Conjugation by Circulant Matrices in Non-commutative Cryptography

Hannah B. Frederick

submitted in partial fulfillment of the requirements for Honors in Mathematics at the University of Mary Washington

Fredericksburg, Virginia

April 2020

This thesis by **Hannah B. Frederick** is accepted in its present form as satisfying the thesis requirement for Honors in Mathematics.

Date	Approved
_____	_____
	Randall Helmstutler, Ph.D. thesis advisor
_____	_____
	Jennifer Magee, M.A. committee member
_____	_____
	Andrew Marshall, Ph.D. committee member

Contents

Abstract

We introduce a procedure in which two trusted individuals, Alice and Bob, may share a secret matrix K from the non-abelian group $\mathrm{GL}_n(\mathbb{F}_q)$. In this procedure, the matrix K is concealed from an eavesdropper, Eve, by a sequence of conjugations by elements from a pre-determined abelian subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. We demonstrate that the group $\mathcal{C}_n^*(\mathbb{F}_q)$ of invertible circulant matrices is one abelian subgroup that may be able to withstand a brute force attack. To analyze this we need a technique to determine the order of $\mathcal{C}_n^*(\mathbb{F}_q)$, and to do this we make use of a well-known isomorphism between the rings $\mathcal{C}_n(\mathbb{F}_q)$ and $\mathbb{F}_q[x]/\langle x^n-1\rangle$. After we show empirically that the order of $\mathcal{C}_n^*(\mathbb{F}_q)$ increases exponentially in n with q fixed, we will give a universal lower bound on the order of this group to prove this mathematically as well.

1 Introduction

1.1 Massey-Omura Background

Non-commutative cryptography is the area of cryptography where the cryptographic systems are based on algebraic structures which are non-commutative. Traditional cryptography has always used commutative groups and rings, but now non-commutative structures are starting to be used in encryption procedures [3]. Non-commutative cryptography has been an area of research in the cryptographic community since the early 2000's because this cryptography might have an advantage over traditional cryptography since the commutative structures may be easier to break than the non-commutative structures, though this has not yet been proved true or false. No one has used these non-commutative structures in practice because no one is sure of the security and complexity of these algebraic structures in encryption procedures. But the hope is that the non-commutativity makes the algebraic calculations harder for an eavesdropper, and therefore increases the security of the system.

One of these encryption systems that uses commutative structures is the Massey-Omura cryptosystem, which uses the commutativity of integer exponentiation for encryption and decryption [2]. In the traditional procedure, Alice picks the public abelian group $\mathbb{Z}_p^*$, and she picks the plaintext m as an element of $\mathbb{Z}_p^*$, where p is a prime number. Alice selects elements e_A and d_A from the public group so that $e_A d_A = 1 \bmod (p-1)$. Likewise, Bob selects elements e_B and d_B from the public group so that $e_B d_B = 1 \bmod (p-1)$. Alice first computes $m^{e_A} \bmod p$ and sends this to Bob. Bob then computes $(m^{e_A})^{e_B} = m^{e_A e_B} \bmod p$ and sends this to Alice. Alice then encrypts to the ciphertext $c = m^{e_A e_B d_A} \bmod p$ and sends this to Bob. Bob finally decrypts to the plaintext $m = m^{e_A e_B d_A d_B} = m^{e_A d_A e_B d_B} = m^1 = m \bmod p$ by Euler's Theorem. Euler's Theorem states that exponents of integers modulo a positive integer n are calculated modulo $\phi(n)$, which is the number of integers from 1 to n that are coprime with n. Since we are taking the exponents modulo a prime number p, $\phi(p) = p-1$ because p is the only number that is not coprime to p, which is why we let $e_A d_A = 1 \bmod (p-1)$ and $e_B d_B = 1 \bmod (p-1)$. The purpose of this research is to consider using non-commutative structures like that of matrix multiplication for concealing and revealing a secret matrix. We will do this by replacing the integer exponentiation of this procedure with matrix conjugation in our new procedure.

Old Massey-Omura	Our Massey-Omura
commutative group: $\mathbb{Z}_p^*$	non-commutative group: $\mathrm{GL}_n(\mathbb{F}_q)$
integer plaintext: m from the group	matrix plaintext: K from the group
session keys: e_A and d_A	session keys: A and A^{-1}
integer exponentation: $m \to m^{e_A}$	matrix conjugation: $K \to A^{-1}KA$

1.2 Procedure

We now show how we will convert integer exponentiation in the group $\mathbb{Z}_p^*$ to matrix conjugation in the group $\mathrm{GL}_n(\mathbb{F}_q)$ in our procedure.

Assumption: Suppose Alice and Bob have a method for selecting private matrices A and B so that $AB = BA$ and so that Alice does not know Bob's B and Bob does not know Alice's A.

Abstract Procedure: Suppose that Alice wants to send Bob a private matrix K from the public non-abelian group $\mathrm{GL}_n(\mathbb{F}_q)$ of $n \times n$ invertible matrices with entries from a finite field $\mathbb{F}_q$. Alice picks a private matrix A and Bob picks a private matrix B according to the preceding assumption. Alice and Bob can encrypt and decrypt K over an open line according to the following procedure:

1. Alice finds the conjugate of A on K by calculating $M_1 = K^A = A^{-1}KA$, and she sends the conjugate M_1 to Bob.
2. Bob finds the conjugate of B on M_1 by calculating $M_2 = M_1^B = B^{-1}M_1B$, and he sends the conjugate M_2 to Alice.
3. Alice finds the conjugate of A^{-1} on M_2 by calculating $M_3 = M_2^{A^{-1}} = AM_2A^{-1}$, and she sends the congujate M_3 to Bob.
4. Bob finds the conjugate of B^{-1} on M_3 by calculating $M_3^{B^{-1}} = BM_3B^{-1}$, and he gets the plaintext matrix K.

A common analogy for this type of encryption in this procedure is the "box and locks" analogy. In this analogy, Alice puts her secret matrix K in a box, then she puts her own lock on the box and locks it with her matrix A, and she sends the box to Bob. Bob then puts his own lock on the box and locks it with his matrix B, and he sends the box back to Alice. Alice then takes her own lock off of the box with her matrix A^{-1}, and she sends the box back to Bob. Bob then takes his own lock off of the box with his matrix B^{-1}, and he can now get K out of the box. But if Eve ever stole the box, then she could never steal K from the box because she can unlock neither Alice's lock nor Bob's lock.

Proposition 1.1. *In this procedure, the plaintext matrix K can always be recovered as long as the private matrices A and B commute.*

Proof. Let Alice pick a private element K from the public non-abelian group $\mathrm{GL}_n(\mathbb{F}_q)$ and a private element A according to the previous method. Let Bob also pick a private element B according to the previous method.

