CRYPTOGRAPHY

HISTORY:

- •2000 B.C. the Egyptians used hieroglyphics on the tombs of their deceased kings and rulers
- •The ancient Chinese used the ideographic nature of their language to conceal the meaning of words
- •In India, the government used secret codes to communicate with numerous spies placed strategically throughout the country
- •The Greek writer Polybius created the 5x5 Polybius Square. Julius Caesar used a method of advancing each letter four positions, also known as a Caesar Shift
- •In 1379, the first European manual of cryptography was a gathering of cyphers by Gabriele de Lavinde of Parma, who served Pope Clement VII
- •In 1917, the United States formed the cryptographic organization MI-8, where they analyzed all types of secret messages, codes, secret links, and encryptions

TERMS:

Cryptography is the practice and study of hiding information. Cryptology comes from the Greek words kryptos, which stands for “hidden” and grafein, which stands for to “write.”Encryption is the process of making information unreadable through an algorithm, called a cipher. This information is only attainable by someone who has the “key.” With this key, one can decipher the unreadable information. Ciphering has always been considered vital for diplomatic and military secrecy.

INFO PROTECTED ONLINE BY CRYPTOGRAPHY:

1. Credit-Card Information
2. Social Security Numbers
3. Personal Details
4. Sensitive Company Information
5. Bank-Account Information

Web browsers will encrypt text automatically. Upon arrival, the browser will decrypt the text. Interception of such information would be usless to someone without the “key.”

APPLYING CRYPTOGRAPHY:

INFORMATION TO BE TRANSMITTED → BE READY FOR FINALS

ASSIGN:	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	26

since there are only 26 letters, we will use 27 as a space between words.

Encoding Matrix: $\begin{bmatrix} -2 & -8 & -4 \\ 0 & 2 & 1 \\ 3 & 4 & 8 \end{bmatrix}$

BE READY FOR FINALS

2 5 27 18 5 1 4 25 27 6 15 18 27 6 9 14 1 12 19

Since the encoding matrix is a 3x3 matrix, we will want to split the message above into a sequence of 3x1 vectors, as follows:

$$\begin{bmatrix} 2 & 18 & 4 & 6 & 27 & 14 & 19 \\ 5 & 5 & 25 & 15 & 6 & 1 & 27 \\ 27 & 1 & 27 & 18 & 9 & 12 & 27 \end{bmatrix} \longrightarrow \begin{bmatrix} 2 & 18 & 4 & 6 & 27 & 14 & 19 \\ 5 & 5 & 25 & 15 & 6 & 1 & 27 \\ 27 & 1 & 27 & 18 & 9 & 12 & 27 \end{bmatrix}$$

Encryption: The message is encrypted by multiplying the encoding matrix with the matrix formed by the message, as follows:

$$\begin{bmatrix} -2 & -8 & -4 \\ 0 & 2 & 1 \\ 3 & 4 & 8 \end{bmatrix} \begin{bmatrix} 2 & 18 & 4 & 6 & 27 & 14 & 19 \\ 5 & 5 & 25 & 15 & 6 & 1 & 27 \\ 27 & 1 & 27 & 18 & 9 & 12 & 27 \end{bmatrix} \approx \begin{bmatrix} -152 & -80 & -316 & -204 & -138 & -84 & -362 \\ 37 & 11 & 77 & 48 & 21 & 14 & 81 \\ 242 & 82 & 328 & 222 & 177 & 142 & 381 \end{bmatrix}$$

The message transmitted into linear form is: -152,-80,-316,-204,-138,-84,-362,37,11,77,48,21,14,81,242,82,328,222,177,142,381, which is totally useless to someone without the “key” or encoding/decoding matrix.

Decryption: The message is decrypted, first, by using the “key” to find it’s inverse, as follows:

$$\left[\begin{array}{ccc:ccc} -2 & -8 & -4 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ 3 & 4 & 8 & 0 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & -1/2 & -2 & 0 \\ 0 & 1 & 0 & -1/8 & 1/6 & -1/12 \\ 0 & 0 & 1 & 1/4 & 2/3 & 1/6 \end{array}\right] \longrightarrow \begin{bmatrix} -1/2 & -2 & 0 \\ -1/8 & 1/6 & -1/12 \\ 1/4 & 2/3 & 1/6 \end{bmatrix}$$

Using the inverse of the “key,” we multiply it with the encrypted matrix previously created, as follows:

$$\begin{bmatrix} -1/2 & -2 & 0 \\ -1/8 & 1/6 & -1/12 \\ 1/4 & 2/3 & 1/6 \end{bmatrix} \begin{bmatrix} -152 & -80 & -316 & -204 & -138 & -84 & -362 \\ 37 & 11 & 77 & 48 & 21 & 14 & 81 \\ 242 & 82 & 328 & 222 & 177 & 142 & 381 \end{bmatrix} \approx \begin{bmatrix} 2 & 18 & 4 & 6 & 27 & 14 & 19 \\ 5 & 5 & 25 & 15 & 6 & 1 & 27 \\ 27 & 1 & 27 & 18 & 9 & 12 & 27 \end{bmatrix}$$

This matrix is the exact matrix we started out with: 2,5,27,18,5,1,4,25,27,6,15,18,27,6,9,14,1,12,19,27,27= BE READY FOR FINALS

RESOURCES: 1. Applications of Linear Algebra. 1 May 2009 <http://aix1.uottowa.ca/~jkhoury/app.htm>
2. A Brief History of Cryptography. 1 May 2009 <http://www.thawte.com/process/crypto/cryptoBriefHistory>
3. Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books, 2000.