



# The Hill Cipher: A Cryptosystem Using Linear Algebra

---

*Robyn N. Taylor*

*Mentor: Gerard LaVarnway*

*Norwich University*

*Northfield, VT*

*April 6, 2013*



# Classic Cryptology

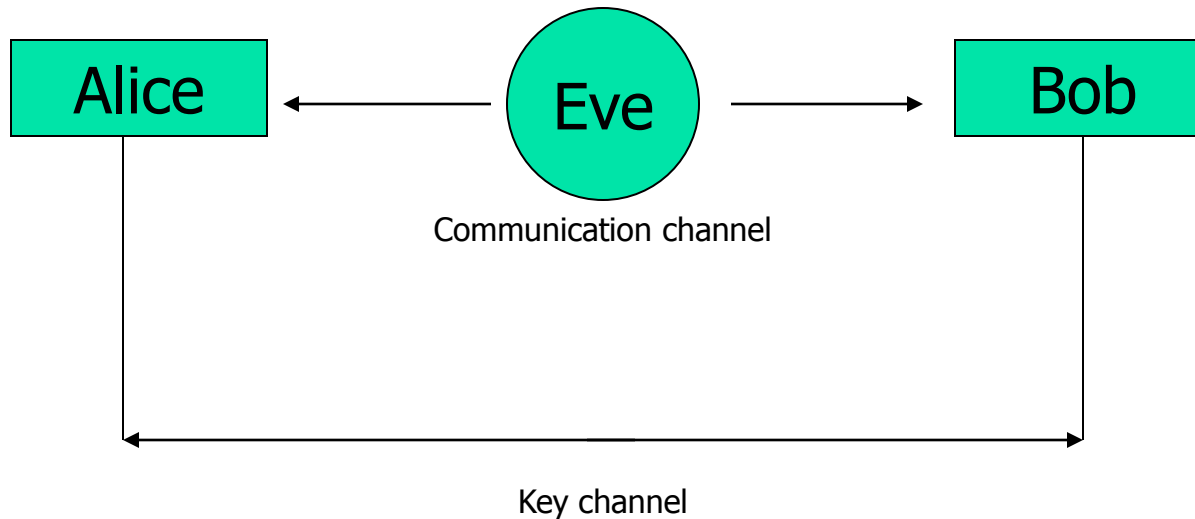
---

- Classic cryptology refers to methods of encipherment from antiquity to the middle of the 20<sup>th</sup> century



