•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 Indía, 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 intormation. 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.

|                  | #  |                         |                 | E               |                              |                       |               |               |               |
|------------------|--|-------------------------|-----------------|-----------------|------------------------------|-----------------------|---------------|---------------|---------------|
|                  |  |                         |                 |                 |                              |                       | 2 1           |               |               |
|                  |  | U A M                   |                 | 04              | X                            |                       |               |               |               |
|                  |  | ST                      |                 | * 7             |                              | E                     | CLI           | ÷             |               |
|                  |  |                         |                 |                 | H                            |                       |               | 7             |               |
| に =              | 948  | I 0                     | ê               | 75              | E                            | 14                    | AB            |               |               |
|                  |  | TRE                     | τ               | 技               | 1                            | 7 給                   | RH            | 10            |               |
| ۲.               | 2  | ILM                     |                 | Ţ               | S                            |                       | RDO           |               |               |
| PR               | OTF  | -CTF                    | ED C            | NIIN            | JE BY                        | CR                    | YPT           | OGR           | CAPF          |
|                  | nformat  |                         |                 |                 |                              | -                     |               |               |               |
|                  | tu Num   |                         |                 | ∎ Ø             | н                            | S 20 1                | M             | オ             | =             |
| Det              | nunn<br>Díle   |                         | ц<br>Ч          | シ               | -                            | 25                    | H "           |               | - L           |
|                  | mpanul   | nformat                 | íon             | 品               |                              | 7                     | Ε             |               | M L           |
| ccour            | nt Inform  | nation                  |                 |                 |                              |                       | N             | ~             | A P           |
| Ш                |  |                         | 36              |                 |                              |                       |               |               | A R           |
| sers w           |  | jpt text                | automat         | ically. U       | pon arriva                   | al, the b             | prowser       | will decr     | ypt the t     |
| onot             | such in  | formatic                | on would        | be usles        | ss to some                   | eone wit              | chout th      | e "key."      | RU            |
| VIN              | CICI   | RVP                     | TOG             | RAP             | HV.                          | 1                     |               | Ð             | I N           |
|                  |  |                         |                 |                 |                              | 保                     |               |               | X D           |
| TO BE            | TRANSMI  | KIMN                    | OPOR            | STUVW           | BE REA                       | ADY FOR I             | =INALS        | 保             |               |
| 5 4 5 6          | 7 8 9 10   | ) 11 17 13 14           | 15 16 17 18 1   | 97071777        | 5747576                      | 文                     |               | Ø             | H             |
| radiu 2.6 le     | etters, we v   | vill use 27 a           | s a space be    | tween words     | A<br>5.                      | 目標                    | А н           | T T           | Ellis         |
| x: [-2 ·         | -8 -4  | 0                       |                 | × 11            | M                            | 0な                    |               | -             |               |
| 0                | 2 1  | U T                     | 文               |                 | W                            | ~ ~                   | CR            | tz            | S T           |
