How to Encipher and Decipher Codes Using the Hill 2-Cipher

Table of Contents

Expectations

****PLEASE READ THIS SECTION BEFORE CONTINUING****

To follow these instructions, you should be familiar with basic matrix theory and modular arithmetic. You will be expected to:

- Know common terms and definitions such as "vector" and "transpose."
- Multiply matrices.
- Find the determinant of a matrix.
- Find the residue modulo 26 of entries in a vector.
- Perform elementary row operations in a matrix.

Background

Cryptography is the study of encoding and decoding secret messages. Substitution ciphers are among one of the first types of ciphers created. These ciphers replaced each letter of the alphabet by a different letter, as shown in Table 1.0.

Table 1.0 – Sample Substitution Cipher: Each Letter Shifts Right by One

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
Z	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

For instance, the word *CODE* becomes *BNCD*.

Although this is a simple method of encryption, it has one significant flaw: the frequency of letters remains the same. For instance, the letter "e" is the most frequently used letter in the English language and makes up an average of 12.702% of all written correspondence [1]. In a substitution ciphertext, the letter or symbol that takes the place of "e" has the same frequency because it is merely a disguised representation of the letter.

To avoid decryption, cryptographers began to apply once-abstract mathematics to cryptography. One of the most successful ciphers, designed by Lester S. Hill in the late 1920s, utilizes matrices and vectors to encode messages two letters at a time [2]. This instruction manual explains how to use Hill's 2-cipher technique.

Enciphering a Message

1. **Obtain a plaintext message to encode in standard English with no punctuation.**

   In this example, we will encipher the message *DR GREER ROCKS*.

2. **Create an enciphering matrix:**

   2.1. Form a square 2x2 matrix with nonnegative integers each less than 26.

$$\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$$

   2.2. Check that its determinant does NOT factor by 2 or 13. If this is so, return to Step 2.1.

$$\det\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} = (1\times 1)-(3\times 2) = -5 \quad \checkmark$$

3. **Group the plaintext into pairs. If you have an odd number of letters, repeat the last letter.**

   D R G R E E R R O C K S

4. **Replace each letter by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3…Z=0. See Table A below for quick reference.**

Table A– Letters and Their Corresponding Positions

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

D R G R E E R R O C K S

4 18 7 18 5 5 18 18 15 3 11 19

5. Convert each pair of letters into plaintext vectors.

$$\begin{matrix} D \to \\ R \to \end{matrix}\begin{bmatrix} 4 \\ 18 \end{bmatrix} \quad \begin{matrix} G \to \\ R \to \end{matrix}\begin{bmatrix} 7 \\ 18 \end{bmatrix} \quad \begin{matrix} E \to \\ E \to \end{matrix}\begin{bmatrix} 5 \\ 5 \end{bmatrix} \quad \begin{matrix} R \to \\ R \to \end{matrix}\begin{bmatrix} 18 \\ 18 \end{bmatrix} \quad \begin{matrix} O \to \\ C \to \end{matrix}\begin{bmatrix} 15 \\ 3 \end{bmatrix} \quad \begin{matrix} K \to \\ S \to \end{matrix}\begin{bmatrix} 11 \\ 19 \end{bmatrix}$$

6. Convert the plaintext vectors into ciphertext vectors.

6.1. Mutiply the enciphering matrix by each plaintext vector.

$$\begin{matrix} D \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} 58 \\ 26 \end{bmatrix} \quad \begin{matrix} G \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 7 \\ 18 \end{bmatrix} = \begin{bmatrix} 61 \\ 32 \end{bmatrix} \quad \begin{matrix} E \to \\ E \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 20 \\ 15 \end{bmatrix}$$

$$\begin{matrix} R \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 72 \\ 54 \end{bmatrix} \quad \begin{matrix} O \to \\ C \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 3 \end{bmatrix} = \begin{bmatrix} 24 \\ 33 \end{bmatrix} \quad \begin{matrix} K \to \\ S \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} 68 \\ 41 \end{bmatrix}$$