1. Alice calculates the conjugate $M_1 = K^A = A^{-1}KA$, and she sends M_1 to Bob.
2. Bob calculates the conjugate $M_2 = M_1^B = B^{-1}M_1B$, and he sends M_2 to Alice.
3. Alice calculates the conjugate $M_3 = M_2^{A^{-1}} = AM_2A^{-1}$, and she sends M_3 to Bob.
4. Bob calculates the conjugate $K = M_3^{B^{-1}} = BM_3B^{-1}$, and he finds Alice's plaintext K.

To prove that Bob recovers the plaintext K, we compute the following:

$$\begin{aligned} BM_3B^{-1} &= B(AM_2A^{-1})B^{-1} \\ &= BA(B^{-1}M_1B)A^{-1}B^{-1} \\ &= BAB^{-1}(A^{-1}KA)BA^{-1}B^{-1} \\ &= ABB^{-1}A^{-1}KBAA^{-1}B^{-1} \leftarrow (AB = BA) \\ &= AA^{-1}KBB^{-1} \\ &= K. \end{aligned}$$

Thus the plaintext matrix K can be recovered as long as the private matrices A and B commute. □

Example 1.2. Suppose Alice picks the private element K from the public non-abelian group $\mathrm{GL}_3(\mathbb{F}_{101})$ and the private element A with the method so that $AB = BA$, and Alice does not know Bob's secret matrix B. Suppose Bob also picks the private element B with the method so that $AB = BA$, and Bob does not know Alice's secret matrix A. The matrices K, A, and B are defined as follows:

$$K = \begin{bmatrix} 17 & 62 & 10 \\ 52 & 26 & 14 \\ 98 & 81 & 51 \end{bmatrix}$$

$$A = \begin{bmatrix} 79 & 83 & 23 \\ 23 & 79 & 83 \\ 83 & 23 & 79 \end{bmatrix} \quad B = \begin{bmatrix} 87 & 63 & 93 \\ 93 & 87 & 63 \\ 63 & 93 & 87 \end{bmatrix}$$

$$AB = \begin{bmatrix} 83 & 96 & 33 \\ 33 & 83 & 96 \\ 96 & 33 & 83 \end{bmatrix} = BA.$$

Here are the steps for encryption and decryption:

1. Alice computes the conjugate matrix:

$$M_1 = A^{-1}KA = \begin{bmatrix} 72 & 66 & 58 \\ 58 & 72 & 66 \\ 66 & 58 & 72 \end{bmatrix} \begin{bmatrix} 17 & 62 & 10 \\ 52 & 26 & 14 \\ 98 & 81 & 51 \end{bmatrix} \begin{bmatrix} 79 & 83 & 23 \\ 23 & 79 & 83 \\ 83 & 23 & 79 \end{bmatrix} = \begin{bmatrix} 74 & 75 & 59 \\ 54 & 94 & 71 \\ 28 & 30 & 27 \end{bmatrix}$$

2. Bob computes the conjugate matrix:

$$M_2 = B^{-1}M_1B = \begin{bmatrix} 19 & 15 & 35 \\ 35 & 19 & 15 \\ 15 & 35 & 19 \end{bmatrix} \begin{bmatrix} 74 & 75 & 59 \\ 54 & 94 & 71 \\ 28 & 30 & 27 \end{bmatrix} \begin{bmatrix} 87 & 63 & 93 \\ 93 & 87 & 63 \\ 63 & 93 & 87 \end{bmatrix} = \begin{bmatrix} 27 & 3 & 17 \\ 68 & 21 & 6 \\ 64 & 58 & 46 \end{bmatrix}$$

3. Alice computes the conjugate matrix:

$$M_3 = AM_2A^{-1} = \begin{bmatrix} 79 & 83 & 23 \\ 23 & 79 & 83 \\ 83 & 23 & 79 \end{bmatrix} \begin{bmatrix} 27 & 3 & 17 \\ 68 & 21 & 6 \\ 64 & 58 & 46 \end{bmatrix} \begin{bmatrix} 72 & 66 & 58 \\ 58 & 72 & 66 \\ 66 & 58 & 72 \end{bmatrix} = \begin{bmatrix} 84 & 13 & 51 \\ 99 & 28 & 33 \\ 27 & 94 & 83 \end{bmatrix}$$

4. Bob recovers the secret matrix:

$$K = BM_3B^{-1} = \begin{bmatrix} 87 & 63 & 93 \\ 93 & 87 & 63 \\ 63 & 93 & 87 \end{bmatrix} \begin{bmatrix} 84 & 13 & 51 \\ 99 & 28 & 33 \\ 27 & 94 & 83 \end{bmatrix} \begin{bmatrix} 19 & 15 & 35 \\ 35 & 19 & 15 \\ 15 & 35 & 19 \end{bmatrix} = \begin{bmatrix} 17 & 62 & 10 \\ 52 & 26 & 14 \\ 98 & 81 & 51 \end{bmatrix}$$

We can see the K that Bob computed at the end is the same K that Alice selected at the start.

Question: How can Alice and Bob select their private matrices A and B so that $AB = BA$ without knowing each other's matrices in the process?

Answer: Alice and Bob can select their private matrices A and B so that $AB = BA$ and not know each other's matrices by selecting a public abelian subgroup C of $\mathrm{GL}_n(\mathbb{F}_q)$.

We propose the solution of Alice publishing an abelian subgroup C, and then Alice and Bob independently picking their own private matrices A and B from the public group C. But this solution produces more questions. How can Alice and Bob find such a C? How can Alice and Bob find such a C that is large enough to hold up against a brute force attack? Moreover, how can Alice and Bob find such a C that is safe enough to not suffer from other security issues? Generally, what types of properties should a public abelian subgroup C have in order to make this secure? In Example 1.2, we selected matrices A and B to be circulant matrices, which will be defined in Definition 2.1. We will see that the group of invertible circulants is an abelian subgroup of the general linear group that can be implemented in our procedure. We will investigate the more important question, which is whether the group of invertible circulants *should* be implemented in our procedure.

2 Circulant Matrices

We will now talk about the properties of circulant matrices over fields to show that they can be implemented in our procedure.

Definition 2.1. A **circulant** matrix C is an $n \times n$ matrix where each row is the prior row shifted one position to the right, so that C takes the form:

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix}.$$

A circulant matrix C is completely determined by its first row, and thus the matrix C above can be represented as $\begin{bmatrix} c_1 & c_2 & \cdots & c_n \end{bmatrix}^\dagger$. The set of all $n \times n$ circulant matrices with entries over the field $\mathbb{F}$ will be denoted as $\mathcal{C}_n(\mathbb{F})$. We wish to prove that the set of all invertible circulant matrices over a field is an abelian subgroup of the general linear group over the same field. This will show that the group of circulant matrices can be implemented as the public abelian subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ in our procedure. In order to do this, it will be convenient to consider the ring structure of the set of all circulant matrices over a field. We want to prove that the set of all circulant matrices over a field is a commutative ring with identity, which will show that the multiplication of circulant matrices is commutative. We will first prove that the set of all circulant matrices over a field is an abelian group under matrix addition, then prove that it is a vector space, and lastly prove that it is a commutative ring. Once we prove that $\mathcal{C}_n(\mathbb{F})$ is a commutative ring with identity, we will look at its group of units under multiplication.