| 3                | 4 8  | R                       | -               | 75              | 0                            |                       |               | ラ             |               |
| 13. 11           | ΒE   | REA                     | DYFO            | OR F            | INALS                        | 社                     |               |               |               |
|                  | 2 5 27   | 18 5 1 4                | + 25 27 6 1     | 5 18 27 6 9     | 14 1 12 19                   | 明                     | T             | <b>34</b> .   | . н .         |
| lingmat          | ríx ís a 3x3   | matríx, we v            | vill want to sp | olit the mess   | sage above int               | to a seque            | nce of 3x1 ve | ectors, as fo | ollows:       |
| 27 1-            | 4 -19  | СТ                      | 21              | 2               | 18 4 6 27                    | 14 19                 |               |               |               |
| <u>6</u> 1       | $\frac{27}{5}$   | HY                      | 明               | 5               | 5 25 15 6                    | 1 27                  | Ε.            | を             | 0 H           |
| e messa          | 2 27 ge is encru   | nted by my              | Itipluing the   | encoding m      | $1 \frac{2}{18} \frac{9}{9}$ | 12 2/j<br>matrix form | ned by the    | nessage as    | follows       |
| 18 4 6           | 27 14 19   | Field Dg IIId           | ~80 ~316        | -704 -138       | -84 -367                     |                       | ned by the i  | neoodge, do   |               |
| 5 25 15          | 6 1 27   | - 37                    | 11 77           | 48 21           | 14 81                        | - <del></del>         |               | <b>C</b>      | E             |
| 1 27 18          | 9 12 27  | 24                      | 2 82 328        | 222 177         | 142 381                      | Eth                   |               | 宇             |               |
| ,<br>ansmítte    | ed ínto línea  | ar form ís: ~           | 152,-80,-316,   | -204,-138,-     | 84,-362,37,11,7              | 77,48,21,14           | ,81,242,82,3  | 28,222,177,14 | -2,381, which |
| eone with        | nout the "k  | ey" or enco             | oding/decod     | ing matrix.     | N in                         | 技                     |               | U             | RH            |
| e messa          | ge is decry  | pted, fírst,            | by using the    | e "key" to fir  | nd it's inverse              | , as follows          | ; <b>k</b>    | 技             | Elle          |
|                  |  | I                       | U.              |                 | -1/2 -2 0                    | £1.                   |               | す             | -1/2 -2       |
| 10-              |  | 3 5                     |                 |                 | -1/8 1/6 -1/1                | 2                     | T             | £7            | -1/8 1/6 -    |
| 0 1<br>se of the | - "ken " wa  | multipluit              | with the enc    | LO O I I        | 1/4 2/3 1/6                  | _ U                   | follows       | 出             | 1/4 2/3       |
| -157             | -80 -316   | -204 -138               | ~84 ~367        | $\Gamma_{7,18}$ | 4 6 27 14                    | + 19                  | 1010 03:      | Ø             | 0 0           |
| 37               | 11 77  | 48 21                   | 14 81           | ~ 5 5           | 25 15 6 1                    | 27                    |               | シ             | RU            |
| 242              | 82 328   | 222 E 177               | 142 381         | 27 1            | 27 18 9 12                   | . 27                  |               | 66            | L             |
| he exact         | matrix we  | started out             | with: 2,5,27.   | 18,5,1,4,25,2   | 7,6,15,18,27,6.              | 9,14,1,12,19.         | 27,27= BE F   | READY FOR     | FINALS        |
| of Linear Algebr | a. 1 May 2009 <http: <="" td=""><td>/aíx1.uottowa.ca/~jkhou</td><td>ury/app.htm&gt;</td><td>(</td><td>I</td><td></td><td></td><td></td><td></td></http:> | /aíx1.uottowa.ca/~jkhou | ury/app.htm>    | (               | I                            |                       |               |               |               |
|                  | 1 114 2000 114   |                         |                 |                 |                              |                       |               |               |               |

|  | T E B  |  |  |                           | R.                      | R           |
|--|--|--|--|---------------------------|-------------------------|-------------|
|  |  |  | E X  |                           |                         |             |
|  |  |  |  |                           | ŝ                       |             |
| Ē  | I O  |  | E  |                           |                         |             |
| ž  | 美工品  | τ  | 技了   | は、ア田の                     | ザ                       | 1           |
| INFO PR  | OTECTE   | DONL                                       | INE BY   | CRYPT                     | OGRAF                   | 24          |
