmatrix} 8 \\ 5 \end{bmatrix} + \begin{bmatrix} 18 \\ 2 \end{bmatrix}\right) = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix} + \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 18 \\ 2 \end{bmatrix}$$

and

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\left(2\begin{bmatrix} 8 \\ 5 \end{bmatrix}\right) = 2\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix}.$$

Linearity also holds when the operations are done modulo 26; so, the encryption process of a Hill cipher is a linear transformation.

Mathematicians like linear transformations because mathematicians understand a great deal about linear transformations. Cryptographers do not like linear transformations because mathematicians understand a great deal about linear transformations.

Because the Hill cipher relies on matrix multiplication, which is a linear transformation, the Hill cipher can be cryptanalyzed. In fact, a known plaintext attack requires knowing only the correspondence between plaintext and ciphertext for two digraphs (between plaintext and ciphertext strings of length 4) when the key is a $2 \times 2$ matrix and requires knowing only the correspondence between plaintext and ciphertext for *n* *n*-graphs (between plaintext and ciphertext strings of length $n^2$) when the key is an $n \times n$ matrix. That amount of information determines a system of linear congruences that can be solved, and the entries of the key or of the key inverse can be determined. It might not be a pleasant process, but it can be done. (What was said above is not quite true. We are claiming that a system of *n* linear congruences in *n* unknowns has a solution. Such a system might not have a solution; it might be indeterminant. What is needed for a solution is that that system of congruences be independent – that there not be redundancy in the system. For example, when using a Hill cipher with a $2 \times 2$ key, if the plaintext-ciphertext correspondence that we knew were acac = FAFA, we would not have enough information to determine the key. If there is redundancy, usually using just "a few more" plaintext-ciphertext correspondences eliminates the redundancy.)

Consider the $2 \times 2$ Hill cipher. If we know only two correspondences between plaintext and ciphertext digraphs, we can determine the key because the encryption process is linear. Consider the Playfair cipher. If we know only two correspondences between plaintext and ciphertext digraphs, it is unlikely that we could determine the key because the Playfair cipher is non-linear.

Cryptographers should attempt to avoid linearity when constructing cryptosystems.

## Introducing Non-linearity into a Hill Cipher

Hill's papers contain techniques that are much more secure than the technique that we have called the Hill cipher. Hill's papers include ciphers that are nonlinear.

One nonlinear technique used by Hill is to do a (nonlinear) simple substitution cipher – a permutation -- prior to the matrix multiplication. Hill uses the following substitutions:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 23 | 2 | 20 | 10 | 15 | 8 | 4 | 18 | 25 | 0 | 16 | 13 | 7 | 3 | 1 | 19 | 6 | 12 | 24 | 21 | 17 | 14 | 22 | 11 | 9 |

For example, th becomes 24 4 and then

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 24 \\ 4 \end{bmatrix} = \begin{bmatrix} 22 \\ 12 \end{bmatrix}$$

V (22) L (12).

Composing nonlinear substitution and linear mixing is the basis of what are called Feistel ciphers. DES the Data Encryption Standard (which was the standard for data encryption from 1977 until the selection of AES the Advanced Encryption Standard in 2001) is a Feistel cipher.

Another nonlinear technique used by Hill is similar to what we did when we went from the multiplicative cipher ($C = mp$) to the affine cipher ($C = mp + b$) by adding a shift. Multiplicative ciphers are linear ciphers; affine ciphers are not linear ciphers. Hill adds a shift to what we have called the Hill cipher. For example, (using a = 1, …, z = 26) to encrypt h (8) e (5)

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \begin{bmatrix} 8 \\ 5 \end{bmatrix} + \begin{bmatrix} 6 \\ 20 \end{bmatrix} = \begin{bmatrix} 13 \\ 16 \end{bmatrix}$$

M (13) P (16).

Hill includes further nonlinear generalizations.

## Size of the Keyspace

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 Keyspace of the Hill Cipher" by Overby, Traves, and Wojdylo in *Cryptologia*, January 2005; there are 157248 possible $2 \times 2$ keys.