2.1 Vector Space Structure of Circulant Matrices

It is clear that $\mathcal{C}_n(\mathbb{F})$ is closed under matrix addition because two circulant matrices added together is a circulant matrix with elements that are the sum of the respective elements of the two matrices. We can also see that addition in $\mathcal{C}_n(\mathbb{F})$ is associative and commutative because the addition of all matrices is associative and commutative. It is also clear that $\mathcal{C}_n(\mathbb{F})$ has the additive identity propery because all circulant matrices added to the zero matrix will be the same circulant matrices, and the zero matrix is also a circulant matrix. We can also see that $\mathcal{C}_n(\mathbb{F})$ is closed under additive inverses because all circulant matrices added to the negative of their matrices will be the zero matrix, and this inverse matrix is also a circulant matrix. Therefore, the set of all circulant matrices over a field is an abelian group under matrix addition.

It is clear that $\mathcal{C}_n(\mathbb{F})$ is closed under scalar multiplication because a circulant matrix multiplied by a scalar will be another circulant matrix with elements that are the products of each element and the scalar. Therefore, the set of all circulant matrices over a field is a vector space with scalars from the field. We can also see that if these scalars are from the finite field $\mathbb{F}_q$, then $\mathcal{C}_n(\mathbb{F}_q)$ has q^n elements and has dimension n. This is because a circulant matrix is determined by its first row and there are q options for each of the n entries in the first row. We want to find a convenient basis for this vector space since it will help us understand its ring structure, and to find this set we will look at Example 2.2.

Example 2.2. Let C be the element $\begin{bmatrix}4 & 2 & 6\end{bmatrix}^\dagger$ of $\mathcal{C}_3(\mathbb{Z}_7)$, the set of all 3×3 circulant matrices with entries from the field $\mathbb{Z}_7$. Consider the circulant matrix C. Note that:

$$C = \begin{bmatrix}4 & 2 & 6\\ 6 & 4 & 2\\ 2 & 6 & 4\end{bmatrix} = \begin{bmatrix}4 & 0 & 0\\ 0 & 4 & 0\\ 0 & 0 & 4\end{bmatrix} + \begin{bmatrix}0 & 2 & 0\\ 0 & 0 & 2\\ 2 & 0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 6\\ 6 & 0 & 0\\ 0 & 6 & 0\end{bmatrix} =$$

$$4\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} + 2\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{bmatrix} + 6\begin{bmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}.$$

Therefore, $\{\begin{bmatrix}1 & 0 & 0\end{bmatrix}^\dagger, \begin{bmatrix}0 & 1 & 0\end{bmatrix}^\dagger, \begin{bmatrix}0 & 0 & 1\end{bmatrix}^\dagger\}$ is a basis for the vector space $\mathcal{C}_3(\mathbb{Z}_7)$.

Likewise, $\{\begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix}^\dagger, \begin{bmatrix}0 & 1 & \cdots & 0\end{bmatrix}^\dagger, \cdots, \begin{bmatrix}0 & 0 & \cdots & 1\end{bmatrix}^\dagger\}$ is a basis of n elements for any $n \times n$ circulant. It turns out that the matrices of this basis are all powers of the second matrix $\begin{bmatrix}0 & 1 & \cdots & 0\end{bmatrix}^\dagger$. The first matrix $\begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix}^\dagger$ is the identity matrix, so it is the second matrix to the zeroth power. The next matrix $\begin{bmatrix}0 & 1 & \cdots & 0\end{bmatrix}^\dagger$ is the original matrix, so it is the second matrix to the first power. The nth matrix $\begin{bmatrix}0 & 0 & \cdots & 1\end{bmatrix}^\dagger$ is the second matrix to the $(n-1)$st power. And it turns out that this second matrix is a cyclic permutation matrix.

Definition 2.3. Let the **cyclic permutation matrix**, P, be the element of $\mathcal{C}_n(\mathbb{F})$ with first row $\begin{bmatrix}0 & 1 & \cdots & 0\end{bmatrix}$. For every row i and every column j in the matrix P, only the entries $a_{i,i+1}$ are a 1, and all other entries $a_{i,j}$ are a 0, so:

$$P = \begin{bmatrix}0 & 1 & \cdots & 0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 0 & \cdots & 0\end{bmatrix}.$$

Proposition 2.4. *Let $x \geq 0$ be an integer. The matrix P^x is a $n \times n$ circulant matrix that shifts every row of the identity matrix x spaces to the right, where the exponent x is interpreted* mod n*. For every row i and every column j in the matrix P^x, only the entries $a_{i,i+x}$ are a 1 and all other entries $a_{i,j}$ are a 0.*

Proof. For the base case, P^0 is the identity matrix because any square matrix to the zero power is the identity matrix. And P^0 is a circulant matrix so that only the entries $a_{i,i+0}$ are a 1 and all other entries $a_{i,j}$ are a 0, so the proposition is true for P^0. Of course, it is also true for P^1. For all other cases, assume that the proposition is true for P^k, then P^k is a circulant matrix of the stated form. Then $P^{k+1} = PP^k$. Suppose the entries of P are $a_{i,j}$ and the entries of P^k are $b_{i,j}$. We want to show that only the entries $c_{i,i+k+1}$ in the matrix P^{k+1} are a 1. We know that $a_{i,i+1} = 1$ for every row i of matrix P by the previous definition and $b_{j-k,j} = 1$ for every column j of matrix P^k by the previous assumption. We also know from the definition of matrix multiplication that the entries $c_{i,j}$ will be a 1 when $a_{i,m}$ and $b_{m,j}$ are a 1 for some m, and all other entries will be a 0. Thus $c_{i,j} = \sum_{m=1}^{n} a_{i,m}b_{m,j} = 1$ when $m = i + 1 = j - k$, thus $j = i + k + 1$. Therefore, P^{k+1} is a circulant matrix so that for every row i and every column j, only the entries $c_{i,i+k+1}$ are a 1, and all other entries $c_{i,j}$ are a 0, so the proposition is true for P^{k+1} if it is true for P^k. By mathematical induction, we are done. □

Note. The matrix P^n is an $n \times n$ circulant that shifts every row of the identity matrix n spaces to the right. The identity matrix is an $n \times n$ matrix, so shifting $n - 1$ spaces to the right is the same as shifting 1 space to the left, and $n - 1 = -1 \bmod n$. Also, shifting n spaces to the right is the same as shifting no spaces at all, and $n = 0 \bmod n$. Thus $P^n = I$, and this is why the exponents must be interpreted mod n.

