

CRYPTANALYSIS

INVESTIGATING THE CYCLIC NATURE OF BLOCK-MATRIX CIPHERS

BRANDON R. GROSSARDT

McNair Scholar Research Project
Summer 1999

Faculty Mentor

CHARLES N. MOORE, PH.D.
Kansas State University

TABLE OF CONTENTS.

Table of Contents i

Acknowledgements ii

§1 – Introduction to Block-Matrix Ciphers 1

§2 – The Encryption Algorithm 3

§3 – Mathematical Representation of Encryption Process 4

§4 – Transformations & Their Matrices 5

§5 – Circulant Matrices & Their Properties 5

§6 – The Order, k 6

§7 – Multi-Reference Ciphers 8

§8 – Permutation Matrix Ciphers 9

§9 – Generalization of Matrix Ciphers 12

APPENDIX A – Restrictions when building a q -fidelity cipher 14

APPENDIX B – Table of k values for given $q \times \ell$ matrix 15

APPENDIX C – The Euler φ -function 16

REFERENCES 17

ACKNOWLEDGEMENTS

First, I want to thank my parents for putting up with my sporadic arrivals and departures from home this summer. Many times I wasn't even sure when I would show up, or when I would be able to help out on the farm. Thanks for understanding Mom and Dad. Second, I would like to thank the *Kansas State University* McNair Scholars' Program for allowing me the opportunity to research and present my topic. It has been a greater growing process than I could have ever imagined. Thanks Elverta, Jon, Kathleen, Laura, and Lora. The program has been great. Next, I would like to thank my mentor, Charles Moore. We met on nearly a daily basis throughout the summer, and Dr. Moore's explanations and insight never ceased to amaze me. I don't know that I could have asked for a better or more knowledgeable mentor. Not to leave anyone out, I would like to thank my best friend, Kipp, for keeping me sane and listening to my constant rambling. In a way, he gave me the idea for my project (i.e., he was there when I stumbled upon it). And finally, I would like to thank God, without whose guidance and love I would never have completed such a task as this.

§1 – INTRODUCTION TO BLOCK-MATRIX CIPHERS

Ciphers have been in existence for more than 2000 years, some dating back as far as the times of Cæsar. There are several different types of ciphers, from simple substitution ciphers, to symbol-representative ciphers, to the more difficult block-matrix ciphers. The simplest of the block-matrix ciphers is what is known as the “bi-fidelity” or bi-fid cipher *. To obtain the standard bi-fid key, one simply arranges the letters of the alphabet in a 5×5 matrix.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Once a key is chosen, one must choose the text he/she wishes to encrypt. For example, say one wishes to encrypt *WILDCAT* using the bi-fid method. First one writes out the letters, finding at the same time their row and column coordinates. For example, the W row-value (denoted by W_r) is 5. Likewise, the W column-value, W_c , is 3. The r and c values are found for all letters of the text.

	W	I	L	D	C	A	T
Row	5	2	3	1	1	1	4
Column	3	4	2	4	3	1	5

To continue, one now reads across the *Row* values and rewrites each pair vertically. For example, the first two values are (5,2), followed by (3,1), and (1,1). These are written as

$$\begin{array}{l} 5_{W_r} \quad 3_{L_r} \quad 1_{C_r} \\ 2_{I_r} \quad 1_{D_r} \quad 1_{A_r} \end{array}$$

If you reach the end of a row and there are not enough numbers to make a pair, then wrap around and continue using the next row values. The next pairs are then, in order, (4, 3), (4, 2), (4, 3), and (1, 5). Our complete listing of values is

$$\begin{array}{l} 5_{W_r} \quad 3_{L_r} \quad 1_{C_r} \quad 4_{T_r} \quad 4_{I_c} \quad 4_{D_c} \quad 1_{A_c} \\ 2_{I_r} \quad 1_{D_r} \quad 1_{A_r} \quad 3_{W_c} \quad 2_{L_c} \quad 3_{C_c} \quad 5_{T_c} \end{array}$$

It is now a matter of using the new arrangement of the row and column indices to form the encrypted message.

$$\begin{array}{l} V \quad K \quad A \quad R \quad Q \quad R \quad E \\ 5_{W_r} \quad 3_{L_r} \quad 1_{C_r} \quad 4_{T_r} \quad 4_{I_c} \quad 4_{D_c} \quad 1_{A_c} \\ 2_{I_r} \quad 1_{D_r} \quad 1_{A_r} \quad 3_{W_c} \quad 2_{L_c} \quad 3_{C_c} \quad 5_{T_c} \end{array}$$

The final encryption yields

$$\left[\begin{array}{cccccc} W & I & L & D & C & A & T \\ 5 & 2 & 3 & 1 & 1 & 1 & 4 \\ 3 & 4 & 2 & 4 & 3 & 1 & 5 \end{array} \right] \rightarrow \left[\begin{array}{cccccc} V & K & A & R & Q & R & E \\ 5 & 3 & 1 & 4 & 4 & 4 & 1 \\ 2 & 1 & 1 & 3 & 2 & 3 & 5 \end{array} \right] \begin{array}{l} \text{New Row Values} \\ \text{New Column Values} \end{array} .$$

Note that even though there are no repeated letters in the original text, the encrypted text has a repeated “R”. This type of encryption is effective for just that reason. The encrypted text is in no direct relation to the original message.

* The “*Russian Nihilist Cipher*” and the “*Polybius Cipher*” are closely related to the bi-fid cipher. See [11, pp.131-309] for an excellent introduction to various ciphers.

The previous example is an introduction to the process of encrypting a message using the bi-fid method. What if we want to use a more secure method, say a triple or quadruple fidelity representation? The method for encryption is similar. One coordinate system of the alphabet for the tri-fid cipher is

$$\begin{array}{c}
 1^{st} \text{ Layer} \\
 \begin{bmatrix} 1 & 2 & 3 \\ 1 & A & B & C \\ 2 & D & E & F \\ 3 & G & H & I \end{bmatrix}
 \end{array}
 \quad
 \begin{array}{c}
 2^{nd} \text{ Layer} \\
 \begin{bmatrix} 1 & 2 & 3 \\ 1 & J & K & L \\ 2 & M & N & O \\ 3 & P & Q & R \end{bmatrix}
 \end{array}
 \quad
 \begin{array}{c}
 3^{rd} \text{ Layer} \\
 \begin{bmatrix} 1 & 2 & 3 \\ 1 & S & T & U \\ 2 & V & W & X \\ 3 & Y & Z & * \end{bmatrix}
 \end{array}$$

The given value for a character is expressed as a coordinate in the order (*Layer, Row, Column*). For example, $A(1, 1, 1), B(1, 1, 2), \dots, Z(3, 3, 2), *(3, 3, 3)$. We define q as the fidelity or complexity of a cipher*. For demonstration purposes let us encipher the word *PROBLEM* using the classification of characters above when $q = 3$.