# The Central Problem of Classic Cryptology

---

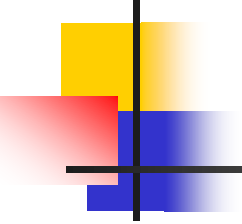




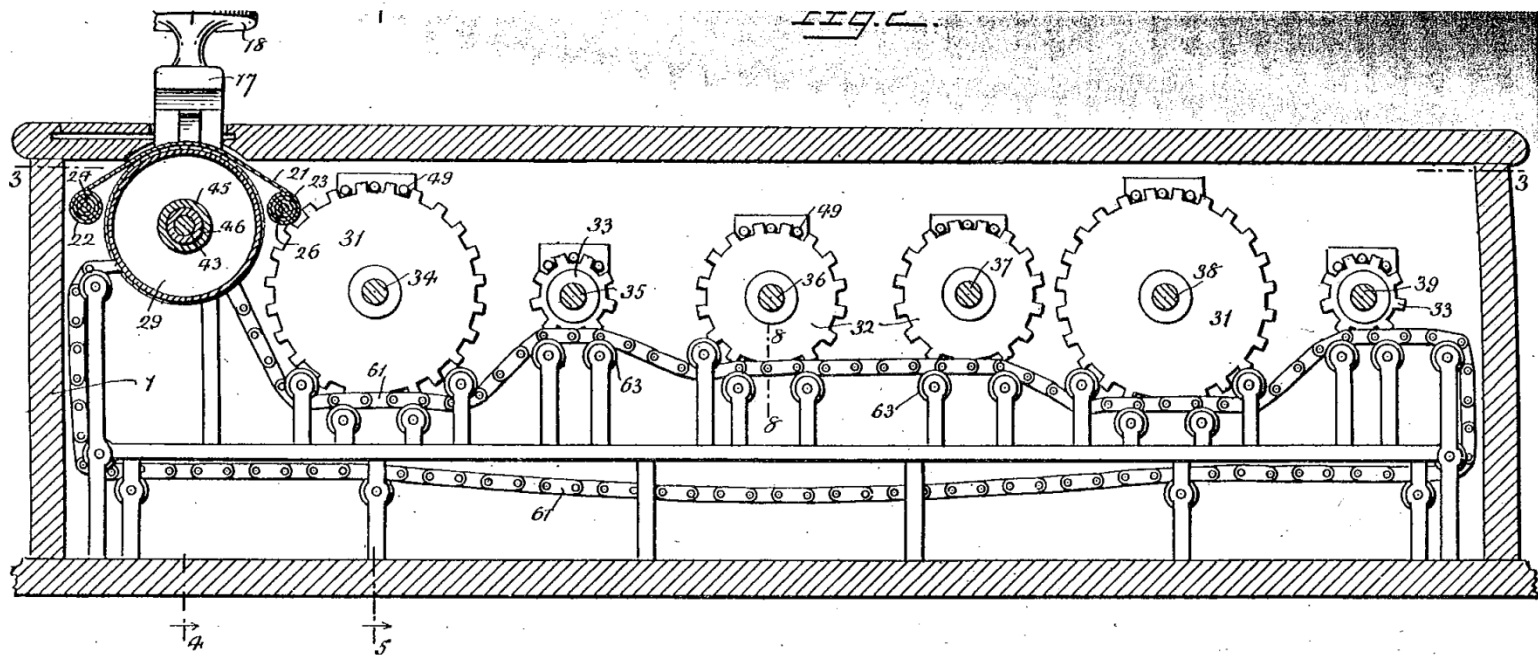
# Polygraphic Substitution Ciphers

---

- *polygraphic substitution cipher:*
  - blocks of plaintext characters are replaced by blocks of ciphertext characters

- 
- 
- Lester Hill of Hunter College first introduced his “system” in an article in 1929 published in the *American Mathematical Monthly* entitled “Cryptology in an Algebraic Alphabet”

# Lester Hill's Cipher Machine



*The mechanism of the cipher machine, U.S. Patent 1,845,947, that was invented by Lester Hill and Louis Weisner, for polygraphic substitution*



# Principle Idea

---

- Group plaintext letters into blocks (size of 2,3,4 ...)
- Encipher blocks as other equal length blocks

plaintext  $\rightarrow$  ciphertext

*MI*  $\rightarrow$  *EQ*

*SS*  $\rightarrow$  *GC*



# Block size

---

- Hill worked in three letter blocks
- We will work in two letter blocks
- Restrict alphabet to capital letters:
  - A, B, C, D, ....Z



# Monoalphabetic Substitution

---

How many two letter blocks can we form from the letters A...Z?

$$26 \times 26 = 676$$

Therefore, we can think of Hill's system as a monoalphabetic substitution cipher on a 676 character alphabet.


$$Y = Ax \bmod 26$$

- $Y$  is a  $2 \times 1$  matrix of ciphertext numerical equivalents
- $A$  is a  $2 \times 2$  matrix
- $x$  is a  $2 \times 1$  matrix of plaintext numerical equivalents.

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \bmod 26$$



# The Key

---

- The key to the encryption scheme is the coefficient matrix  $A$ .
- We have to choose  $a$ ,  $b$ ,  $c$ , and  $d$  in such a way so that  $A$  is invertible mod 26

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \pmod{26}$$



## Example:

---

- Suppose we chose to encipher the word MISSISSIPPI
- We pad with a suitable character to have an even number of plaintext characters

MISSISSIPPIK



# Numerical Equivalents

---

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
0	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