In light of Example 2.2, Proposition 2.4 immediately gives the following corollary.

Corollary 2.5. *Every circulant matrix C in $\mathcal{C}_n(\mathbb{F})$ can be uniquely expressed as a linear combination of powers of P in the following way:*

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix} = c_1 I + c_2 P + c_3 P^2 + \cdots + c_n P^{n-1}.$$

Corollary 2.6. *The set $\{I, P, P^2, \ldots, P^{n-1}\}$ of powers of the cyclic permutation matrix P forms a basis for the vector space of all $n \times n$ circulant matrices over a field $\mathbb{F}$.*

Proposition 2.7. *The set of all circulant matrices over a field $\mathbb{F}$ is closed under matrix multiplication.*

Proof. Let C and D be $n \times n$ circulant matrices over $\mathbb{F}$ so that $C = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \end{bmatrix}^\dagger$ and $D = \begin{bmatrix} d_1 & d_2 & \cdots & d_n \end{bmatrix}^\dagger$. Then $C = c_1 I + c_2 P + c_3 P^2 + \cdots + c_n P^{n-1}$ and $D = d_1 I + d_2 P + d_3 P^2 + \cdots + d_n P^{n-1}$. Thus $CD = (c_1 I + c_2 P + c_3 P^2 + \cdots + c_n P^{n-1})(d_1 I + d_2 P + d_3 P^2 + \cdots + d_n P^{n-1}) = x_1 I + x_2 P + x_3 P^2 + \cdots + x_n P^{n-1}$ for some coefficients x_i for $1 \leq i \leq n$ after combining the coefficients in polynomials C and D. This is a closed operation because all of the coefficients are elements of the field. Thus CD is also a circulant matrix because the multiplication of polynomials over a field is closed. This is because we will make repeated use of reducing the powers of P mod n. □

Proposition 2.8. *Let C be an invertible circulant matrix in $\mathcal{C}_n(\mathbb{F})$. Then its inverse is also a circulant matrix in $\mathcal{C}_n(\mathbb{F})$.*

Proof. Let C be an invertible circulant with $\det(C) \neq 0$ and with entries over a field $\mathbb{F}$. Suppose that its characteristic polynomial is:

$$p(x) = \det(xI - C) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0 = (-1)^n \det(C) \neq 0$. Then the Cayley-Hamilton Theorem states that

$$a_n C^n + a_{n-1}C^{n-1} + \cdots + a_1 C + a_0 I = 0.$$

We can see from this that

$$I = -\frac{1}{a_0}(a_n C^n + a_{n-1}C^{n-1} + \cdots + a_1 C),$$

which shows us that

$$C^{-1} = -\frac{1}{a_0}(a_n C^{n-1} + a_{n-1}C^{n-2} + \cdots + a_1 I).$$

But circulants are closed under scalar multiplication, matrix multiplication, and matrix addition, so C^{-1} is a circulant because C was a circulant. □

We now know that the inverse of an invertible circulant is a circulant, and we have a formula for finding the inverse of a circulant. We will now look at an example with a 3×3 circulant matrix.

Example 2.9. Let $C = \begin{bmatrix}1 & 2 & 3\end{bmatrix}^\dagger$ be an element of $\mathcal{C}_3(\mathbb{F}_{97})$. The determinant of C is 18, so C is invertible. Then the characteristic polynomial of C with the coefficients calculated modulo 97 is:

$$p(x) = x^3 - 3x^2 - 15x - 18 = x^3 + 94x^2 + 82x + 79.$$

The Cayley-Hamilton Theorem states that:

$$p(C) = C^3 + 94C^2 + 82C + 79I = 0.$$

We can see from this that

$$I = \frac{-1}{79}(C^3 + 94C^2 + 82C),$$

which shows us that

$$C^{-1} = 27(C^2 + 94C + 82I) = 27C^2 + 16C + 80I =$$

$$\begin{bmatrix}60 & 60 & 76\end{bmatrix}^\dagger + \begin{bmatrix}16 & 32 & 48\end{bmatrix}^\dagger + \begin{bmatrix}80 & 0 & 0\end{bmatrix}^\dagger = \begin{bmatrix}59 & 92 & 27\end{bmatrix}^\dagger.$$

When we calculate C^{-1} in Mathematica, the result is $\begin{bmatrix}59 & 92 & 27\end{bmatrix}^\dagger$, so the formula is correct.

Proposition 2.8 will be important in the following section, when we prove that the set of all invertible circulants in the ring $\mathcal{C}_n(\mathbb{F})$ is also a group $\mathcal{C}_n^*(\mathbb{F})$.

2.2 Ring Structure of Circulant Matrices

We will now prove that the set of all circulant matrices over a field is a commutative ring with identity.

Proposition 2.10. *The set of all circulant matrices over a field $\mathbb{F}$ is a ring with identity.*

Proof. Let $\mathcal{C}_n(\mathbb{F})$ be the set of all $n \times n$ circulant matrices over a field $\mathbb{F}$. We have previously established that $\mathcal{C}_n(\mathbb{F})$ has all of the properties of an abelian group under matrix addition. By Proposition 2.7, matrix multiplication is a closed operation on $\mathcal{C}_n(\mathbb{F})$. Therefore, $\mathcal{C}_n(\mathbb{F})$ inherits the multiplicative associativity, the multiplicative identity, and the left and right distributive properties. □

We have now proved that the set of all circulant matrices over a field is a ring with identity. But we have yet to prove that the set of all circulant matrices over a field is a **commutative** ring with identity. While many of the previous properties of the ring of circulant matrices have been clear, this is not true of all its properties. Is it true that the multiplication of a circluant matrix with another circulant matrix is commutative? We will prove that this ring has this property with the following propositions.

Proposition 2.11. *There is an onto ring homomorphism from the ring $\mathbb{F}[x]$ of polynomials over the field $\mathbb{F}$ to the ring $\mathcal{C}_n(\mathbb{F})$ of circulants over the field $\mathbb{F}$.*

Proof. Let the map $\alpha : \mathbb{F}[x] \to \mathcal{C}_n(\mathbb{F})$ be $\alpha(f(x)) = f(P)$, so for every polynomial $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_mx^m$ in the ring of polynomials, $\alpha(f(x)) = f(P) = a_0I + a_1P + a_2P^2 + \cdots + a_mP^m$ in the ring of circulants. We want to show that α is an onto homomorphism. According to Corollary 2.5, every circulant can be uniquely expressed as a polynomial in such a form. Therefore, for every element of the ring of circulants, there is an element of the ring of polynomials that α maps to that circulant. Thus, α is onto. We also want to show that α is a ring homomorphism.