	<i>P</i>	<i>R</i>	<i>O</i>	<i>B</i>	<i>L</i>	<i>E</i>	<i>M</i>
<i>Layer</i>	2	2	2	1	2	1	2
<i>Row</i>	3	3	2	1	1	2	2
<i>Column</i>	1	3	3	2	3	2	1

We read across the *Layer* values grouping the digits into coordinates of length q , in this case 3. So first we get (2, 2, 2), and then (1, 2, 1). When we reach the end of a line and we have less than q values remaining, we merely wrap-around to the beginning of the next row. For example, after (2, 2, 2), (1, 2, 1) would follow (2, 3, 3), (2, 1, 1), (2, 2, 1), (3, 3, 2), and (3, 2, 1). We always end up with complete groupings since it is obvious that $[(length\ of\ text) \cdot q] \equiv 0 \pmod{q}$ ** . The values are accompanied with labels below, denoting where they came from. For example, P_l denotes the layer value for P, M_r is the row value for M, &c.

$$\begin{array}{ccccccc}
 2_{P_l} & 1_{B_l} & 2_{M_l} & 2_{O_r} & 2_{E_r} & 3_{R_c} & 3_{L_c} \\
 2_{R_l} & 2_{L_l} & 3_{P_r} & 1_{B_r} & 2_{M_r} & 3_{O_c} & 2_{E_c} \\
 2_{O_l} & 1_{E_l} & 3_{R_r} & 1_{L_r} & 1_{P_c} & 2_{B_c} & 1_{M_c}
 \end{array}$$

Just as before, we find the corresponding letter representations for the new array of elements—i.e., (2, 2, 2) → *N*, (1, 2, 1) → *D*, and so forth. The final encryption process yields

$$\begin{bmatrix} P & R & O & B & L & E & M \\ 2 & 2 & 2 & 1 & 2 & 1 & 2 \\ 3 & 3 & 2 & 1 & 1 & 2 & 2 \\ 1 & 3 & 3 & 2 & 3 & 2 & 1 \end{bmatrix}
 \rightarrow
 \begin{bmatrix} N & D & R & J & M & Z & V \\ 2 & 1 & 2 & 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 1 & 2 & 3 & 2 \\ 2 & 1 & 3 & 1 & 1 & 2 & 1 \end{bmatrix}
 \begin{array}{l}
 \text{New Layer Values} \\
 \text{New Row Values} \\
 \text{New Column Values}
 \end{array}
 .$$

The methods used to encrypt bi-fid and tri-fid ciphers are models, and any ciphers with greater q are tackled in the same manner. Obviously, as q increases, the ciphers become more difficult to handle in the absence of computers. This method of encryption is important, however, in the explanation of materials to come. In effect, we seek a mathematical way of expressing the encryption process. Furthermore, we will investigate the cyclic nature of the encryption process—i.e., how several encryptions lead back to the original text.

* From this point on, q will be the general variable used to denote the fidelity (or complexity) of a cipher. For more information on the restrictions regarding q , refer to APPENDIX A.

** This is simply the total number of elements in the array of numbers given for *PROBLEM*.

§2 – THE ENCRYPTION ALGORITHM

The encryption process can be generalized for any text of length ℓ and complexity, q . That is, given any message of length ℓ and the value of q , we construct a set of rules—an *algorithm*—to lead through the encryption process step by step. The x labels are of the form $x_{row, column}$.

Encryption Algorithm.

$$\text{Given } \begin{bmatrix} X_1 & X_2 & X_3 & \cdots & X_\ell \\ x_{1,1} & x_{1,2} & x_{1,3} & \cdots & x_{1,\ell} \\ x_{2,1} & x_{2,2} & x_{2,3} & \cdots & x_{2,\ell} \\ x_{3,1} & x_{3,2} & x_{3,3} & \cdots & x_{3,\ell} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{q,1} & x_{q,2} & x_{q,3} & \cdots & x_{q,\ell} \end{bmatrix}$$

- (I) Note the value of q . From the first row of x 's, select the first q elements— $x_{1,1}, x_{1,2}, x_{1,3}, \dots, x_{1,q}$. In the event $q > \ell$, when you reach the end of the first row, return to the left hand column and select the remaining $(q - \ell)$ elements from the second row.

$$\text{When } q < \ell \begin{bmatrix} X'_1 & X'_2 & X'_3 & \cdots & X'_\ell \\ x_{1,1} & x_{1,q+1} & x_{2,2q-\ell+1} & \cdots & \vdots \\ x_{1,2} & \vdots & \vdots & \cdots & x_{q,\ell-3} \\ x_{1,3} & x_{1,\ell} & x_{2,\ell} & \vdots & x_{q,\ell-2} \\ \vdots & x_{2,1} & x_{3,1} & \vdots & x_{q,\ell-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{1,q} & x_{2,2q-\ell} & x_{3,3q-2\ell} & \cdots & x_{q,\ell} \end{bmatrix}$$

- (II) Continue across the rows of the original matrix, advancing to the beginning of the next row when you reach the end of a row.
- (III) Place the elements of the new matrix in the same order as they are encountered in the original matrix. However, place these elements vertically such that the matrix holds its original dimensions. In other words, when you reach the bottom of a column—whose height should still be q —wrap to the top of the next column and continue.
- (IV) The final product should be a matrix with q rows and ℓ columns. Note that the elements $x_{1,1}$ and $x_{q,\ell}$ held their positions in the new matrix.
- (V) Upon completion of the encrypted matrix, the new X values (denoted by X') should be determined. The X' values are the encrypted message. Decryption of an encrypted message is accomplished by reversing the algorithmic process.

§3 – MATHEMATICAL REPRESENTATION OF ENCRYPTION PROCESS

Trying to express mathematically what one can say in words is no easy task. Moreover, it doesn't always seem possible at first attempt. Take for instance the encryption of *KANSAS* when $q = 2$.

$$\begin{bmatrix} K & A & N & S & A & S \\ 3 & 1 & 3 & 4 & 1 & 4 \\ 1 & 1 & 4 & 4 & 1 & 4 \end{bmatrix}$$

Definition. Carrying out the encryption algorithm one complete time will be henceforth referred to as a *transformation*. The notation used for denoting a *transformation* is the right arrow (\rightarrow).

At first glance, it is hard to imagine how we are going to express mathematically the algorithmic instructions necessary for *transformation*. To begin, though, ignore the reference to the letter representations and focus on the numerical array. The problem is then simplified to finding a way to manipulate the order of elements in a matrix. That is, transforming the matrix from its original form to the encrypted form.

$$\begin{bmatrix} 3 & 1 & 3 & 4 & 1 & 4 \\ 1 & 1 & 4 & 4 & 1 & 4 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 3 & 1 & 1 & 4 & 1 \\ 1 & 4 & 4 & 1 & 4 & 4 \end{bmatrix}.$$

So, in the original matrix (or the encrypted matrix) there are exactly $q\ell$ elements. By expressing the original text as an $q\ell \times 1$ matrix, and defining an $q\ell \times q\ell$ matrix that consists of only 1's and 0's—the transformation matrix—we can express the transformation as

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 1 \\ 1 \\ 1 \\ 3 \\ 4 \\ 4 \\ 4 \\ 1 \\ 4 \\ 4 \\ 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 3 \\ 4 \\ 1 \\ 4 \\ 1 \\ 4 \\ 1 \\ 4 \\ 1 \\ 4 \\ 4 \end{bmatrix}.$$

Note that the 1's in the transformation matrix proceed across by exactly q columns from row to row. There is an exception when the 1 wraps around between the 6th and 7th rows. In this case the 1 jumps $q + 1$ columns. In a similar way, the 1's proceed down by exactly ℓ rows as one goes from column to column. Again, there are exceptions when they must wrap from bottom to top. In this case, the 1 advances $\ell + 1$ rows.

Advancing down the rows, the columns that contain the 1's are, in order, 1, 3, 5, 7, 9, 11, 2, 4, 6, 8, 10, 12. Advancing across the columns from left to right, the rows that contain the 1's are 1, 7, 2, 8, 3, 9, 4, 10, 5, 11, 6, 12. Both sequences are complete residue systems (mod $q\ell$)—in this case (mod 12). So each row and column have **exactly** one position filled by a 1.