6.2. Replace each new vector by its residue modulo 26 if possible.

$$\begin{matrix} D \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} 58 \\ 26 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix} \pmod{26}$$

$$\begin{matrix} G \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 7 \\ 18 \end{bmatrix} = \begin{bmatrix} 61 \\ 32 \end{bmatrix} = \begin{bmatrix} 9 \\ 6 \end{bmatrix} \pmod{26}$$

$$\begin{matrix} E \to \\ E \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 20 \\ 15 \end{bmatrix}$$

$$\begin{matrix} R \to \\ R \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 72 \\ 54 \end{bmatrix} = \begin{bmatrix} 20 \\ 2 \end{bmatrix} \pmod{26}$$

$$\begin{matrix} O \to \\ C \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 15 \\ 3 \end{bmatrix} = \begin{bmatrix} 24 \\ 33 \end{bmatrix} = \begin{bmatrix} 24 \\ 7 \end{bmatrix} \pmod{26}$$

$$\begin{matrix} K \to \\ S \to \end{matrix}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} 68 \\ 41 \end{bmatrix} = \begin{bmatrix} 16 \\ 15 \end{bmatrix} \pmod{26}$$

7. **Convert each entry in the ciphertext vector into its corresponding position in the alphabet.**

$$\begin{matrix} D \rightarrow \\ R \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} 58 \\ 26 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix} (\bmod 26) \begin{matrix} \rightarrow F \\ \rightarrow Z \end{matrix}$$

$$\begin{matrix} G \rightarrow \\ R \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 7 \\ 18 \end{bmatrix} = \begin{bmatrix} 61 \\ 32 \end{bmatrix} = \begin{bmatrix} 9 \\ 6 \end{bmatrix} (\bmod 26) \begin{matrix} \rightarrow I \\ \rightarrow F \end{matrix}$$

$$\begin{matrix} E \rightarrow \\ E \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 20 \\ 15 \end{bmatrix} \begin{matrix} \rightarrow T \\ \rightarrow O \end{matrix}$$

$$\begin{matrix} R \rightarrow \\ R \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 72 \\ 54 \end{bmatrix} = \begin{bmatrix} 20 \\ 2 \end{bmatrix} (\bmod 26) \begin{matrix} \rightarrow T \\ \rightarrow B \end{matrix}$$

$$\begin{matrix} O \rightarrow \\ C \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 15 \\ 3 \end{bmatrix} = \begin{bmatrix} 24 \\ 33 \end{bmatrix} = \begin{bmatrix} 24 \\ 7 \end{bmatrix} (\bmod 26) \begin{matrix} \rightarrow X \\ \rightarrow G \end{matrix}$$

$$\begin{matrix} K \rightarrow \\ S \rightarrow \end{matrix} \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 11 \\ 19 \end{bmatrix} = \begin{bmatrix} 68 \\ 41 \end{bmatrix} = \begin{bmatrix} 16 \\ 15 \end{bmatrix} (\bmod 26) \begin{matrix} \rightarrow P \\ \rightarrow O \end{matrix}$$

8. **Align the letters in a single line without spaces. The message is now enciphered.**

$$FZIFTOTBXGPO$$

Deciphering a Message: Known Enciphering Matrix

In order to decipher the matrix, you must know the enciphering matrix used. All parties with legitimate access to the ciphertext should know the enciphering matrix.

1. **Obtain a plaintext message to encode in standard English with no punctuation.**

In the example, we will decipher the message *SAKNOXAOJX* given that it is a Hill cipher with enciphering matrix $\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$.

2. **Group the ciphertext into pairs.**

S A K N O X A O J X

3. **Replace each letter by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3…Z=0. See Table A, repeated below, for quick reference.**

Table A– Letters and Their Corresponding Positions

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

S	A	K	N	O	X	A	O	J	X
19	1	11	14	15	24	1	15	10	24

4. **Convert each pair of letters into ciphertext vectors.**

$$\begin{matrix} S \to \\ A \to \end{matrix} \begin{bmatrix} 19 \\ 1 \end{bmatrix} \quad \begin{matrix} K \to \\ N \to \end{matrix} \begin{bmatrix} 11 \\ 14 \end{bmatrix} \quad \begin{matrix} O \to \\ X \to \end{matrix} \begin{bmatrix} 15 \\ 24 \end{bmatrix} \quad \begin{matrix} A \to \\ O \to \end{matrix} \begin{bmatrix} 1 \\ 15 \end{bmatrix} \quad \begin{matrix} J \to \\ X \to \end{matrix} \begin{bmatrix} 10 \\ 24 \end{bmatrix}$$