Let $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_mx^m$ and $g(x) = b_0 + b_1x^1 + b_2x^2 + \cdots + b_kx^k$ be elements of the ring of polynomials. We wish to show that $\alpha(f(x) + g(x)) = \alpha(f(x)) + \alpha(g(x))$. The variables of the two polynomials are the same because the exponents of P are collected in the same way as the exponents of x since these exponents are interpreted mod m. The coefficients are also the same because the coefficients of the P polynomial are combined in the same way as the coefficients of the x polynomial since these coefficients are from the same field. Thus, the two polynomials are the same, so $\alpha(f(x) + g(x)) = \alpha(f(x)) + \alpha(g(x))$ is true. We also wish to show that $\alpha(f(x) \times g(x)) = \alpha(f(x)) \times \alpha(g(x))$. The variables of the two polynomials are the same because the exponents of P are calculated in the same way as the exponents of x since the exponents are interpreted mod m. The coefficients of the two polynomials are also the same because the coefficients of the P polynomial are multiplied in the same way as the coefficients of the x polynomial since the coefficients are from the same field. Thus, the two polynomials are the same, so $\alpha(f(x) \times g(x)) = \alpha(f(x)) \times \alpha(g(x))$ is true. Therefore, α is a ring homomorphism. Thus, α is an onto ring homomorphisn from the ring of polynomials to the ring of circulants. □

This onto ring homomorphism between the ring of polynomials and the ring of circulants proves that the commutativity of multiplication of circulants is inherited from the commutativity of multiplication of polynomials. But for a more comprehensive understanding, we will remind the reader of some facts about the ring $\mathbb{F}[x]$ of polynomials over the field $\mathbb{F}$:

- In $\mathbb{F}[x]$, every ideal is a principal ideal, so every ideal I is generated by some polynomial $g(x)$.
- In $\mathbb{F}[x]$, a generator $g(x)$ of I is any element of the ideal I that is a polynomial of least degree.
- In $\mathbb{F}[x]$, the generator $g(x)$ is unique if it is chosen to be monic.

For proof of these facts, refer to [1, Section 8.1, Proposition 1]. We have now proved that there is an onto homomorphism between the ring of polynomials and the ring of circulants. We next

want to prove that this homomorphism induces an isomorphism via quotients, but to do this we need to find the kernel of our function α. We will prove that $\langle x^n - 1\rangle$ is the kernel of our function α in the following proposition.

Proposition 2.12. *Given the homomorphism $\alpha : \mathbb{F}[x] \to \mathcal{C}_n(\mathbb{F})$ as in Proposition 2.11, $x^n - 1$ is the unique monic polynomial of least possible degree in the kernel of α.*

Proof. Recall that the function $\alpha : \mathbb{F}[x] \to \mathcal{C}_n(\mathbb{F})$ is defined as $\alpha(f(x)) = f(P)$. The kernel of the function is an ideal of $\mathbb{F}[x]$, so the kernel must be generated by some polynomial $g(x)$ in $\mathbb{F}[x]$. If $\ker(\alpha) = \langle g(x)\rangle$, then $g(x)$ is an element of the kernel of α that is a polynomial of minimum degree. We will now show that the polynomial $x^n - 1$ generates the kernel. Since $P^n = I$, $P^n - I = 0$, so if $g(x) = x^n - 1$, $\alpha(g(x)) = g(P) = P^n - I = 0$. We have now shown that $x^n - 1$ is an element of the kernel, but we still need to show that $x^n - 1$ has minimum degree among all elements of the kernel. Suppose $f(x)$ is a non-zero element of $\ker(\alpha)$ of degree less than n; this will lead to a contradiction. Then $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^{n-1} \neq 0$ so that $\alpha(f(x)) = f(P) = 0$. If $f(P) = 0$, then $a_0P^0 + a_1P^1 + a_2P^2 + \cdots + a_{n-1}P^{n-1} = 0$. Therefore, we have:

$$f(P) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Then $a_0 = a_1 = a_2 = \cdots = a_{n-1} = 0$, thus $f(x) = 0 + 0x^1 + 0x^2 + \cdots 0x^{n-1} = 0$. But $f(x)$ has to be a nonzero polynomial by assumption, so there is no nonzero polynomial in the kernel of degree less than n. Thus, $g(x) = x^n - 1$ is the polynomial of least possible degree in the kernel of α, so $\ker(\alpha) = \langle x^n - 1\rangle$. □

Theorem 2.13 (Fundamental Homomorphism Theorem)**.** *If there is a ring homormorphism $f : A \to B$ from ring A onto ring B and if K is the kernel of f, then there is a ring isomorphism from A/K onto B.*

Corollary 2.14. *There is a ring isomorphism from the ring $\mathbb{F}[x]/\langle x^n - 1\rangle$ onto $\mathcal{C}_n(\mathbb{F})$.*

Since the multiplication of two polynomials is commutative, the isomorphism between the ring of circulants and this quotient of the ring of polynomials proves that the multiplication of two circulants is commutative. We have now proved that the set of all circulant matrices over a field $\mathbb{F}$ is a commutative ring with identity.

Proposition 2.15. *The set R^* of invertible elements in a ring R with identity is also a group under multiplication.*

Proof. A unit multiplied with another unit equals a unit in any group. Thus the set of all invertible elements, or units, in a ring with identity is also a group. □

Definition 2.16. Let $\mathcal{C}_n^*(\mathbb{F})$ be the set of all $n \times n$ invertible circulant matrices with entries over the field $\mathbb{F}$.

Corollary 2.17. *The set $\mathcal{C}_n^*(\mathbb{F})$ of invertible circulants in the ring $\mathcal{C}_n(\mathbb{F})$ is an abelian subgroup of $\mathrm{GL}_n(\mathbb{F})$.*

Convention 2.18. For the set $\mathcal{C}_n(\mathbb{F}_q)$ of all $n \times n$ circulant matrices over a finite field $\mathbb{F}_q$, $n \geq 2$ will always be a positive integer and $q \geq 2$ will always be a power of a prime number p.

We can now use the group $\mathcal{C}_n^*(\mathbb{F}_q)$ of invertible circulants as the public abelian subgroup of the group $\mathrm{GL}_n(\mathbb{F}_q)$ in our encryption procedure.