§4 – TRANSFORMATIONS & THEIR MATRICES

Definition. A *transformation matrix* is the matrix of 1's and 0's that dictates the placement of the elements in an encrypted matrix. A *transformation matrix* is denoted by \mathcal{T} and has dimensions $q\ell \times q\ell$.

Definition. A *reduced transformation matrix* is the *transformation matrix* with the $q\ell^{\text{th}}$ column and the $q\ell^{\text{th}}$ row removed. We denote the *reduced transformation matrix* by \mathcal{T}' . The dimensions of \mathcal{T}' are $(q\ell - 1) \times (q\ell - 1)$.

***Notes.** *Transformation matrices* have certain properties that are of interest and importance. If given a *transformation matrix*, then:

- (i) Starting from a coordinate of the matrix that contains a 1, movement of q columns to the right, and one row down, should yield a position that also contains a 1. The only exception to this rule occurs when you reach the right edge of the matrix, in which case you must wrap to the left edge and move a total of $q + 1$ columns.
- (ii) Starting from a position of the matrix that contains a 1, movement of ℓ rows down and one column to the right will yield a position that also contains a 1. The only exception to this rule occurs when you reach the bottom edge of the matrix, in which case you must wrap to the top and move a total of $\ell + 1$ rows.
- (iii) For the matrix \mathcal{T}' , notes (i) and (ii) above hold true, disregarding the stated exceptions.
- (iv) By experimentation, it was noted that for every transformation matrix there always exists a minimal power, k^* , such that $\mathcal{T}^k = \mathbf{I}$, where \mathbf{I} is the identity matrix with dimensions $q\ell \times q\ell$.

§5 – CIRCULANT MATRICES & THEIR PROPERTIES

Considering the immense amount of work and abstract explanations to describe the *reduced transformation matrix*, a shortened method of expressing the matrix does exist. It so happens that a reduced transformation matrix fits the definition of what is known as a *circulant matrix*.

Definition. A *circulant matrix* is a matrix with an initial row, say (f_1, f_2, \dots, f_t) , that is shifted to the right (or sometimes the left) a set number of columns, say α , to obtain the next row. For example, given initial row, F , its α -circulant matrix of order t is**

$$F = (f_1, f_2, \dots, f_t)$$

$$\begin{bmatrix} f_1 & f_2 & \cdots & f_t \\ f_{t-\alpha+1} & f_{t-\alpha+2} & \cdots & f_{t-\alpha} \\ f_{t-2\alpha+1} & f_{t-2\alpha+2} & \cdots & f_{t-2\alpha} \\ \vdots & \vdots & & \vdots \\ f_{\alpha+1} & f_{\alpha+2} & \cdots & f_{\alpha} \end{bmatrix}$$

* See APPENDIX B for a table of k values.

** See [2, pp.155-56] for an in-depth explanation of the notation and concepts regarding circulant matrices.

An example easy to understand is the definition of the identity matrix, \mathbf{I} , given in terms of the circulant notation.

$\mathbf{I}_{\beta \times \beta}$ = 1-circulant matrix of order β given initial row $I = (1, 0_1, 0_2, \dots, 0_{\beta-1})$

$$\mathbf{I}_{\beta \times \beta} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \begin{array}{l} \text{Initial Row} \\ I \text{ shifted } 1 \rightarrow \\ I \text{ shifted } 2 \rightarrow \\ \vdots \\ I \text{ shifted } (\beta - 1) \rightarrow \end{array}$$

The reduced transformation matrix, \mathcal{T}' , can be expressed in the circulant matrix notation in the following manner.

$\mathcal{T}'_{(q\ell-1) \times (q\ell-1)}$ = q -circulant matrix of order $(q\ell - 1)$ given initial row $L = (1, 0_1, 0_2, \dots, 0_{(q\ell-1)-1})$

$$\mathcal{T}'_{(q\ell-1) \times (q\ell-1)} = \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & \ddots & 1 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \ddots & 1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots & 0 \end{bmatrix} \begin{array}{l} \text{Initial Row} \\ L \text{ shifted } q \rightarrow \\ L \text{ shifted } 2q \rightarrow \\ \vdots \\ L \text{ shifted } ((q\ell - 1) - 1)q \rightarrow \end{array}$$

In short notation, $\mathcal{T}' = q\text{-circ}(1, 0_1, 0_2, \dots, 0_{(q\ell-1)-1})$.

§6 – THE ORDER, k

It has been stated previously that for every reduced transformation matrix, there exists some minimal k such that $[\mathcal{T}']^k = \mathbf{I}$. The value of k is given in terms of a function $\Theta(q, \ell)$, that is $\Theta(q, \ell) = k$ is defined as the minimal power function.

Definition. If n is a positive integer, we define $\varphi(n)$ to be the number of integers $f, 1 \leq f \leq n$, such that $(n, f) = 1$. The function φ is called the **Euler phi function***.

Definition. Given the congruence $a^k \equiv 1 \pmod{m}$, where $(a, m) = 1$, we define the minimal positive integer value of k that satisfies the congruence as the **order** of $a \pmod{m}$. The value of k always divides $\varphi(m)$.

Lemma 1. Given q and ℓ , then $(q, q\ell - 1) = 1$.

PROOF. If $(q, q\ell - 1) \neq 1$, then this implies there exists some prime, p , such that it divides both q and $(q\ell - 1)$. This would imply $q \equiv 0 \pmod{p}$ and $q\ell - 1 \equiv 0 \pmod{p}$. The last congruence can be rewritten as $q\ell \equiv 1 \pmod{p}$. This can't be possible since $p|q$ by definition, therefore $(q, q\ell - 1) = 1$. \square

Theorem (Euler). If w is a positive integer and if $(x, w) = 1$, then $x^{\varphi(w)} \equiv 1 \pmod{w}$.

PROOF. Define x_1, x_2, \dots, x_n as a reduced residue system \pmod{w} . Since $(x, w) = 1$, then xx_1, xx_2, \dots, xx_n is also a reduced residue system \pmod{w} . It is well known that a reduced residue system \pmod{w} has exactly $\varphi(w)$ elements, obvious by the definition of the φ -function. So we know $n = \varphi(w)$. This gives us

$$\prod_{i=1}^n x_i \equiv \prod_{i=1}^n xx_i \pmod{w}$$

* See APPENDIX C for more information on the Euler φ -function.