5. Find the inverse of the enciphering matrix.

5.1. Find the determinant of the enciphering matrix.

$$\det\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = (4 \times 2) - (1 \times 3) = 5$$

5.2. Find the determinant's reciprocal modulo 26. See Table B below for quick reference.

Table B– Determinants' Reciprocals Modulo 26												
Determinant	1	3	5	7	9	11	15	17	19	21	23	25
Reciprocal Modulo 26	1	9	21	15	3	19	7	23	11	5	17	25

$$\det\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = (4 \times 2) - (1 \times 3) = 5 \therefore 5^{-1} (\bmod 26) = 21$$

5.3. Multiply the reciprocal modulo 26 by the enciphering matrix.

$$21\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 42 & -21 \\ -63 & 84 \end{bmatrix}$$

5.4. Find the residue modulo 26 of the new matrix. This is the deciphering matrix.

$$21\begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 42 & -21 \\ -63 & 84 \end{bmatrix} = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} (\bmod 26)$$

6. Convert the ciphertext vectors into plaintext vectors.

6.1. Mutiply the deciphering matrix by each ciphertext vector.

$$\begin{matrix} S\rightarrow \\ A\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}19\\1\end{bmatrix}=\begin{bmatrix}309\\291\end{bmatrix} \quad \begin{matrix} K\rightarrow \\ N\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}11\\14\end{bmatrix}=\begin{bmatrix}246\\249\end{bmatrix} \quad \begin{matrix} O\rightarrow \\ X\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}15\\24\end{bmatrix}=\begin{bmatrix}360\\369\end{bmatrix}$$

$$\begin{matrix} A\rightarrow \\ O\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}1\\15\end{bmatrix}=\begin{bmatrix}91\\105\end{bmatrix} \quad \begin{matrix} J\rightarrow \\ X\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}10\\24\end{bmatrix}=\begin{bmatrix}280\\294\end{bmatrix}$$

6.2. Replace each new vector by its residue modulo 26 if possible.

$$\begin{matrix} S\rightarrow \\ A\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}19\\1\end{bmatrix}=\begin{bmatrix}309\\291\end{bmatrix}=\begin{bmatrix}23\\5\end{bmatrix}(\bmod 26)$$

$$\begin{matrix} K\rightarrow \\ N\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}11\\14\end{bmatrix}=\begin{bmatrix}246\\249\end{bmatrix}=\begin{bmatrix}12\\15\end{bmatrix}(\bmod 26)$$

$$\begin{matrix} O\rightarrow \\ X\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}15\\24\end{bmatrix}=\begin{bmatrix}360\\369\end{bmatrix}=\begin{bmatrix}22\\5\end{bmatrix}(\bmod 26)$$

$$\begin{matrix} A\rightarrow \\ O\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}1\\15\end{bmatrix}=\begin{bmatrix}91\\105\end{bmatrix}=\begin{bmatrix}13\\1\end{bmatrix}(\bmod 26)$$

$$\begin{matrix} J\rightarrow \\ X\rightarrow \end{matrix}\begin{bmatrix}16 & 5\\15 & 6\end{bmatrix}\begin{bmatrix}10\\24\end{bmatrix}=\begin{bmatrix}280\\294\end{bmatrix}=\begin{bmatrix}20\\9\end{bmatrix}(\bmod 26)$$

7. Convert each entry in the ciphertext vector into its corresponding position in the alphabet.

$$\begin{matrix} S \rightarrow \\ A \rightarrow \end{matrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}\begin{bmatrix} 19 \\ 1 \end{bmatrix} = \begin{bmatrix} 309 \\ 291 \end{bmatrix} = \begin{bmatrix} 23 \\ 5 \end{bmatrix}(\bmod 26)\begin{matrix} \rightarrow W \\ \rightarrow E \end{matrix}$$

$$\begin{matrix} K \rightarrow \\ N \rightarrow \end{matrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}\begin{bmatrix} 11 \\ 14 \end{bmatrix} = \begin{bmatrix} 246 \\ 249 \end{bmatrix} = \begin{bmatrix} 12 \\ 15 \end{bmatrix}(\bmod 26)\begin{matrix} \rightarrow L \\ \rightarrow O \end{matrix}$$