Concrete Procedure: Suppose that Alice wants to send Bob a plaintext matrix K from the public non-abelian group $\mathrm{GL}_n(\mathbb{F}_q)$. Alice picks a private matrix A and Bob picks a private matrix B from the public abelian subgroup $\mathcal{C}_n^*(\mathbb{F}_q)$ independently. Alice and Bob can encrypt and decrypt K over an open line according to the following procedure:

1. Alice finds the conjugate of K by A by calculating $M_1 = A^{-1}KA$, and she sends the conjugate M_1 to Bob.
2. Bob finds the conjugate of M_1 by B by calculating $M_2 = B^{-1}M_1B$, and he sends the conjugate M_2 to Alice.
3. Alice finds the conjugate of M_2 by A^{-1} by calculating $M_3 = AM_2A^{-1}$, and she sends the congujate M_3 to Bob.
4. Bob finds the conjugate of M_3 by B^{-1} by calculating BM_3B^{-1}, and he gets the plaintext K.

Just the fact that we *can* use circulant matrices in our procedure does not mean that we *should* use circulant matrices. The mathematical complexity of our procedure is based on the **conjugacy search problem** [3]. The complexity of this problem depends on the groups in question, and it seems that not much is known about the complexity of the conjugacy search problem in $\mathrm{GL}_n(\mathbb{F}_q)$. The question of this problem in the group $\mathrm{GL}_n(\mathbb{F}_q)$ is: for $S = X^{-1}TX$ where S and T are public and X and thus X^{-1} are private, is it possible for an eavesdropper to find out what X or X^{-1} is? Since the complexity of the conjugacy search problem is not known for $\mathrm{GL}_n(\mathbb{F}_q)$, we cannot find out if our procedure is vulnerable to attacks that depend on it. But we can find out if our procedure is vulnerable to a known ciphertext attack or a brute force attack. The other standard message attacks reduce to the conjugacy search problem, so we cannot know if our procedure is vulnerable to them. We will now consider the weakest of the standard message attacks, which is the known ciphertext attack.

2.3 Message Attacks on the Protocol

What can Eve discover by observing only the information that is public? Let's evaluate the security of all three passes in our three-pass protocol in order to examine its baseline security. The terms that are public to Eve will be underlined.

1. Alice finds the conjugate of K by A by calculating $M_1 = A^{-1}KA$, and she sends the conjugate M_1 over an open line; thus, the only public matrix in this pass is M_1:

$$\underline{M_1} = A^{-1}KA \Rightarrow A\underline{M_1} = KA \Rightarrow A\underline{M_1} - KA = 0.$$

   Eve can't use this last identity to solve for the private matrices A or K in the first pass because this pass results in a non-linear system. Because K and A are not public in this pass, if Eve wrote out all n^2 equations in terms of the variable entries of K and A, then the KA term would have quadratic entries. Thus, Eve can't solve this system with linear algebra methods.

2. Bob finds the conjugate of M_1 by B by calculating $M_2 = B^{-1}M_1B$, and he sends the conjugate M_2 over an open line; thus, the public matrices in this pass are M_1 and M_2:

$$\underline{M_2} = B^{-1}\underline{M_1}B \Rightarrow B\underline{M_2} = \underline{M_1}B \Rightarrow B\underline{M_2} - \underline{M_1}B = 0.$$

Eve can use the last identity to solve for some private matrix B in the second pass because this pass results in a linear system, but the true test is if she can solve for Bob's B. If Eve followed the previous technique, then this will lead to a solvable linear system. Thus, Eve can solve this system with linear algebra methods, but there will be multiple solutions. If Eve finds some matrix E that solves the system like matrix B, then Eve still cannot necessarily find the matrix K when she acts as Bob because E is not guaranteed to conjugate the same way that B does. Even if Eve does guess the secret matrix K she can't check to see if her guess is right. Let's consider the substitution of Eve's matrix E for Bob's matrix B in the third pass:

$$EM_3E^{-1} = EAM_2A^{-1}E^{-1} = \cdots = EB^{-1}KBE^{-1} = K \text{ if } E = B.$$

Let's try to act as Eve in Example 1.2 by trying to solve for B in $B\underline{M_2} - \underline{M_1}B = 0$:

$$\text{if } \begin{bmatrix} b_1 & b_2 & b_3 \\ b_3 & b_1 & b_2 \\ b_2 & b_3 & b_1 \end{bmatrix} \begin{bmatrix} 27 & 3 & 17 \\ 68 & 21 & 6 \\ 64 & 58 & 46 \end{bmatrix} - \begin{bmatrix} 74 & 75 & 59 \\ 54 & 94 & 71 \\ 28 & 30 & 27 \end{bmatrix} \begin{bmatrix} b_1 & b_2 & b_3 \\ b_3 & b_1 & b_2 \\ b_2 & b_3 & b_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\text{then } B = \begin{bmatrix} b_1 & b_2 & b_3 \\ b_3 & b_1 & b_2 \\ b_2 & b_3 & b_1 \end{bmatrix} = \begin{bmatrix} 27b_3 & 30b_3 & b_3 \\ b_3 & 27b_3 & 30b_3 \\ 30b_3 & b_3 & 27b_3 \end{bmatrix} = \begin{bmatrix} 87 & 63 & 93 \\ 93 & 87 & 63 \\ 63 & 93 & 87 \end{bmatrix} \text{ when } b_3 = 93.$$

3. Alice finds the conjugate of M_2 by A^{-1} by calculating $M_3 = AM_2A^{-1}$, and she sends the congujate M_3 over an open line; thus, the public matrices in this pass are M_2 and M_3:

$$\underline{M_3} = A\underline{M_2}A^{-1} \Rightarrow \underline{M_3}A = A\underline{M_2} \Rightarrow \underline{M_3}A - A\underline{M_2} = 0.$$

Eve can use the last identity to solve for some private matrix A in the third pass because this pass also results in a linear system, but the true test is if she can solve for Alice's A. If Eve followed the previous technique, then this will lead to a solvable linear system. Thus, Eve can solve this system with linear algebra methods, but there will be multiple solutions. If Eve finds some matrix D that solves for the system like matrix A, then Eve still cannot necessarily find the matrix K when she acts as Alice because D is not guaranteed to conjugate the same way that A does. Even if Eve does guess the secret matrix K she can't check to see if her guess is right. Let's consider the substitution of Eve's matrix D for Alice's matrix A in the second pass:

$$BM_3B^{-1} = BDM_2D^{-1}B^{-1} = \cdots = DA^{-1}KAD^{-1} = K \text{ if } D = A.$$