Since $(\prod_{i=1}^n x_i, w) = 1$, we can divide both sides of the congruence by $\prod_{i=1}^n x_i$. This leaves us with

$$1 \equiv \prod_{i=1}^n x \pmod{w} \Rightarrow 1 \equiv x^n \pmod{w} \Rightarrow 1 \equiv x^{\varphi(w)} \pmod{w}. \quad \boxtimes$$

Lemma 2. If A is a g -circulant and B is an h -circulant, then AB is a gh -circulant.**

Theorem (k -Value). If a message has length ℓ and complexity q , then the number of transformations necessary to return the original text is given by

$$\Theta(q, \ell) = \mathbf{order} \ q \pmod{q\ell - 1}$$

PROOF. Suppose we define \mathcal{T}' to be the q -circulant matrix of order $(q\ell - 1)$.

$$\mathcal{T}' = q\text{-circ}(1, 0_1, 0_2, \dots, 0_{(q\ell-1)-1})$$

Application of Lemma 2 implies $[\mathcal{T}']^n$ is a $q^n \pmod{q\ell - 1}$ -circulant matrix. To return the original text, we are looking for the minimal positive power of q that gives a 1-circulant matrix—namely the identity matrix, \mathbf{I} . By Lemma 1 we know $(q, q\ell - 1) = 1$. We can then apply Euler's theorem to show that there always exists some value to satisfy $q^k \equiv 1 \pmod{q\ell - 1}$, namely $\varphi(q\ell - 1)$. Sometimes, however, there exists a $k < \varphi(q\ell - 1)$, $k | \varphi(q\ell - 1)$, such that $q^k \equiv 1 \pmod{q\ell - 1}$. This value is defined above and is the **order** of $q \pmod{q\ell - 1}$. Therefore $[\mathcal{T}']^k = \mathbf{I}$ when $k = \mathbf{order} \ q \pmod{q\ell - 1}$. \boxtimes

Corollary. If a message has length ℓ and complexity q , then the number of transformations necessary to return the original text is given by

$$\Theta(q, \ell) = \mathbf{order} \ \ell \pmod{q\ell - 1}$$

PROOF. Suppose we define \mathcal{P} to be the ℓ -vertical-circulant matrix of order $(q\ell - 1)$.

$$\mathcal{P} = \ell\text{-vcirc}(1, 0_1, 0_2, \dots, 0_{(q\ell-1)-1})$$

Application of Lemma 2 implies \mathcal{P}^n is a $\ell^n \pmod{q\ell - 1}$ -vcirculant matrix. To return the original text, we are looking for the minimal positive power of ℓ that gives a 1-circulant matrix—namely the identity matrix, \mathbf{I} . By Lemma 1 we know $(\ell, q\ell - 1) = 1$. We can then apply Euler's theorem to show that there always exists some value to satisfy $\ell^k \equiv 1 \pmod{q\ell - 1}$, namely $\varphi(q\ell - 1)$. Sometimes, however, there exists a $k < \varphi(q\ell - 1)$, $k | \varphi(q\ell - 1)$, such that $\ell^k \equiv 1 \pmod{q\ell - 1}$. This value is defined as the **order** of $\ell \pmod{q\ell - 1}$. Therefore $\mathcal{P}^k = \mathbf{I}$ when $k = \mathbf{order} \ \ell \pmod{q\ell - 1}$. \boxtimes

Remark: Since the k defined in the k -Value Theorem and the Corollary are both minimal, they are also therefore equal. See direct proof of (3) below.

Implications of the k -Value Theorem.

- (1) For a given \mathcal{T}' , $[\mathcal{T}']^{\varphi(q\ell-1)} = \mathbf{I}$.
- (2) For a given \mathcal{P} , $\mathcal{P}^{\varphi(q\ell-1)} = \mathbf{I}$.
- (3) For any q and ℓ both ≥ 2 , $\mathbf{order} \ q \pmod{q\ell - 1} = \mathbf{order} \ \ell \pmod{q\ell - 1}$. That is, for $q^x \equiv 1 \pmod{q\ell - 1}$ and $\ell^y \equiv 1 \pmod{q\ell - 1}$, the minimal positive x and y such that the congruences hold true are equal.
- (4) By (3), it is true that $\Theta(q, \ell) = \Theta(\ell, q)$.
- (5) Given any $q = \ell$ such that $q, \ell > 1$ then $\Theta(q, \ell) = 2$. This is merely solving the congruence $q^k \equiv 1 \pmod{q^2 - 1}$. This is equivalent to $q^k - 1 \equiv 0 \pmod{q^2 - 1}$. By inspection the obvious minimal positive solution is $k = 2$.

** For a PROOF see: [2, p.159, Theorem 5.1.2].

There are some interesting implications, especially of (3). By (3), given any two numbers both ≥ 2 , their orders are equivalent (mod their product minus one). For example, given 13 and 17, $13^x \equiv 1 \pmod{220}$ and $17^y \equiv 1 \pmod{220}$, we know that $x = y = 20$ is the minimal solution for x and y —the **order** of 13 and 17 (mod 220).

Direct PROOF of (3):

We are trying to prove that $q^x \equiv 1 \pmod{q\ell - 1} \Rightarrow \ell^x \equiv 1 \pmod{q\ell - 1}$. We know that $q\ell \equiv 1 \pmod{q\ell - 1}$. Therefore we know $(q\ell)^x \equiv 1 \pmod{q\ell - 1} \Rightarrow q^x \cdot \ell^x \equiv 1 \pmod{q\ell - 1}$. This last congruence goes to $\ell^x \equiv 1 \pmod{q\ell - 1}$ since $q^x \equiv 1 \pmod{q\ell - 1}$ by definition. \square

§7 – MULTI-REFERENCE CIPHERS

The possible variations when dealing with matrix ciphers are innumerable. To increase the difficulty of a cipher it is possible to do more than just increase the value of q . Consider the following matrices:

$$\left(\begin{array}{c} \begin{bmatrix} A & B & C & D & E \\ F & G & H & I & J \\ K & L & M & N & O \\ P & Q & R & S & T \\ U & V & W & X & Y/Z \end{bmatrix} \quad \begin{bmatrix} F & G & H & I & J \\ K & L & M & N & O \\ P & Q & R & S & T \\ U & V & W & X & Y/Z \\ A & B & C & D & E \end{bmatrix} \\ \\ \begin{bmatrix} K & L & M & N & O \\ P & Q & R & S & T \\ U & V & W & X & Y/Z \\ A & B & C & D & E \\ F & G & H & I & J \end{bmatrix} \quad \begin{bmatrix} P & Q & R & S & T \\ U & V & W & X & Y/Z \\ A & B & C & D & E \\ F & G & H & I & J \\ K & L & M & N & O \end{bmatrix} \end{array} \right)$$

We have created a matrix of matrices. The coordinates of each letter are now given in the form of two ordered pairs. The first of the ordered pairs indicates which 5×5 matrix the character is in. For instance a first ordered pair of (1, 2) refers to the right matrix in the top row. The second ordered pair refers to the (row, column) where the letter is located. Since each letter of the alphabet occurs four times, there are four possible references for each letter. For example, the letter “X” has the following references—[(1, 1)-(5, 4)], [(1, 2)-(4, 4)], [(2, 1)-(3, 4)], [(2, 2)-(2, 4)]. Let us encrypt *WILDCAT* as in §1 using the new matrices above. We will vary the matrix that we use to encrypt.

	<i>W</i>	<i>I</i>	<i>L</i>	<i>D</i>	<i>C</i>	<i>A</i>	<i>T</i>		<i>X</i>	<i>K</i>	<i>Z</i>	<i>W</i>	<i>B</i>	<i>W</i>	<i>O</i>
<i>Cipher Row</i>	1	2	1	1	2	1	1		1	1	2	1	2	1	2
<i>Cipher Column</i>	2	2	1	1	2	2	1	→	2	1	1	2	1	2	1
5×5 Row	4	4	3	1	3	5	4		4	3	3	4	4	4	1
5×5 Column	3	4	2	4	3	1	5		4	1	5	3	2	3	5

Note that the top two rows (the *Cipher* references), and the bottom two rows (the references within the 5×5 matrix) are transformed independent of one another. In other words, enciphering *WILDCAT* would actually be equivalent to transforming two separate matrices and piecing them back together to give the two ordered pair references.

$$\begin{array}{l} \begin{array}{l} \textit{Cipher Row} \\ \textit{Cipher Column} \end{array} \begin{bmatrix} 1 & 2 & 1 & 1 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 2 & 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 2 & 1 & 2 & 1 \end{bmatrix} \\ \\ \begin{array}{l} 5 \times 5 \textit{ Row} \\ 5 \times 5 \textit{ Column} \end{array} \begin{bmatrix} 4 & 4 & 3 & 1 & 3 & 5 & 4 \\ 3 & 4 & 2 & 4 & 3 & 1 & 5 \end{bmatrix} \rightarrow \begin{bmatrix} 4 & 3 & 3 & 4 & 4 & 4 & 1 \\ 4 & 1 & 5 & 3 & 2 & 3 & 5 \end{bmatrix} \end{array}$$

One might note, that given the encrypted text “*XKZWBWO*” in the previous example, it is next to impossible for someone to decrypt the text, unless given both the matrix key and the numerical array of references $\begin{bmatrix} 1 & 1 & 2 & 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 2 & 1 & 2 & 1 \end{bmatrix}$. This array of numbers allows the receiver to determine which particular matrix was used to encipher each letter. In general, if one chooses a key that doesn’t repeat letters, it is significantly simpler to decipher any given text without any further assistance other than the key.