Hill ciphers are asymmetric ciphers: one key is used for encryption and a second key (the key inverse) is used for decryption. Of course, anyone who knows some elementary linear algebra can construct the key inverse from the key, but the encryption and decryption keys are not the same – except in certain cases. Hill, in his second paper, discusses using involutory matrices (matrices that are self-inverse) as keys.

$$\begin{bmatrix} 0 & 1 & 25 \\ 4 & 22 & 4 \\ 3 & 22 & 4 \end{bmatrix} \text{ is involutory.}$$

Using involutory keys would make encryption and decryption completely symmetric, but this significantly restricts the number of keys (see the previously cited article in *Cryptologia*.)

## Diffusion and Confusion

Two properties are often considered when discussing the strength of modern block ciphers.

> Claude Shannon, in one of the fundamental papers on the theoretical foundations of cryptography ["Communication theory of secrecy systems," *Bell Systems Technical Journal* 28 (1949), 656 – 715], gave

two properties that a good cryptosystem should have to hinder statistical analysis: **diffusion** and **confusion**.

Diffusion means that if we change a character of the plaintext, then several characters of the ciphertext should change, and similarly, if we change a character of the ciphertext, then several characters of the plaintext should change. We saw that the Hill cipher has this property. This means that frequency statistics of letters, [digraphs], etc. in the plaintext are diffused over several characters in the ciphertext, which means that much more ciphertext is needed to do a meaningful statistical attack.

Confusion means that the key does not related in a simple way to the ciphertext. In particular, each character of the ciphertext should depend on several parts of the key. For example, suppose we have a Hill cipher with an $n \times n$ matrix, and suppose we have a plaintext-ciphertext pair of length $n^2$ with which we are able to solve for the encryption matrix. If we change one character of the ciphertext, one column of the matrix can change completely. Of course, it would be more desirable to have the entire key change. When a situation like that happens, the cryptanalyst would probably need to solve for the entire key simultaneously, rather than piece by piece.

The Vigenère and substitution ciphers do not have the properties of diffusion and confusion, which is why they are so susceptible to frequency analysis. *Introduction to Cryptography and Coding Theory*, Wade Trappe and Lawrence C. Washington.

Keys containing lots of zero entries weaken diffusion.

## Hill ciphers with $n \times n$ keys form a group

Encrypting with a Hill cipher and re-encrypting with another key of the same size does not improve security because the Hill ciphers with $n \times n$ keys form a group.

For example, if we encrypted digraphs with a Hill cipher using the key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ (which has determinant 1 modulo 26) and then encrypted that ciphertext using a Hill cipher with key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ (which has determinant 17 modulo 26), the result would be the same as encrypting once with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} = \begin{bmatrix} 47 & 111 \\ 50 & 119 \end{bmatrix} = \begin{bmatrix} 21 & 7 \\ 24 & 15 \end{bmatrix} \mod 26$. Because "the determinant of a product is the product of the determinants" (even modulo 26), the determinant of $\begin{bmatrix} 21 & 7 \\ 24 & 15 \end{bmatrix}$ is $17 \times 1 = 17 \mod 26$; so, it is a valid Hill cipher key.

The point is, you have only one shot at using a Hill cipher – re-encrypting does not improve security.

## Public key cryptology

In 1976 a paper appeared that would revolutionize cryptology. The paper was by Whitfield Diffie and Martin Hellman. Their paper "New Directions in Cryptography" was published in the *IEEE Transactions on Information Theory* (vol. 22, no. 6, November 1976). Diffie and Hellman were concerned with the key distribution problem that would be created by increased use of communications networks like the internet (which developed later). The problem is: How do you distribute secret keys to people with whom you have not communicated before? Using classical cryptology, (essentially) the same key is used to encrypt and to decrypt messages. If you know how to encrypt, then you know how to decrypt. The

usual way to distribute secret keys was by courier. Imagine that you've never purchased from Amazon.com before, but you just found a book on their website that you'd like to order. You need to send credit card information to Amazon, but you'd like that information to be encrypted. What do you do? You don't want to have to contact Amazon and wait until they have a courier show up at your door with a secret key. Diffie and Hellman suggested a solution.