$$\begin{matrix} O \rightarrow \\ X \rightarrow \end{matrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}\begin{bmatrix} 15 \\ 24 \end{bmatrix} = \begin{bmatrix} 360 \\ 369 \end{bmatrix} = \begin{bmatrix} 22 \\ 5 \end{bmatrix}(\bmod 26)\begin{matrix} \rightarrow V \\ \rightarrow E \end{matrix}$$

$$\begin{matrix} A \rightarrow \\ O \rightarrow \end{matrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}\begin{bmatrix} 1 \\ 15 \end{bmatrix} = \begin{bmatrix} 91 \\ 105 \end{bmatrix} = \begin{bmatrix} 13 \\ 1 \end{bmatrix}(\bmod 26)\begin{matrix} \rightarrow M \\ \rightarrow A \end{matrix}$$

$$\begin{matrix} J \rightarrow \\ X \rightarrow \end{matrix}\begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix}\begin{bmatrix} 10 \\ 24 \end{bmatrix} = \begin{bmatrix} 280 \\ 294 \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \end{bmatrix}(\bmod 26)\begin{matrix} \rightarrow T \\ \rightarrow H \end{matrix}$$

8. Align the letters in a single line without spaces.

$$WELOVEMATH$$

9. Use logic and phonetics to determine individual words. The message is now deciphered.

$$WE\ LOVE\ MATH$$

Deciphering a Message: Unknown Enciphering Matrix

As stated previously, all parties with legitimate access to the ciphertext should know the enciphering matrix to quickly obtain the plaintext from the enciphered message. However, intercepted ciphertext can be deciphered without the matrix if a minimum of four letters of ciphertext can be correctly matched to plaintext.

1. Obtain an intercepted message.

In this example, we have obtained the message *LNGIHGYBVRENJYQO.*

2. Determine four ciphertext letters for which the plaintext is known.

We know that the last four ciphertext letters correspond to the word *ATOM.*[1]

3. Create corresponding plaintext and ciphertext vectors.

3.1. Replace each letter in the ciphertext and plaintext by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3…Z=0. See Table A, repeated below, for quick reference.

Table A – Letters and Their Corresponding Positions

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Ciphertext			
J	Y	Q	O
10	25	17	15

Plaintext			
A	T	O	M
1	20	15	13

[1] Many letters and written correspondence begin with common words such as "dear" or "hello" or the name of the intended recipient. Real ciphertext can be deciphered by making and using these assumptions.

3.2. Convert each pair of letters in the ciphertext and plaintext into vectors.

Ciphertext

$$\begin{matrix} J \to \\ Y \to \end{matrix}\begin{bmatrix} 10 \\ 25 \end{bmatrix}$$

$$\begin{matrix} Q \to \\ O \to \end{matrix}\begin{bmatrix} 17 \\ 15 \end{bmatrix}$$

Plaintext

$$\begin{matrix} A \to \\ T \to \end{matrix}\begin{bmatrix} 1 \\ 20 \end{bmatrix}$$

$$\begin{matrix} O \to \\ M \to \end{matrix}\begin{bmatrix} 15 \\ 13 \end{bmatrix}$$

3.3. Name the ciphertext vectors c_1 and c_2 and the plaintext vectors p_1 and p_2.

$$c_1 = \begin{bmatrix} 10 \\ 25 \end{bmatrix} \qquad p_1 = \begin{bmatrix} 1 \\ 20 \end{bmatrix}$$

$$c_2 = \begin{bmatrix} 17 \\ 15 \end{bmatrix} \qquad p_2 = \begin{bmatrix} 15 \\ 13 \end{bmatrix}$$

4. Group the ciphertext and plaintext vectors into 2x2 matrices.

4.1. Take the transpose of all vectors.

$$c_1^T = \begin{bmatrix} 10 & 25 \end{bmatrix} \qquad p_1^T = \begin{bmatrix} 1 & 20 \end{bmatrix}$$

$$c_2^T = \begin{bmatrix} 17 & 15 \end{bmatrix} \qquad p_2^T = \begin{bmatrix} 15 & 13 \end{bmatrix}$$

4.2. Create the 2x2 matrix C such that $C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix}$.

$$C = \begin{bmatrix} c_1^T \\ c_2^T \end{bmatrix} = \begin{bmatrix} 10 & 25 \\ 17 & 15 \end{bmatrix}$$

4.3. Create the 2x2 matrix P such that $P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix}$.

$$P = \begin{bmatrix} p_1^T \\ p_2^T \end{bmatrix} = \begin{bmatrix} 1 & 20 \\ 15 & 13 \end{bmatrix}$$

5. Solve for the deciphering matrix.

5.1. Augment matrix C to matrix P such that $[C \mid P]$.

$$[C \mid P] = \left[\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 17 & 15 & 15 & 13 \end{array}\right]$$

5.2. Perform elementary row operations on $[C \mid P]$ to obtain the 2x2 identity matrix on the left side of the augmented matrix. The 2x2 matrix formed on the right side of the matrix is the deciphering matrix.