Theorem (Multi-Reference Cipher). Given a multi-reference cipher with n fidelities, q_1, q_2, \dots, q_n , then the original text of length ℓ can be recovered only after t transformations, where t equals the least common multiple of $\Theta(q_1, \ell), \Theta(q_2, \ell), \dots, \Theta(q_n, \ell)$.

PROOF. For each independent i^{th} part of the encryption process, exactly $\Theta(q_i, \ell)$ transformations are required to return to the original array of numbers. If for the values $1, 2, \dots, n$ there is some $q_i \neq q_j, 1 \leq i, j \leq n$, then $\Theta(q_i, \ell) \neq \Theta(q_j, \ell)$. In other words, the j^{th} part requires a number of transformations different from the i^{th} part to return it to its original array of values. Clearly, then, it is necessary to continue transformation until one reaches the least common multiple of all $\Theta(q_i, \ell), i = 1, 2, \dots, n$. \square

The possibilities are boundless for layering ciphers within ciphers, and thus matrices within matrices. One could continue in the manner above *ad infinitum*, however, the greater the number of q ’s, and the greater the value of each q , the more difficult it is to make sense of anything without the assistance of computers and other machinery. For obvious reasons, room does not permit an in depth investigation or explanation of such complex and mathematically daunting ciphers.

§8 – PERMUTATION MATRIX CIPHERS

Consider again the standard 5×5 bi-fid cipher matrix given in §1.

$$\begin{bmatrix} A & B & C & D & E \\ F & G & H & I & J \\ K & L & M & N & O \\ P & Q & R & S & T \\ U & V & W & X & Y/Z \end{bmatrix}$$

Suppose we want to encipher the text *WILDCAT*, but this time we don’t follow the encryption algorithm in §2. Instead we construct an α -circulant permutation matrix with dimensions $q\ell \times q\ell$. The value of α can vary as long as $(\alpha, q\ell) = 1$ and $1 \leq \alpha < q\ell$. For $\alpha > q\ell$, we merely consider the $\alpha \pmod{q\ell}$ -circulant matrix (which is identical to the α -circulant matrix). For varying α , the encrypted message also varies. For example, encrypting *WILDCAT* when $\alpha = 3$, we get the following:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 3 \\ 2 \\ 4 \\ 3 \\ 2 \\ 1 \\ 4 \\ 1 \\ 3 \\ 1 \\ 3 \\ 4 \\ 5 \\ 1 \\ 2 \\ 1 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \\ 1 \\ 3 \\ 4 \\ 3 \\ 3 \\ 4 \\ 1 \\ 4 \\ 1 \\ 5 \\ 2 \\ 1 \\ 2 \\ 1 \\ 4 \\ 1 \\ 1 \end{bmatrix}$$

This large circulant matrix transformation can be written in shortened form as

$$\begin{bmatrix} W & I & L & D & C & A & T \\ 5 & 2 & 3 & 1 & 1 & 1 & 4 \\ 3 & 4 & 2 & 4 & 3 & 1 & 5 \end{bmatrix} \xrightarrow{(3\text{-circ})} \begin{bmatrix} X & C & R & N & E & G & A \\ 5 & 1 & 4 & 3 & 1 & 2 & 1 \\ 4 & 3 & 3 & 4 & 5 & 2 & 1 \end{bmatrix}$$

To avoid confusion with the standard transformation procedure, we place an indicator over the right arrow. In the example above, it is noted that the transformation is a (3-circ) transformation, **not** the encryption algorithm transformation. If we define $\{x_1, x_2, \dots, x_{q\ell}\}$ as any complete residue system (mod $q\ell$), when $(\alpha, q\ell) = 1$, then $\{\alpha x_1, \alpha x_2, \dots, \alpha x_{q\ell}\}$ is also a complete residue system (mod $q\ell$). This means each column of a $q\ell \times q\ell$ matrix will contain only one 1 if an α -circulant matrix is formed given initial row $L = (1, 0_1, 0_2, \dots, 0_{q\ell-1})$.

For *WILDCAT*, an α value of 4 is not allowed since $(4, 14) = 2 \neq 1$. However $\alpha = 5$ is permissible. Below are the different transformations for $\alpha = 5, 9, 11$, and 13.

$$\begin{array}{l} \begin{bmatrix} W & I & L & D & C & A & T \\ 5 & 2 & 3 & 1 & 1 & 1 & 4 \\ 3 & 4 & 2 & 4 & 3 & 1 & 5 \end{bmatrix} \xrightarrow{(5\text{-circ})} \begin{bmatrix} V & C & A & I & S & E & M \\ 5 & 1 & 1 & 2 & 4 & 1 & 3 \\ 2 & 3 & 1 & 4 & 4 & 5 & 3 \end{bmatrix} \\ \xrightarrow{(9\text{-circ})} \begin{bmatrix} W & O & D & S & F & C & B \\ 5 & 3 & 1 & 4 & 2 & 1 & 1 \\ 3 & 5 & 4 & 4 & 1 & 3 & 2 \end{bmatrix} \\ \xrightarrow{(11\text{-circ})} \begin{bmatrix} U & B & J & D & M & R & D \\ 5 & 1 & 2 & 1 & 3 & 4 & 1 \\ 1 & 2 & 5 & 4 & 3 & 3 & 4 \end{bmatrix} \\ \xrightarrow{(13\text{-circ})} \begin{bmatrix} Z & P & C & D & B & N & H \\ 5 & 4 & 1 & 1 & 1 & 3 & 2 \\ 5 & 1 & 3 & 4 & 2 & 4 & 3 \end{bmatrix} \end{array}$$

In general, we know that $\varphi(n)$ is defined as the number of integers f , such that $1 \leq f \leq n$ and $(f, n) = 1$. For any given $q\ell$, there exists exactly $\varphi(q\ell)$ valid values for α that are by definition relatively prime to $q\ell$. However, this includes the valid value of 1 for α . When $\alpha = 1$ we simply have the identity matrix, and the encrypted text is equivalent to the original text. Therefore, there are $\varphi(q\ell) - 1$ values for α that give an encrypted message that differs from the original text. For our example, $q\ell = 14$. Since $\varphi(14) = \varphi(2)\varphi(7) = (2 - 1)(7 - 1) = 6$, we know there are $(\varphi(14) - 1) = 5$ different ways of encrypting *WILDCAT* using α -circulant matrices. All encryptions are given above.