Classical cryptology uses essentially the same key for encryption and decryption. Such a key is called a **symmetric key**. Diffie and Hellman suggested that there be two keys – a public key which would be used for encryption and a private key which would be used for decryption. Communication would be a one-way process. The sender would look up the receiver's public key and use that key to encrypt the message. Upon receiving the message, the receiver would use the private key to decrypt it. The important point, of course, is that knowledge of the encryption key should yield no information about the decryption key. This is called **public key** or **asymmetric key** cryptography.

Public key cryptography solves the key distribution problem. If you want to send your credit card number to Amazon, you (actually your web browser does this) look up Amazon's public key and use that key to encrypt your credit card number. There is no need to keep the encryption key secret – everyone may know it.

But, is such a scheme possible? Is it possible to encyrpt with one key and decrypt with another and design the keys in such a way that knowing the encryption key does not provide enough information to construct the decryption key?

In their paper, Diffie and Hellman did not describe such an encryption system, but they suggested that one was needed. Various systems developed, and today they dominate much of cryptology. These public key systems seem to be characterized by having the encryption key being a rather easy calculation – but a calculation that is not possible to undo without additional information (which the receiver keeps private).

The Hill cipher suggests how such a method might work. Now, the Hill cipher is *not* a public key encryption scheme because anyone who knows the encryption matrix can, using elementary linear algebra, calculate the

decryption matrix – the key inverse. But, assume that it were not known how to calculate the inverse of a matrix. Then, the Hill cipher would be a public key encryption scheme. The receiver (usually called Bob) could construct an encryption matrix and its inverse and make public his encryption matrix. Any sender (usually called Alice) who wanted to send a message to Bob could look up Bob's encryption matrix and use it to encrypt a message to Bob. When Bob received the ciphertext he could use the inverse of the matrix (which he is keeping a secret) to decrypt the ciphertext.

Remember that this is one-way communication. If Bob wanted to reply to Alice, he would have to look up Alice's encryption matrix and use that matrix to encrypt his reply. Then Alice could use the inverse of her encryption matrix (which she is keeping a secret) to decrypt the ciphertext of Bob's reply.

This would solve the problem of key distribution because all encryption keys are public.

But, can we actually find such mathematical processes – processes that are easy to do but hard or impossible to undo without additional, secret information?

It is not surprising that multiplication/factoring was an early choice. It is easy to multiply together two integers even if the integers are very large. But, given a large integer, there is no efficient way to factor it. This is the basis of the RSA public key encryption system.

Another mathematical problem involves logarithms. Raising an integer to an exponent is relatively easy. But, given an integer and a base, it can be hard to determine the exponent -- the logarithm. This is the basis of the El Gamal public key encryption system.

Not surprisingly, the calculations for both RSA and El Gamal involve modular arithmetic.

## Was the Hill cipher ever used?

Hill's papers contributed two important ideas to cryptology. First, they freed cryptology from encrypting just single letters and digraphs – they showed that encryption of blocks of more than two letters was possible. And, Hill's papers showed the close connection between cryptology and mathematics. This connection was emphasized by A.A. Albert in an address to the American Mathematical Society in 1941.

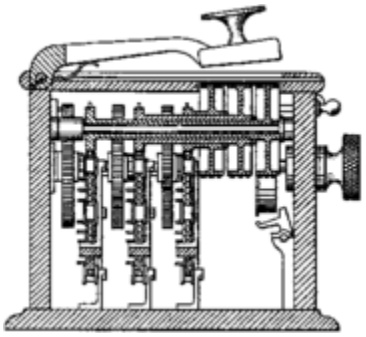
But, was the Hill cipher ever used?