(1) $\left[\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 17 & 15 & 15 & 13 \end{array}\right]$ Form the matrix $[C \mid P]$.

(2) $\left[\begin{array}{cc|cc} 27 & 40 & 16 & 33 \\ 17 & 15 & 15 & 13 \end{array}\right]$ Add row 2 to row 1.

(3) $\left[\begin{array}{cc|cc} 1 & 14 & 16 & 7 \\ 17 & 15 & 15 & 13 \end{array}\right]$ Replace row 1 entries by their residues mod 26.

(4) $\left[\begin{array}{cc|cc} 1 & 14 & 16 & 7 \\ 0 & -223 & -257 & -106 \end{array}\right]$ Add -17 times the first row to the second.

(5) $\left[\begin{array}{cc|cc} 1 & 14 & 16 & 7 \\ 0 & 11 & 3 & 24 \end{array}\right]$ Replace row 2 entries by their residues mod 26.

(6) $\left[\begin{array}{cc|cc} 1 & 14 & 16 & 7 \\ 0 & 1 & 57 & 456 \end{array}\right]$ Multiply row 2 by $11^{-1} = 19$.

(7) $\left[\begin{array}{cc|cc} 1 & 14 & 16 & 7 \\ 0 & 1 & 5 & 14 \end{array}\right]$ Replace row 2 entries by their residues mod 26.

(8) $\left[\begin{array}{cc|cc} 1 & 0 & -54 & -189 \\ 0 & 1 & 5 & 14 \end{array}\right]$ Add -14 times the second row to the first.

(9) $\left[\begin{array}{cc|cc} 1 & 0 & 24 & 19 \\ 0 & 1 & 5 & 14 \end{array}\right]$ Replace row 1 entries by their residues mod 26.

The deciphering matrix is $\begin{bmatrix} 24 & 19 \\ 5 & 14 \end{bmatrix}$.

6. Group the whole ciphertext into pairs.

L N   G I   H G   Y B   V R   E N   J Y   Q O

7. Replace each letter by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3, etc. See Table A, repeated below, for quick reference.

Table A – Letters and Their Corresponding Positions																									
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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

L	N	G	I	H	G	Y	B	V	R	E	N	J	Y	Q	O
12	14	7	9	8	7	25	2	22	18	5	14	10	25	17	15

8. Convert each pair of letters into ciphertext vectors.

$$\begin{matrix} L \to \\ N \to \end{matrix}\begin{bmatrix} 12 \\ 14 \end{bmatrix} \quad \begin{matrix} G \to \\ I \to \end{matrix}\begin{bmatrix} 7 \\ 9 \end{bmatrix} \quad \begin{matrix} H \to \\ G \to \end{matrix}\begin{bmatrix} 8 \\ 7 \end{bmatrix} \quad \begin{matrix} Y \to \\ B \to \end{matrix}\begin{bmatrix} 25 \\ 2 \end{bmatrix}$$

$$\begin{matrix} V \to \\ R \to \end{matrix}\begin{bmatrix} 22 \\ 18 \end{bmatrix} \quad \begin{matrix} E \to \\ N \to \end{matrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} \quad \begin{matrix} J \to \\ Y \to \end{matrix}\begin{bmatrix} 10 \\ 25 \end{bmatrix} \quad \begin{matrix} Q \to \\ O \to \end{matrix}\begin{bmatrix} 17 \\ 15 \end{bmatrix}$$