By the same logic as was presented for the original encryption algorithm, for the α -circulant permutation matrix cipher, if one encrypts a message of length ℓ and fidelity q , then after k encryptions the original message will be restored. In this case, $k = \mathbf{order}$ of $\alpha \pmod{q\ell}$.

In the case above, in order for someone receiving the message to decipher it, it would be required that the sender also include a value for α . For example, the word *WILDCAT* could be sent in encrypted form to someone by sending the string “*VCAISEM(5)*”. To complicate matters an entire sentence could be sent such that each word was accompanied by an α value. Of course this α value would have to be relatively prime to the specific value of $q\ell$ for each word as well. In this manner one could send an entire message changing the circulant matrix used to encrypt each word.

Another way of looking at an α -circulant transformation is to consider the matrix for any given text string. Write the matrix such that each element has its own unique subscript from 0 to $(q\ell - 1)$, thus there are

$q\ell$ elements. We assign subscripts such that each column contains a set of subscripts that are a complete residue system (mod q) and each row contains a set of subscripts that are a complete residue system (mod ℓ).

$$\begin{bmatrix} a_0 & a_q & a_{2q} & \cdots & a_{(\ell-1)q} \\ a_1 & a_{q+1} & a_{2q+1} & \cdots & a_{(\ell-1)q+1} \\ a_2 & a_{q+2} & a_{2q+2} & \cdots & a_{(\ell-1)q+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{q-1} & a_{2q-1} & a_{3q-1} & \cdots & a_{\ell q-1} \end{bmatrix}$$

After we describe any matrix of values with fidelity q and length ℓ by using a matrix like that above, it is very simple to characterize an α -circulant transformation. Each subscript is merely multiplied by α and reduced (mod $q\ell$) to get the new value of each position. Since α is relatively prime to $q\ell$, then if $\{x_1, x_2, \dots, x_{q\ell}\}$ is any complete residue system (mod $q\ell$), then $\{\alpha x_1, \alpha x_2, \dots, \alpha x_{q\ell}\}$ is also a complete residue system (mod $q\ell$) thus each old subscript will reappear in the new matrix only once, but will be permuted by the α -circulant permutation matrix. Remember, it is important each new subscript is reduced (mod $q\ell$) to make any sense.

$$\begin{bmatrix} a_0 & a_q & a_{2q} & \cdots & a_{(\ell-1)q} \\ a_1 & a_{q+1} & a_{2q+1} & \cdots & a_{(\ell-1)q+1} \\ a_2 & a_{q+2} & a_{2q+2} & \cdots & a_{(\ell-1)q+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{q-1} & a_{2q-1} & a_{3q-1} & \cdots & a_{\ell q-1} \end{bmatrix} \xrightarrow{(\alpha\text{-circ})} \begin{bmatrix} a_0 & a_{q\alpha} & a_{2q\alpha} & \cdots & a_{(\ell-1)q\alpha} \\ a_\alpha & a_{(q+1)\alpha} & a_{(2q+1)\alpha} & \cdots & a_{((\ell-1)q+1)\alpha} \\ a_{2\alpha} & a_{(q+2)\alpha} & a_{(2q+2)\alpha} & \cdots & a_{((\ell-1)q+2)\alpha} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{(q-1)\alpha} & a_{(2q-1)\alpha} & a_{(3q-1)\alpha} & \cdots & a_{(\ell q-1)\alpha} \end{bmatrix}$$

As a demonstration of this process, let us encrypt the message “*SENDMONEY*” using a fidelity $q = 3$. In this case $\ell = 9$, thus $q\ell = 27$. We chose any α relatively prime to 27, say 7, and proceed with the transformation. Our character references for $q = 3$ are the same as those used in §1 on page 2.

$$\begin{bmatrix} S & E & N & D & M & O & N & E & Y \\ (3)_0 & (1)_3 & (2)_6 & (1)_9 & (2)_{12} & (2)_{15} & (2)_{18} & (1)_{21} & (3)_{24} \\ (1)_1 & (2)_4 & (2)_7 & (2)_{10} & (2)_{13} & (2)_{16} & (2)_{19} & (2)_{22} & (3)_{25} \\ (1)_2 & (2)_5 & (2)_8 & (1)_{11} & (1)_{14} & (3)_{17} & (2)_{20} & (2)_{23} & (1)_{26} \end{bmatrix}$$

extract subscripts

↓

$$\begin{bmatrix} 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \\ 1 & 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 \\ 2 & 5 & 8 & 11 & 14 & 17 & 20 & 23 & 26 \end{bmatrix}$$

multiply the subscripts through by α and reduce (mod $q\ell$)

↓

$$\begin{bmatrix} 0 & 21 & 42 & 63 & 84 & 105 & 126 & 147 & 168 \\ 7 & 28 & 49 & 70 & 91 & 112 & 133 & 154 & 175 \\ 14 & 35 & 56 & 77 & 98 & 119 & 140 & 161 & 182 \end{bmatrix} \quad \begin{bmatrix} 0 & 21 & 15 & 9 & 3 & 24 & 18 & 12 & 6 \\ 7 & 1 & 22 & 16 & 10 & 4 & 25 & 19 & 13 \\ 14 & 8 & 2 & 23 & 17 & 11 & 5 & 26 & 20 \end{bmatrix}$$

reconstruct the matrix, placing the original values in their new locations based on subscripts

↓

$$\begin{bmatrix} V & B & M & E & F & V & Q & M & N \\ (3)_0 & (1)_{21} & (2)_{15} & (1)_9 & (1)_3 & (3)_{24} & (2)_{18} & (2)_{12} & (2)_6 \\ (2)_7 & (1)_1 & (2)_{22} & (2)_{16} & (2)_{10} & (2)_4 & (3)_{25} & (2)_{19} & (2)_{13} \\ (1)_{14} & (2)_8 & (1)_2 & (2)_{23} & (3)_{17} & (1)_{11} & (2)_5 & (1)_{26} & (2)_{20} \end{bmatrix}$$

Many of the aspects of matrix ciphers already discussed are specific and interesting cases of their more general underlying structure. There are several things that can be said about matrix ciphers in general, without regard to their internal structural basis.

Definition. Suppose we are given the set $\mathcal{Q} = \{i_1, i_2, \dots, i_r\}$ where i_j is any distinct integer and $1 \leq i_j \leq n$. Any permutation of these integers can be viewed as a remapping. For example, assume i_1 maps to i_3 , i_3 maps to i_5 , and i_5 maps back to i_1 . At the same time, assume i_2 maps to i_4 which in turn maps to i_6 and back to i_2 . We can denote this systematically as

$$\begin{array}{l} \text{Initial values} \\ \text{Remapped values} \end{array} \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & i_6 \\ i_3 & i_4 & i_5 & i_6 & i_1 & i_2 \end{pmatrix}$$

We define these independent mappings—namely the (1 to 3 to 5) and (2 to 4 to 6)—as *cycles**.

Lemma (Permutation Cycles). Given any arbitrary permutation matrix, \mathcal{R} , there exist internal “cycles” associated with the matrix.

PROOF. Assume that the 1 in the first column resides in the n^{th} row. Then, the 1 can be given an ordered pair (*row, column*) such that the first would always be $(n, 1)$. Thought of in terms of the definition of a cycle, we say n is mapped on 1. From there we can say 1 is mapped to a , and a is then mapped to b , etc., etc. We continue in this fashion until we return to the starting coordinate. For example, $\{(n, 1), (1, a), (a, b), (b, c), \dots, (\gamma, n), (n, 1)\}$. This remapping creates a chain or “cycle” of substitution within the matrix. \square

Many times there are many sub-chains associated with one permutation matrix. These are obtained by starting in the first column, finding the first sub-chain, and then beginning the process over with the 1 furthest to the left that has not yet been referenced.