Hill's cipher is a nice application of matrices, but matrix multiplication is probably not easily done by soldiers who are in the trenches and watching artillery shells flying overhead.

As a cipher to encrypt digraphs, Hill's cipher is harder to use and weaker than the Playfair cipher.

> … Hill's cipher system itself saw almost no practical use …
>
> The real obstacle to practical use of the Hill system is, of course, it ponderousness. Hill sought to minimize this by patenting a device that will encipher small polygrams (up to hexagrams). It consists of a series of geared wheels connected by a sprocketed chain so that the rotation of one wheel will turn all the others, but the range of its keys appears to be limited.
>
> … the Hill system has served as a U.S. governmental cryptosystem in only one minor capacity – to encipher the three-letter groups of radio call-signs. *The Codebreakers* by David Kahn

A view from one end of the Hill cipher machine.



http://en.wikipedia.org/wiki/Hill_cipher

The drawing on the next page is a side view of the Hill cipher machine and is taken from *The Codebreakers* by David Kahn.

Exercises

1. Multiply the following matrices, if possible.

1a. $\begin{bmatrix} 3 & 6 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} 8 \\ 5 \end{bmatrix}$.

1b. $\begin{bmatrix} 3 & 6 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} -2 \\ 3 \end{bmatrix}$.

1c. $\begin{bmatrix} 3 & 6 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} 8 & -2 \\ 5 & 3 \end{bmatrix}$.

1d. $\begin{bmatrix} 3 & 6 \\ -1 & 4 \end{bmatrix}\begin{bmatrix} -2 & 8 \\ 3 & 5 \end{bmatrix}$.

1e. $\begin{bmatrix} 3 & 5 & 13 \\ 2 & 7 & 21 \\ 9 & 4 & 1 \end{bmatrix}\begin{bmatrix} -1 \\ 3 \\ 2 \end{bmatrix}$.

1f. $\begin{bmatrix} 3 & 5 & 13 \\ 2 & 7 & 21 \\ 9 & 4 & 1 \end{bmatrix}\begin{bmatrix} 3 \\ -5 \end{bmatrix}$.

1g. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} -11 \\ 23 \end{bmatrix}$.

1h. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 12 \\ -7 \end{bmatrix}$.

1i. $5\begin{bmatrix} -1 \\ 3 \\ 2 \end{bmatrix}$.

1j. $2\begin{bmatrix} 3 & 5 & 13 \\ 2 & 7 & 21 \\ 9 & 4 & 1 \end{bmatrix}$.

1k. $\begin{bmatrix} 1 & -3 & 2 \\ 0 & 4 & 1 \\ -7 & 8 & 5 \end{bmatrix}\begin{bmatrix} 4 & 6 & -2 \\ 3 & 3 & 9 \\ 5 & -7 & 4 \end{bmatrix}$.

1l. $\begin{bmatrix} 3 & 0 & -2 & 2 \\ 4 & 6 & -1 & 1 \\ 1 & 5 & 6 & -3 \\ 9 & -7 & 4 & 0 \end{bmatrix}\begin{bmatrix} 4 \\ -1 \\ 1 \\ 3 \end{bmatrix}$.

2. Use a Hill cipher with key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ to encrypt the following message.

```
Agnes Driscoll worked for NSA.
```

3. The following message was encrypted with a Hill cipher with key $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$. Decrypt the message.

```
ZKYZR  QHBDM   JMPVX   WLCGF   MIXGM   PKBUZ
FHPCI  XZTIW
```

4. Find the determinant of each of the following matrices modulo 26.

4a. $\begin{bmatrix} 5 & 2 \\ 7 & 3 \end{bmatrix}$.

4b. $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$.

4c. $\begin{bmatrix} 20 & 2 \\ 5 & 4 \end{bmatrix}$.

4d. $\begin{bmatrix} 5 & 8 \\ 12 & 3 \end{bmatrix}$.