9. Follow Steps 6 through 9 under <u>Deciphering a Message: Known Enciphering Matrix</u>.

$$\begin{matrix} L \to \\ N \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} 358 \\ 424 \end{bmatrix} = \begin{bmatrix} 20 \\ 8 \end{bmatrix} (\bmod 26) \begin{matrix} \to T \\ \to H \end{matrix}$$

$$\begin{matrix} G \to \\ I \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 7 \\ 9 \end{bmatrix} = \begin{bmatrix} 213 \\ 259 \end{bmatrix} = \begin{bmatrix} 5 \\ 25 \end{bmatrix} (\bmod 26) \begin{matrix} \to E \\ \to Y \end{matrix}$$

$$\begin{matrix} H \to \\ G \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 8 \\ 7 \end{bmatrix} = \begin{bmatrix} 227 \\ 250 \end{bmatrix} = \begin{bmatrix} 19 \\ 16 \end{bmatrix} (\bmod 26) \begin{matrix} \to S \\ \to P \end{matrix}$$

$$\begin{matrix} Y \to \\ B \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 25 \\ 2 \end{bmatrix} = \begin{bmatrix} 610 \\ 503 \end{bmatrix} = \begin{bmatrix} 12 \\ 9 \end{bmatrix} (\bmod 26) \begin{matrix} \to L \\ \to I \end{matrix}$$

$$\begin{matrix} V \to \\ R \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 22 \\ 18 \end{bmatrix} = \begin{bmatrix} 618 \\ 670 \end{bmatrix} = \begin{bmatrix} 20 \\ 20 \end{bmatrix} (\bmod 26) \begin{matrix} \to T \\ \to T \end{matrix}$$

$$\begin{matrix} E \to \\ N \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 190 \\ 291 \end{bmatrix} = \begin{bmatrix} 8 \\ 5 \end{bmatrix} (\bmod 26) \begin{matrix} \to H \\ \to E \end{matrix}$$

$$\begin{matrix} J \to \\ Y \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 10 \\ 25 \end{bmatrix} = \begin{bmatrix} 365 \\ 540 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} (\bmod 26) \begin{matrix} \to A \\ \to T \end{matrix}$$

$$\begin{matrix} Q \to \\ O \to \end{matrix}\begin{bmatrix} 24 & 5 \\ 19 & 14 \end{bmatrix}\begin{bmatrix} 17 \\ 15 \end{bmatrix} = \begin{bmatrix} 483 \\ 533 \end{bmatrix} = \begin{bmatrix} 15 \\ 13 \end{bmatrix} (\bmod 26) \begin{matrix} \to O \\ \to M \end{matrix}$$

THEYSPLITTHEATOM

The entire deciphered message is *THEY SPLIT THE ATOM*.

Conclusion

The Hill 2-cipher is a great example of how mathematics can change the way we communicate. In fact, the Hill cipher can be modified to work for a variety of situations and codes. While the intricacies and proofs of the math are beyond the scope of this guide, here are a few suggestions for your own unique messages:

Desired Action	Calculation Changes	Suggestions
Include punctuation; Encrypt in other languages	Choose a new modulus equal to the total number of letters and symbols.	Choose the new modulus carefully. Prime mods work best because they form inverses more easily.
Encrypt large amounts of text at once	Instead of using a Hill 2-cipher, use a Hill *n*-cipher and group according to *n*.	Performing the Hill 3- or Hill 4-ciphers on paper can result in easy calculating errors. Always check your work with a calculator or other tool.
Create a more secure message system overall	N/A	Combine mathematically complex ciphers with simple ciphers (i.e. Caesar's cipher or the Freemason cipher).

Appendix

GLOSSARY

Ciphers – codes

Ciphertext – coded messages

Cryptography – the study of encoding and decoding secret messages

Decipher – to accurately extract written information from coded messages

Encipher – to effectively hide written information behind seemingly useless jargon

Mod – abbr. modulus

Modular arithmetic – the technique of working with remainders to secure a non-negative integer between zero and positive integer *m*.

Modulo 26 – in modular arithmetic, this refers to the act of cycling a number through 26 different entities, which in this case represent letters.

Plaintext – uncoded messages

Substitution ciphers – the simplest ciphers, which replace each letter of the alphabet by a different letter

REFERENCES

[1] D. Wright, "Nineteenth Century: Statistics," [online document], 1999 Nov 19, [cited 2007 Oct 4], Available HTTP: http://www.math.okstate.edu/~wrightd/crypt/crypt-intro/node9.html

[2] X. Yuan, "Lecture 6: Classic Ciphers," [online document], Available HTTP: http://vanets.vuse.vanderbilt.edu/~xue/cs291fall06/lecture6.pdf