| 1. Credit-Card I   | nformation   | 絵  |  |                           | <b>*</b> H              | A           |
| 2. Social Securi<br>3. Personal Det  | ity Numbers  |  | ショ   | 観日日式                      | 会 E                     |             |
| 4. Sensítíve Co  | mpany Informatio   | on   |  | 1 = u                     | <u>ب</u> م              |             |
| 5. Bank-Accour   | nt Information   |  |  | カ <sup>N</sup> 5          |                         | R           |
| Web browsers w<br>Interception of  | such information   | utomatically.<br>would be usl              | Upon arrival,<br>ess to someor   | the browser without the   | will decrypt the "key." | ne t        |
| APPIVIN  | CCRVPT   | OGRAI                                      | JHV.   | L O T                     | E I                     |             |
| NFORMATION TO BE   | TRANSMITTED  |  | BE READ'   | Y FOR FINALS              | X                       | D           |
| SSIGN: A B C D E I   | FGHIJKLMNC   | PQRSTUV                                    | W X Y Z  | 文 W T                     | <b>の</b> H              |             |
| ince there are only 26 l   | letters, we will use 27 as a   | a space between wo                         | ords.  | H A H                     | E X                     |             |
| Encoding Matrix: -2  | -8 -4<br>2 -8 -4   | *  | ¥ M<br>₩   |                           |                         |             |
|  | 4 8 R  | Î.   | <b>5</b> 0   | ► H E                     | 3                       |             |
| · · · · · · · · · · · · · · · · · · ·  | BE READ<br>252718514   | 25 27 6 15 18 27                           | FINALS<br>691411219  | 社<br>明 T                  | ŀ. ⊺                    |             |
| Since the encoding mat   | ríx ís a 3x3 matríx, we wil  | l want to split the m                      | essage above ínto a  | sequence of 3x1 ve        | ctors, as follows:      | S           |
| 2     18     4     6     2/     1       5     5     25     15     6     1              | $\begin{array}{c c} -27 \end{array} & \begin{array}{c} \hline \\ \hline \\ \hline \\ \end{array} \end{array}$                      | <u>21</u>                                  | 5 5 25 15 6 1  | 27                        |                         |             |
| 27  1  27  18  9  1  | 2 27   | pluing the encoding                        | 27 1 27 18 9 12<br>matrix with the mat   | 27<br>ríx formed by the n | lessage as follows      | E           |
| -2 -8 -4 2 18 4 6  | 27 14 19 -152  | -80 -316 -204 -1                           | 138 <b>-</b> 84 -362   | <b>7</b>                  | Ε Ε                     | R           |
| 0     2     1     5     5     25     15       3     4     8     27     1     27     18 | 6 1 27 <b>≈</b> 37<br>9 12 27 242  | 11 77 48<br>82 328 222                     | 21 14 81<br>177 142 381  | ep 5 o                    | 字                       |             |
| The message transmitte   | ed into linear form is: -15  | 2,-80,-316,-204,-13                        | 8,-84,-362,37,11,77,4  | +8,21,14,81,242,82,32     | 28,222,177,142,381, w   | hích        |
| iseless to someone wit<br>Decryption: The messa  | hout the "key" or encod<br>age is decrypted, first, b  | ing/decoding matri<br>y using the "key" to | x.<br>find it's inverse, as  | follows:                  | び臣                      |             |
| -2 -8 -4   1 0 0   | I I  |  | -1/2 -2 0<br>-1/8 1/6 -1/12 -  | A                         | -1/2                    | -2<br>1/6 - |
| 3 4 8 0 0 1  | I  | 001  | 1/4 2/3 1/6  |                           | 1/4 2                   | 2/3         |
| Using the inverse of th $-1/2$ -2 0 $-152$   | e "key," we multiply it wi<br>-80 -316 -204 -138 -   | th the encrypted matrix $-362$             | atrix previously created atrix previously created atrix previously created atrix atrians and the second structures at the | ated, as tollows:         | <i>o</i> 0              | 0           |
| -1/8 1/6 -1/12 37  | 11 77 48 21  | 14 81 = 5                                  | 5 25 15 6 1 2;   | 7                         |                         |             |
| /4 2/3 1/6 242<br>This matrix is the exact   | 82 328 222 177<br>t matríx we started out w  | 142 381 27<br>ith: 2,5,27,18,5,1,4,2       | 1 27 18 9 12 27<br>5,27,6,15,18,27,6,9,14  | -,1,12,19,27,27= BE R     | EADY FOR FINAL          | S           |
| RESOURCES: 1. Applications of Linear Algeb   | ra. 1 May 2009 <http: <="" aix1.uottowa.ca="" td="" ~jkhoury=""><td>'app.htm&gt;</td><td>Ι</td><td></td><td></td><td></td></http:> | 'app.htm>                                  | Ι  |                           |                         |             |

|                             | /                      | ΙΨ  | EI   |                           |                              | A                         |                |               | 75              |              |
|-----------------------------|------------------------|---|--|---------------------------|------------------------------|---------------------------|----------------|---------------|-----------------|--------------|