Let's try to act as Eve in Example 1.2 by trying to solve for A in $\underline{M_3}A - A\underline{M_2} = 0$:

$$\text{if } \begin{bmatrix} 84 & 13 & 51 \\ 99 & 28 & 33 \\ 27 & 94 & 83 \end{bmatrix} \begin{bmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{bmatrix} - \begin{bmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{bmatrix} \begin{bmatrix} 27 & 3 & 17 \\ 68 & 21 & 6 \\ 64 & 58 & 46 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\text{then } A = \begin{bmatrix} a_1 & a_2 & a_3 \\ a_3 & a_1 & a_2 \\ a_2 & a_3 & a_1 \end{bmatrix} = \begin{bmatrix} 21a_3 & 8a_3 & a_3 \\ a_3 & 21a_3 & 8a_3 \\ 8a_3 & a_3 & 21a_3 \end{bmatrix} = \begin{bmatrix} 79 & 83 & 23 \\ 23 & 79 & 83 \\ 83 & 23 & 79 \end{bmatrix} \text{ when } a_3 = 23.$$

We have now shown that our procedure is likely not vulnerable to the weakest message attack. We will now look at the next weakest attack, which is a brute force attack. Can an eavesdropper just search through all the possible private keys via a guess-and-check method? To consider this method of attack, we will need to count the number of elements in $\mathcal{C}_n^*(\mathbb{F}_q)$, or the order of the group $\mathcal{C}_n^*(\mathbb{F}_q)$, for different parameters of n and q.

3 Order of the Group of Invertible Circulants

3.1 Ring Theory Background

We know that we can use the group of invertible circulants as the abelian subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ in our procedure. We also know that our procedure with circulants is probably not vulnerable to standard message attacks. But we will need to count the number of invertible circulants in the group to see if our procedure is vulnerable to a brute force attack, and we hope that these counts are very large. To calculate the number of invertible circulants, we will need to remind the reader about rings, ideals, and polynomials over a field.

Definition 3.1. Let R be a commutative ring with the identity element 1 and let I and J be ideals of R. The ideals I and J are **coprime** if there is an element i of I and an element j of J so that $i + j = 1$.

We will need this definition so that we can use the Chinese Remainder Theorem.

Theorem 3.2 (Chinese Remainder Theorem)**.** *Let $I_1, I_2, \ldots, I_m$ be ideals in the commutative ring with identity R. The map π: $R \to R/I_1 \times R/I_2 \times \cdots \times R/I_m$ defined as $\pi(r) = (r+I_1, r+I_2, \ldots, r+I_m)$ is a ring homomorphism with kernel $I_1 \cap I_2 \cap \cdots \cap I_m$. If for each x, y with $1 \leq x, y \leq m$ and $x \neq y$ the ideals I_x and I_y are coprime, then this map is onto, so:*

$$R/(I_1 \cap I_2 \cap \cdots \cap I_m) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_m.$$

The Chinese Remainder Theorem is a standard theorem in ring theory. For a proof of this result, refer to [1, Section 7.6, Theorem 17]. We have now shown that the ring $R/I_1 \times R/I_2 \times \cdots \times R/I_m$ is isomorphic to the ring $R/\ker(\pi)$, by the Fundamental Homomorphism Theorem. We have also shown that $\ker(\pi) = \bigcap_{k=1}^{m} I_k$, by the Chinese Remainder Theorem. We also know that the ring $\mathcal{C}_n(\mathbb{F}_q)$ is isomorphic to the ring $\mathbb{F}_q[x]/\ker(\alpha)$ and $\ker(\alpha) = \langle x^n - 1 \rangle$, by Corollary 2.14. We wish to know the number of elements in the group $\mathcal{C}_n^*(\mathbb{F}_q)$, but this is a difficult question to answer.

We do know that the number of elements in $\mathcal{C}_n(\mathbb{F}_q)$ is the same as the number of elements in $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ because of the isomorphism of Proposition 2.12. But we cannot calculate the number of units in the ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ until we get the direct product of rings as distinct irreducible factors of the polynomial $x^n - 1$ over $\mathbb{F}_q$. When we find the distinct irreducible factors of this polynomial, the ideals of these factors will be coprime. We can then use the Chinese Remainder Theorem to find the number of units in this direct product is the same as the number of units in the ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, which is the number of elements in the group $\mathcal{C}_n^*(\mathbb{F}_q)$.

Definition 3.3. Let $f(x)$ and $g(x)$ be any polynomials over the field $\mathbb{F}$. Then $f(x)$ and $g(x)$ are **distinct** if $g(x)$ and $f(x)$ are not constant multiples of each other so $g(x) \neq cf(x)$ for any constant c in $\mathbb{F}$.

Proposition 3.4. *If $f_1(x)$ and $f_2(x)$ are distinct irreducible polynomials in $\mathbb{F}[x]$, then the ideals $\langle f_1(x) \rangle$ and $\langle f_2(x) \rangle$ are coprime.*

Proof. Let's look at the set $I = \{af_1(x) + bf_2(x) \mid a, b \text{ are in } \mathbb{F}[x]\}$. It is clear that I is an ideal that is nonzero; therefore, there is an element $g(x)$ in I of minimum degree that generates I. Because $I = \langle g(x) \rangle$, by the definition of generators every element of I is a multiple of $g(x)$. Therefore, every polynomial in I is a multiple of $g(x)$, thus $g(x)$ is a common divisor of $f_1(x)$ and $f_2(x)$ because $f_1, f_2 \in I$. But $f_1(x)$ and $f_2(x)$ are irreducible polynomials, so their only divisors are nonzero constants and constant multiples of themselves, so $g(x)$ must be a constant or a constant multiple of $f_1(x)$ and $f_2(x)$. If $g(x)$ is a constant multiple, then $g(x) = c_1 f_1(x) = c_2 f_2(x)$ for some c_1, c_2 in $\mathbb{F}$. This means that $f_1(x)$ and $f_2(x)$ are not distinct because both polynomials are irreducible, but this is a contradiction because $f_1(x)$ are $f_2(x)$ are distinct polynomials by assumption. Thus $g(x)$ is a nonzero constant, and therefore a unit. But $g(x)$ is in I, and the only ideal that contains a unit is $\mathbb{F}[x]$. Thus $I = \mathbb{F}[x]$, and I must contain 1. Then there are polynomials a, b in $\mathbb{F}[x]$ with $af_1(x) + bf_2(x) = 1$, thus $\langle f_1(x) \rangle$ and $\langle f_2(x) \rangle$ are coprime. □

Definition 3.5. For any polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ in $\mathbb{F}[x]$, the **derivative** of $f(x)$ is $f'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}$.

Definition 3.6. For any polynomial $f(x)$ in $\mathbb{F}[x]$, a root $x = c$ of $f(x)$ in the field $\mathbb{F}$ is a **repeated** root if the factor $x - c$ has a power greater than one in the factorization of $f(x)$; that is $f(x) = (x - c)^k g(x)$ where $k \geq 2$.