4e. $\begin{bmatrix} 21 & 13 \\ 7 & 16 \end{bmatrix}$

5. Which of the matrices in exercise 4 can be used as keys for a Hill cipher?

6. For each of the matrices in exercise 4 that can be used as keys for a Hill cipher, find the inverse modulo 26.

7. Use a Hill cipher with key $\begin{bmatrix} 2 & 7 & 19 \\ 0 & 5 & 8 \\ 1 & 3 & 7 \end{bmatrix}$ to encrypt the following message: `enigma`.

8. Use a Hill cipher with key $\begin{bmatrix} 5 & 6 & 4 & 1 \\ 2 & 1 & 0 & 3 \\ 1 & 8 & 9 & 2 \\ 2 & 4 & 6 & 7 \end{bmatrix}$ to encyrpt the following message: `united states`.

9. Find a $2 \times 2$ matrix that can be used as a key for a Hill cipher.

10. What is special about the Hill cipher key $\begin{bmatrix} 5 & 8 \\ 10 & 21 \end{bmatrix}$? Does this make this matrix a good or bad choice for a key?

11. A message is first encrypted with a Hill cipher with key $\begin{bmatrix} 6 & 3 \\ 7 & 8 \end{bmatrix}$ and then encrypted again with key $\begin{bmatrix} 3 & 2 \\ 8 & 5 \end{bmatrix}$. What is the resulting cipher?

12. Assume that an $n \times n$ matrix is the key for a Hill cipher. If one letter of plaintext is changed, how many letters of ciphertext are likely to change?

13. Assume that an $n \times n$ matrix is the key for a Hill cipher. How many blocks of plaintext letters would we need to cryptanalyze the ciphertext? How many total letters of plaintext is this?

14. Known plaintext attack on the Hill cipher. Find the key for the following ciphertext message that was enciphered with a Hill cipher.

```
VRAAU  OTNLK  NJWVJ  QJXXY  BEOLW  CVRYK  FOYPQ
TWVMP  ALUEA  ACWWE  GB
```

The plaintext message begins "The Riddle."

15. For the very (very) brave – a ciphertext attack on the Hill cipher.

```
TZZOK  HMOTZ  MOINY  FTWCO  UWINH  CAGZH  AZXME
ICZVH  ZOTWE  IUGGG  AETWE  ICZVH  ZOYKX  ZFAMW
PGWQQ  JTZGT  YRFAI  KTWEI  HIQTN  ZAGVM  YKXZP
GWQQJ  ZCHNE  ITZXG  IKTWE  IVUOZ  XUXBQ  DPTPS
WQZHA  ZXMEI  CZVHZ  OYKXZ  FAMWP  GWQQJ  ELTZQ
POZRF
```

16. Another ciphertext attack on the Hill cipher.

```
xrqsx ibkfy lawcc jrohm ouyyl mrqgi ucscc ahakc
zwuhg axroc bipwe zatqd eqrmh zgtmv ygoyq qlmqd
kbpyd dqqcj glhka pbkae clxru cuhbg wtetx riymt
ezdyd dhksj opgia piwzw fmzwa egpgi jpqxn oaady
```

17. You know that you are intercepting messages that are encrypted with a $2 \times 2$ Hill cipher. You are able to trick one of the parties of the communications to send the plaintext digraphs `az` and `za`. You are able to determine that `az` is enciphered as `OJ` and `za` is enciphered as `YI`. Determine the encryption matrix and the decryption matrix.

18. Consider the affine version of the Hill cipher. First encrypt a message by multiplying by the matrix $\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ and then adding to the result the matrix $\begin{bmatrix} 6 \\ 20 \end{bmatrix}$. Encrypt again by multiplying by the matrix $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and adding the matrix $\begin{bmatrix} 3 \\ 17 \end{bmatrix}$. What is the resulting cipher?

19. Again, consider the affine version of the Hill cipher. Would re-encrypting using this cryptosystem increase security?

20. Show that the affine version of the Hill cipher is not a linear transformation.

21. Would using a involutory key reduce the security of a Hill cipher?