M	I	S	S	I	S	S	I	P	P	I	K
12	8	18	18	8	18	18	8	15	15	8	10



# Then We Encrypt

Suppose our key matrix A is

$$A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \text{mod } 26$$

$$\begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 16 \end{bmatrix} \text{mod } 26 \begin{bmatrix} M \\ I \end{bmatrix} \rightarrow \begin{bmatrix} E \\ Q \end{bmatrix}$$

$$\begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \end{bmatrix} = \begin{bmatrix} 6 \\ 2 \end{bmatrix} \text{mod } 26 \begin{bmatrix} S \\ S \end{bmatrix} \rightarrow \begin{bmatrix} G \\ C \end{bmatrix}$$

*etc.*



# The Ciphertext Becomes

---

*MISSISSIPPIK* → *EQGCUWGEFGUI*

- The Hill cipher masks letter frequencies
- S does not always map to the same letter
- I does not always map to the same letter



# Ciphertext Only Attack

---

- Since the letter frequencies are masked the Hill cipher is considerably more difficult to crack than a monoalphabetic substitution that is vulnerable to frequency analysis.



# Cryptanalysis Of The Hill Cipher

---

- You only have the ciphertext
- You suspect the Hill cipher was used for encryption
- You do not know the key matrix
- How would you go about recovering the plaintext?



# Brute force?

---

- Try all possible  $2 \times 2$  matrices on the first few letters until you recover an intelligible message
- Requires testing around  $24^4 = 456,976$  different matrices



# Known Plaintext Attack

---

- You know
  - the methods of encipherment and decipherment
  - portion of the ciphertext
  - portion of the corresponding plaintext.



# Decryption

---

AS LONG AS  $A^{-1}$  EXISTS!

$$x = A^{-1}Y \bmod 26$$

When does  $A^{-1}$  exists?



# Invertible Modulo $m$

---

A  $2 \times 2$  matrix  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$  is invertible modulo  $m$

if and only if  $\det(A)$  is relatively prime to  $m$ . In this case,

the inverse is given by  $A^{-1} = \det(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \bmod m$



# Mod 26

---

- determinant of coefficient matrix  $A$  must be relatively prime to 26
- $\det(A)$  cannot be even or 13



# Example for Finding A Inverse

---

$$A = \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}$$

$$\det(A) = (22)(5) - (11)(13) = -33 = 19 \bmod 26$$

19 is relatively prime to 26  $\rightarrow 19^{-1}$  exists

$$19^{-1} \bmod 26 = 11 \quad (19 \times 11) = 209 \bmod 26 = 1 \bmod 26$$

$$A^{-1} = 19^{-1} \begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} \bmod 26 = 11 \begin{bmatrix} 5 & -13 \\ -11 & 22 \end{bmatrix} \bmod 26 = \begin{bmatrix} 3 & 13 \\ 9 & 8 \end{bmatrix} \bmod 26$$



# Decryption

---

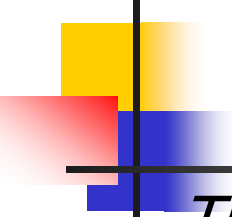
$$MISSISSIPPIK \leftarrow EQGCUWGEFGUI$$

$$E, Q, = 4, 16$$

$$x = A^{-1}Y$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 & 13 \\ 9 & 8 \end{bmatrix} \begin{bmatrix} 4 \\ 16 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 12 \\ 18 \end{bmatrix} \rightarrow \begin{bmatrix} M \\ I \end{bmatrix}$$



*The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others. Some are fortunate enough to find a job which consists in the solution of mysteries, but most are driven to sublimate this urge by solving artificial puzzles devised for our entertainment. Detective stories or crossword puzzles cater for the majority; the solution of secret codes may be the pursuit of a few*

*John Chadwick*

*The Decipherment of Linear B*



# References

---

- T. Barr, *Invitation to Cryptology*, Prentice Hall, Upper Saddle River, NJ 2002
- S. Flannery, *In Code*, Algonquin Books, Chapel Hill, 2002
- D. Kahn, *The Code-Breakers*, MacMillan Publishing Company, New York, 1967
- R.. Lewand, *Cryptological Mathematics*, The Mathematics Association of America, Washington, 2000
- S. Singh, *The Code Book*, Doubleday, New York, 1999