| 2 6                         |                        |   | U A H  |                           | 02                           | X                         | Ľ              |               |                 |              |
|                             |                        |   | s T?   |                           |                              |                           | Ē              | 5 L 1         | Ż               |              |
|                             |                        | 日日金                                       |  | Ż                         |                              | H                         | -15            | H LJ          | モー              |              |
|                             |                        | 天 #                                       | T K 33   | 7                         | 7¥<br>\$\$                   | I                         | - 14           |               | 2023            |              |
| 6                           |                        | 2 7                                       | IL   | -                         | <b>*</b>                     | S                         |                | Roo           | ザ               | S            |
| IN                          | FOI                    | PRO                                       | TECT   | ED C                      | )NLIM                        | VE B'                     | YCR            | YPT           | OGR             | APF          |
| 1. C                        | redit-C                | ard Info                                  | rmation  | 総                         | 出<br>の                       | 1                         | 金田             | M N           | オ               | H A          |
| 2. S<br>3 P                 | Personal S             | ecurity [<br>Details                      | Numbers  | Ŀ                         | - ž                          | Ε                         | ž              | H             | 会<br>第          | - L          |
| 4.5                         | Sensitiv               | e Compa                                   | any Informat   | tion                      |                              |                           | 31             | Eu            | 美               | MA           |
| 5. E                        | Bank-Ac                | count <sup>'</sup> Ir                     | aformation   | 観                         | 数                            |                           | 0カ             | N S           | 1               | AR           |
| Weł                         | o brows                | ers will e                                | encrypt text   | automat                   | ically. U                    | pon arrív                 | al, the b      | prowser v     | will decry      | pt the t     |
| Inte                        | erceptic               | on of suc                                 | ch informatio  | on would                  | be usles                     | s to som                  | eone wit       | chout the     | e "key."        | RU           |
| AF                          | PPLY                   | /ING                                      | CRYP   | TOG                       | RAP                          | HY:                       | <b>R</b>       |               | Ĕ               | × N<br>X D   |
|                             | RMATION                | TOBETRA                                   | NSMITTED   |                           |                              | BE RE                     | ADY FOR I      | =INALS        | 保               |              |
| 1                           | 1 2 3                  | 45678                                     | 8 9 10 11 12 13 14   | 15 16 17 18               | 19 20 21 22 2 <sup>3</sup>   | 5 24 25 26                | 文              |               | Ø               | H            |
| ínce t                      | there are or           | nly 26 letter                             | s, we will use 27 a  | s a space be              | etween word:                 | A.<br>5.<br>M             | 構力             | TH            | X               | Es           |
| _ncoc                       | aing Matrix            | · -2 -8 -                                 |  | Ŷ                         |                              | W                         | 5              | CR            | 相力              | s.           |
|                             |                        | 3 4                                       | 8R   | -                         | 75                           | 0                         |                |               | 5               |              |
| 采                           |                        | H o E                                     | 5 27 18 5 1 4  | DYF<br>4 25 27 6 1        | OR F<br>5 18 27 6 9          | INALS<br>1411219          | 前              |               | F               |              |