Example. We are given \mathcal{R} .

$$\mathcal{R} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

We start at the left column and write down the coordinate of the first 1, $(3, 1)$. This means 3 maps onto 1, and then we find that 1 maps onto 3, so the sub-chain has two distinct elements, $\{(3, 1), (1, 3)\}$. We have used the 1 in the first column so we go to the 1 in the second column. We get $\{(4, 2), (2, 6), (6, 4)\}$ and this sub-chain consists of three distinct elements. The only 1 that remains is that in the fifth column, $\{(5, 5)\}$. It maps onto itself, so this sub-chain consists of one distinct element. This particular permutation matrix consists of three sub-chains— $\{(3, 1), (1, 3)\}$, $\{(4, 2), (2, 6), (6, 4)\}$, $\{(5, 5)\}$ —of length two, three, and one, respectively. We will denote the length of the i^{th} sub-chain of a permutation matrix by λ_i . In our example, $\lambda_1 = 2$, $\lambda_2 = 3$, $\lambda_3 = 1$.

Theorem (Generalization 1). Given \mathcal{R} , as defined in the Lemma above, there always exists a k such that $\mathcal{R}^k = \mathbf{I}$.

PROOF. Every permutation matrix can be broken down into its respective sub-chains as given in the Lemma above. By defining the sub-chains, a row of a matrix with a 1 in the f^{th} column will eventually be mapped onto the f^{th} row, thus making this particular row of the matrix coincide with the identity matrix of the

* See [3, p.86, Lemma 1] for a complete proof and explanation.

same dimensions. If every row of the given permutation matrix \mathcal{R} is expected to coincide with \mathbf{I} , then the least instance where this occurs is when k is equal to the least common multiple of $\lambda_1, \lambda_2, \dots, \lambda_t$ where t is the number of sub-chains of \mathcal{R} and λ_i is the length of the i^{th} sub-chain. \square

Remark: In the example above, the least common multiple of λ_1, λ_2 , and λ_3 is 6, thus $\mathcal{R}^6 = \mathbf{I}$.

Definition. We define \mathcal{S} as the set of all $q\ell \times 1$ matrices, such that each element $\delta_i, i = 1, 2, \dots, q\ell$, is allowed to range from 1 to some upper value, s . Assume we are also given some arbitrary $q\ell \times 1$ matrix of values to encrypt that we call \mathcal{A}_0 . If $f : \mathcal{S} \rightarrow \mathcal{S}$ is a 1-to-1 function, we call f a 1-to-1 cipher method. Therefore, any $q\ell \times 1$ matrix \mathcal{A}_i , is *uniquely* encrypted by f such that $f(\mathcal{A}_i) = \mathcal{A}_{i+1}$. Likewise, any matrix \mathcal{A}_{i+1} is uniquely decrypted by what we will call the inverse cipher method function, f^{-1} , such that $f^{-1}(\mathcal{A}_{i+1}) = \mathcal{A}_i$. Note that given the restrictions on the element values for some matrix \mathcal{A} , there are only a finite number of possibilities for the encrypted matrix—maximally there are $s^{q\ell}$ possible matrices where each element, δ_i , falls within the range $1 \leq \delta_i \leq s$ for $i = 1, 2, \dots, q\ell$.

Theorem (Generalization 2). Given any 1-to-1 cipher method, iterated encryptions will always return the original text.

PROOF. Suppose \mathcal{A}_0 is encrypted to \mathcal{A}_1 by some valid 1-to-1 cipher method function f . In turn, $\mathcal{A}_1 \rightarrow \mathcal{A}_2 \rightarrow \dots \rightarrow \mathcal{A}_i \rightarrow \mathcal{A}_{i+1} \rightarrow \dots$ where i is the minimal index where a string, $\mathcal{A}_j, 0 \leq j < i$, is repeated. We know \mathcal{A}_1 can only come from the encryption of \mathcal{A}_0 , \mathcal{A}_2 can only come from the encryption of \mathcal{A}_1 , \dots \mathcal{A}_i can only come from the encryption of \mathcal{A}_{i-1} , etc. Assume j is greater than 0. Because \mathcal{A}_j and \mathcal{A}_i can only come from \mathcal{A}_{j-1} and \mathcal{A}_{i-1} respectively, then $\mathcal{A}_{j-1} = \mathcal{A}_{i-1}$. This is a contradiction of the minimality of i since $(i-1)$ is also a repeated index. By this contradiction, we know that j must then equal 0, that is $\mathcal{A}_j = \mathcal{A}_0 = \mathcal{A}_i$. Therefore, not only does the initial text repeat, but it must repeat before any other encryption. \square

RESTRICTIONS WHEN BUILDING A q -fidelity CIPHER.

When building matrices on which ciphers will be based, one must take many things into consideration. First, the value of q refers **only** to the number of coordinates for each character. For example, in the bi-fid cipher each character was denoted by two coordinates—in our example $A(1, 1), B(1, 2), \dots, Y/Z(5, 5)$. However, one is by no means limited to a 5×5 bi-fid cipher. One could just as easily have a 16×16 matrix of characters. In this manner the entire character set for a standard computer could be included in the set of possible characters. Even though the dimensions of the matrix are increased, each character is still only given by two coordinates, thus $q = 2$.

When $q = 3$ there are innumerable ways to define the system of matrices. Since $q = 3$ it is obvious there must be three coordinates for each character. If we define the three coordinates as (*Layer, Column, Row*), then certain restrictions are placed on the number of layers, columns, and rows. Most importantly, the number of layers must equal the number of columns and rows in each layer. A valid example of a cipher when $q = 3$ is the 2-layer, 2×2 matrix cipher.

$$1^{st} \text{ Layer } \begin{bmatrix} & 1 & 2 \\ 1 & A & B \\ 2 & C & D \end{bmatrix} \quad 2^{nd} \text{ Layer } \begin{bmatrix} & 1 & 2 \\ 1 & E & F \\ 2 & G & H \end{bmatrix}$$

Clearly, for a setup like that above it would be difficult to make any sensible encrypted message. However, when you increase the number of layers, it is quite possible to create a useful and difficult cipher. Consider when $q = 4$ and we have 3 dimensions, each containing 3 layers, and each layer in turn consisting of a 3×3 matrix of characters. Let us refer to the coordinates in a $q = 4$ cipher as (*Dimension, Layer, Column, Row*). One of the three dimensions for our example is given below.

$$1^{st} \text{ Dimension } \left(\begin{array}{c} \begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix} \quad \begin{bmatrix} J & K & L \\ M & N & O \\ P & Q & R \end{bmatrix} \\ \begin{bmatrix} S & T & U \\ V & W & X \\ Y & Z & * \end{bmatrix} \end{array} \right)$$

The other two dimensions for this particular $q = 4$ cipher are constructed in the same manner. It is standard practice to either fill the other dimensions with different characters, or to permute the first dimension to create the others. For encryption to be possible, it is necessary that all 3 dimensions be defined. If the coordinates of a particular character are given by (a, b, c, d) , then it is necessary that all possible values of a, b, c , and d are defined. If the value of one coordinate is undefined for another coordinate, when transformation is completed a position may contain a value not allowed. In the example given above there are restrictions on the possible values for the coordinates, namely $1 \leq a, b, c, d \leq 3$. Assume for demonstration purposes that we allowed only 2 dimensions but still had 3 layers each consisting of 3×3 matrices. What if after transformation some new dimension value is taken from an old layer, column, or row value and is greater than 2? In our encrypted message we would have an undefined dimension, and therefore there would be no character for this coordinate reference.