| Sínce                       | the encodí             | ng matrix is                              | a 3x3 matríx, we v   | vill want to s            | plit the mess                | sage above in             | nto a sequer   | nce of 3x1 ve | ectors, as foll | ows:         |
| 2 18                        | 8 4 6                  | 27 14 1                                   |  | 社                         | 2                            | 18 4 6 27<br>5 25 15 (    | 14 19          |               |                 | = T          |
| ) )<br>27 1                 | 27 18                  | 9 12 2                                    | T H Y  | 明                         | 27                           | 1 27 18 9                 | 1 2/           |               | を               | 0 =          |
| Encry                       | ption: The             | message is                                | encrypted by mu  | Itiplying the             | encoding ma                  | atrix with the            | matrix forn    | ned by the n  | nessage, as fo  | ollows:      |
| -2 -8<br>0 2                | 1 5 5                  | 8 4 6 2/ 14<br>5 25 15 6 1                | + 19 $-1327 = -37$   | 2 -80 -516<br>11 77       | -204 -138<br>48 21           | 14 81                     | 二字             |               | 5               | EE           |
| 3 4                         | - 8 27 1               | 1 27 18 9 12                              | 2.27 2.4   | -2 82 328                 | 222 177                      | 142 381                   | 75             |               | 子の              | D w          |
| The m                       | iessage tra            | insmitted int                             | to línear form ís: -   | 152,-80,-316              | ,-204,-138,-                 | 84,-362,37,11,            | ,77,48,21,14,  | 81,242,82,32  | 28,222,177,142  | .,381, which |
| Decry                       | ption: The             | e message is                              | decrypted, first,  | by using the              | e "key" to fir               | nd ít's ínverse           | e, as follows  |               | 技               | E            |
| -2 -8                       | 8 -4 1 0<br>1<br>1 0 1 |   |  | U                         |                              | -1/2 -2 0<br>-1/8 1/6 -1/ | 12             | A             | <b>T</b>        | -1/2 -2      |
| 3 4                         |                        |   | I  | 投す                        |                              | 1/4 2/3 1/6               | 0              | E I           |                 | 1/4 2/3      |
| $\frac{\text{Using}}{-1/2}$ | g the invers $-2$      | e of the "ke $-157 = 80$                  | ey," we multiply it $-316 - 204 = 138$   | with the enc $-84$ $-367$ | rypted matri $\Gamma_{2}$ 18 | ix previously $4 6 27 1$  | created, as    | tollows:      | Ø               | 0 0          |
| -1/8                        | 1/6 -1/12              | 37 11                                     | 77 48 21   | 14 81                     | ≈ 5 5                        | 25 15 6 1                 | 1 27           |               | ショ              | RU           |
| 1/4 2                       | 2/3 1/6                | 242 82                                    | 328 222 <sup>E</sup> 177   | 142 381                   | 27 1                         | 27 18 9 12                | 2 27_          | T             |                 | L            |
| This r<br>RESOURCE          | matrix is the          | e exact mati<br>f Línear Algebra. 1 May 2 | rix we started out<br>2009 <http: aix1.uottowa.ca="" td="" ~jkhc<=""><td>ury/app.htm&gt;</td><td>,18,5,1,4,25,2</td><td>7,6,15,18,27,6</td><td>,9,14,1,12,19,</td><td>27,27= BE R</td><td>EADY FOR I</td><td>FINALS</td></http:> | ury/app.htm>              | ,18,5,1,4,25,2               | 7,6,15,18,27,6            | ,9,14,1,12,19, | 27,27= BE R   | EADY FOR I      | FINALS       |
|                             | 2 AR ( LIL'            | raf Court 1 1                             | "2000  |                           | fuiter                       |                           |                |               |                 |              |

ptography. Anchor Books, 2000

|                    | 5          |         |                  |         | 0       |      |
|--------------------|------------|---------|------------------|---------|---------|------|
| 02101              | 0          |         | 3 3              |         | 技       |      |
| 34800              | 1          |         |                  |         | す       |      |
| Using the inverse  | of the "ke | ey," we | multip           | ly it v | víth th | e e  |
| -1/2 -2 0          | -152 -80   | -316    | -204             | -138    | -84     | -36  |
| -1/8 1/6 -1/12     | 37 11      | 77      | 48               | 21      | 14      | 81   |
| 1/4 2/3 1/6        | 242 82     | 328     | 222 <sup>E</sup> | 177     | 142     | 38   |
| This matrix is the | exact mat  | ríx we  | started          | dout    | with: 2 | 2,5, |

3. Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum C