For each possible value of q it is important to remember that the number of layers, rows, columns, etc., can be varied in any way desired. It is only integral that q be equal to the number of coordinates given for each character. Thus, if $q = 5$, every character must be given in the form (a, b, c, d, e) . It is necessary, however, that whatever value, say n , one chooses for layers, rows, etc., all coordinates be allowed to run the entire gamut from 1 to n . That is, the values $1 \leq a, b, c, d, e \leq n$ must be valid references.

TABLE OF k VALUES FOR A GIVEN $q \times \ell$ MATRIX.

		$q \rightarrow$						
		1	2	3	4	5	6	7
ℓ	1	1	1	1	1	1	1	1
	2	1	2	4	3	6	10	12
\downarrow	3	1	4	2	5	6	16	4
	4	1	3	5	2	9	11	9
	5	1	6	6	9	2	14	16
	6	1	10	16	11	14	2	40
	7	1	12	4	9	16	40	2

The table is read by finding the q and ℓ values and following them across and down to their intersection. We define $\Theta(q, \ell)$ as the function that gives the k value for a given matrix. Then, for example, $\Theta(3, 4) = 5$.

FINDING k FOR A GIVEN $q \times \ell$ MATRIX.

Given any $q, \ell \geq 2$ such that $q \neq \ell$, the process is quite straightforward for computing $\Theta(q, \ell)$ with the assistance of a hand-held calculator. Using the previous example from page 8, with $q = 13, \ell = 17$, the process is carried out as follows:

- (i) Compute $(q\ell - 1)$. In our case $13 \cdot 17 - 1 = 220$.
- (ii) Compute $\varphi(q\ell - 1)$ using the formula given for $\varphi(n)$ in APPENDIX C. For our case, $\varphi(220) = \varphi(2^2 \cdot 5 \cdot 11) = \varphi(2^2)\varphi(5)\varphi(11) = (2 - 1)2 \cdot 4 \cdot 10 = 80$.
- (iii) Write out the factors of $\varphi(q\ell - 1)$. In our case $\varphi(q\ell - 1) = 80$, so we list the factors of 80, the set \mathbf{F} , as $\mathbf{F} = \{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$.
- (iv) We are now looking for the minimal element k of set \mathbf{F} , such that $q^k \equiv 1 \pmod{q\ell - 1}$. In other words, for the example above you test all values in \mathbf{F} , starting from the smallest element, until the congruence $13^k \equiv 1 \pmod{220}$ holds true. For $k = 1, 2$ the congruence is obviously false. For $k = 4$, we have $13^4 = 28561 \equiv 181 \pmod{220}$ so it is false. For $k = 5$, $13^5 = 371293 \equiv 153 \pmod{220}$, $k = 8$ yields $13^8 = (13^4)^2 \equiv 181^2 \pmod{220} \equiv 201 \pmod{220}$, $k = 10$ gives $13^{10} = (13^5)^2 \equiv 153^2 \pmod{220} \equiv 89 \pmod{220}$, $k = 20$ returns $13^{20} = (13^{10})^2 \equiv 89^2 \pmod{220} \equiv 1 \pmod{220}$. Therefore $k = 20$ is the minimal element in set \mathbf{F} that solves the congruence $13^k \equiv 1 \pmod{220}$. Notice that this agrees with the **order** of $13 \pmod{220}$ value given on page 8.
- (v) The k value from (iv) is equivalent to the number of transformations necessary to return the original text of an encrypted block-matrix cipher. In functional terms, $k = \Theta(q, \ell)$.

THE EULER PHI FUNCTION — $\varphi(n)$

Definition. If n is a positive integer, we define $\varphi(n)$ to be the number of integers $f, 1 \leq f \leq n$, such that $(n, f) = 1$. The function φ is called the **Euler phi function**.

Known facts about the φ -function.

- (C.1) If $(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$
- (C.2) If p is a prime, then $\varphi(p) = (p - 1)$.
- (C.3) If α is a non-negative integer and p is a prime, then $\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p}) = (p - 1)p^{\alpha-1}$.
- (C.4) If $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_t^{k_t}$ where p_i is a prime, then $\varphi(n) = \prod_{i=1}^t (p_i - 1)p_i^{k_i-1}$
- (C.5) $\sum_{d|n} \varphi(d) = n$.
- (C.6) (**Euler.**) $n^{\varphi(m)} \equiv 1 \pmod{m}$ for $(n, m) = 1$.

Table of $\varphi(n)$ for given n .

n	$\varphi(n)$	n	$\varphi(n)$	n	$\varphi(n)$
1	1	16	8	31	30
2	1	17	16	32	16
3	2	18	6	33	20
4	2	19	18	34	16
5	4	20	8	35	24
6	2	21	12	36	30
7	6	22	10	37	36
8	4	23	22	38	18
9	6	24	8	39	24
10	4	25	20	40	16
11	10	26	12	41	40
12	4	27	18	42	12
13	12	28	12	43	42
14	6	29	28	44	20
15	8	30	8	45	24

The value of the φ -function is easily found for any given number. First, the number must be broken into its canonical factorization. For example, given the number 786, one must break it into $(2 \cdot 3 \cdot 131)$. Then, using [C.1], we can write $\varphi(786) = \varphi(2 \cdot 3 \cdot 131) = \varphi(2)\varphi(3)\varphi(131) = (2 - 1)(3 - 1)(131 - 1) = 260$.

The implications of [C.5] are interesting. This means that given any number, n , the sum of the φ -function values evaluated at all factors is equal to n itself. For example, consider the number 12. The factors of 12 are $\{1, 2, 3, 4, 6, 12\}$. Application of [C.5] means that $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$. Indeed, $1 + 1 + 2 + 2 + 2 + 4$ does equal 12.

REFERENCES

1. Brualdi, Richard A. and Herbert J. Ryser. *Combinatorial Matrix Theory*. Cambridge University Press, New York, 1991, 157-63.
2. Davis, Philip J. *Circulant Matrices*. Wiley & Sons, New York, 1979, 155-91.
3. Goldstein, Larry Joel. *Abstract Algebra: a first course*. Prentice-Hall, Inc., 1973, 85-88.
4. Langie, Andre. *Cryptography, A Study of Secret Writing*. Aegean Park Press, 1982.
5. McCormick, Donald. *Love in Code: or How to Keep Your Secrets*. Eyre Methuen Ltd., 1980.
6. Roberts, Joe. *Elementary Number Theory*. The MIT Press, Cambridge, Mass., 1977, 50-58.
7. Shanks, Daniel. *Solved and Unsolved Problems in Number Theory*. Chelsea Publishing Company, New York, 1978, 65-74.
8. Smith, Laurence Dwight. *Cryptology, The Science of Secret Writing*. W. W. Norton & Company, 1943.
9. Stinson, Douglas R. *Cryptography, Theory and Practice*. CRC Press, 1995.
10. Vanden Eynden, Charles. *Elementary Number Theory*. McGraw-Hill, Inc., New York, 1987, 128-34.
11. Wrixon, Fred B. *Codes, Ciphers, & Other Cryptic & Clandestine Communication.*, Black Dog & Leventhal Pub., Inc., 1998.

Any questions or comments are welcome by sending me a message at brg5658@yahoo.com or brg5658@hotmail.com.