Proposition 3.7. *If $x = c$ is a root of the polynomial $f(x)$ as an element of $\mathbb{F}[x]$, then $x = c$ is a repeated root if and only if $x = c$ is a root of the derivative $f'(x)$.*

Proof. If $x = c$ is a repeated root of $f(x)$, then $f(x) = (x - c)^k g(x)$, for $k \geq 2$ where $g(c) \neq 0$. Then $f'(x) = k(x - c)^{k-1} g(x) + (x - c)^k g'(x)$. Thus $f'(c) = k(c - c)^{k-1} g(c) + (c - c)^k g'(c) = 0g(c) + 0g'(c) = 0 + 0 = 0$. This is because $k - 1$ is greater than or equal to 1 since k was greater than or equal to 2. Therefore, if $x = c$ is a repeated root of $f(x)$, then $x = c$ is root of $f'(x)$.

If $x = c$ is a root of $f(x)$ and $f'(x)$, then $f(x) = (x - c)^k g(x)$, for $k \geq 1$ and $g(c) \neq 0$. If $k = 1$, then $f(x) = (x - c)g(x)$ and $f'(x) = g(x) + (x - c)g'(x)$. Thus $f'(c) = g(c) + (c - c)g'(c) = g(c) + 0g'(c) = g(c) + 0 = g(c)$. Because $x = c$ is a root of $f'(x)$, $f'(c) = 0$ so $g(c) = f'(c) = 0$. But $g(c) \neq 0$, thus k is greater than 1. Therefore, if $x = c$ is a root of $f'(x)$, then $x = c$ is a repeated root of $f(x)$. □

Let $\mathbb{F}$ be a field. If $f(x)$ is any polynomial in $\mathbb{F}[x]$, then there is a field $\mathbb{E}$ that is an extension of the field $\mathbb{F}$ in which $f(x)$ has a root. The construction is a consequence of basic results in field theory. This construction can be iterated to give what are called "splitting fields" [1, Section 13.4, Definition].

Definition 3.8. An extension field $\mathbb{E}$ of the field $\mathbb{F}$ is a **splitting field** for the polynomial $f(x)$ in $\mathbb{F}[x]$ if $f(x)$ factors completely into linear factors in $\mathbb{E}[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of $\mathbb{E}$ containing $\mathbb{F}$.

Theorem 3.9. *For any field $\mathbb{F}$, if $f(x)$ is a polynomial in $\mathbb{F}[x]$, then there is an extension $\mathbb{E}$ of $\mathbb{F}$ that is a splitting field for $f(x)$.*

For a proof of this theorem, refer to [1, Section 13.4, Theorem 25]. We want to see if there are any repeated roots of the polynomial $x^n - 1$ in *any* extension field of the field $\mathbb{F}_q$. If we want to get the direct product of rings as distinct irreducible factors of this polynomial, then we can't have any repeated roots in any extension fields because then we would have repeated factors. If we want to use the Chinese Remainder Theorem on $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$, we must have coprime ideals in $\mathbb{F}_q[x]$, and to have this we must have distinct irreducible factors of $x^n - 1$. For

an example of repeated roots not in the original field but in an extension field, take the polynomial $f(x) = x^4 + 2x + 1 = (x^2 + 1)(x^2 + 1) = (x + i)^2(x - i)^2$. We can see that $f(x)$ has no roots in the field $\mathbb{R}$, but it has two repeated roots, i and $-i$, in the extension field $\mathbb{C}$. We know that a polynomial in any field has all of its roots in an extension of that field, this is the splitting field. So we need to make sure that the polynomial $x^n - 1$ has no repeated roots in $\mathbb{F}_q$ or in any extension of $\mathbb{F}_q$.

Proposition 3.10. *The polynomial $f(x) = x^n - 1$ has no repeated roots over any extension of the field $\mathbb{F}_q$ if and only if $\gcd(n, q) = 1$.*

Proof. Let $\gcd(n, q) = 1$ and $x = c$ be a root of $f(x) = x^n - 1$. If $x = c$ is a repeated root of $f(x) = x^n - 1$, then $x = c$ is a root of $f'(x) = nx^{n-1}$. If $x = c$ is a root of $f'(x)$, then $f'(c) = 0$, and $f'(x) = nx^{n-1} = 0$. Therefore, because n is a unit $x^{n-1} = 0$, so $x = 0$ is the only root of $f'(x)$. But $x = 0$ is not a root of $f(x)$ because $f(0) = 0^n - 1 = -1$. Then there is no $x = c$ that is a root of $f(x)$ and $f'(x)$. Therefore, if $\gcd(n, q) = 1$, then $f(x) = x^n - 1$ has no repeated roots.

Let $\gcd(n, q) \neq 1$, we want to show that $f(x)$ has repeated roots. Let $x = c$ be a root of $f(x) = x^n - 1$, we wish to show that $x = c$ is also a root of $f'(x)$. Because $\gcd(n, q) \neq 1$ and $q = p^d$ for some prime number p and positive integer d, $n = pk$ for some integer k. Then $f'(x) = nx^{n-1} = pkx^{pk-1}$. In any extension of the field $\mathbb{F}_{p^d}$, the characteristic of the field is p. For a proof of this fact, refer to [1, Section 13.1, Proposition 1]. Then $p = 0$, so $f'(x) = 0(kx^{0(k)-1}) = 0$. Thus, $x = c$ is a root of $f'(x)$, so $x = c$ is a repeated root of $f(x)$. Therefore, if $\gcd(n, q) \neq 1$, then $f(x) = x^n - 1$ has repeated roots, which is equivalent to the contrapositive that if $f(x) = x^n - 1$ has no repeated roots, then $\gcd(n, q) = 1$. □

Theorem 3.11. *The polynomial $f(x) = x^n - 1$ factors into distinct irreducible polynomials over the finite field $\mathbb{F}_q$ if and only if $\gcd(n, q) = 1$.*

Proof. Let $\gcd(n, q) = 1$ and let's say that the polynomial $x^n - 1$ does not factor into distinct irreducible polynomials over $\mathbb{F}_q$, so at least one of these polynomials is repeated. Then without loss of generality, $x^n - 1 = f_1(x)f_1(x)f_2(x) \cdots f_k(x)$. If $x^n - 1$ is passed to a splitting field, then the repeated polynomial $f_1(x)$ has a root, so $x^n - 1$ has a repeated root. But this is a contradiction to previous proposition. Therefore, $x^n - 1$ factors into distinct irreducible polynomials.

Let $x^n - 1$ factor into distinct irreducible polynomials over $\mathbb{F}_q$. Let's say that $\gcd(n, q) \neq 1$. Then by the previous proposition $x^n - 1$ has repeated roots over some extension of $\mathbb{F}_q$. If r is this repeated root in the extension field, then $x - r$ is a repeated irreducible factor in the polynomial. But this is a contradiction because we assumed $x^n - 1$ has only distinct irreducible factors. Therefore, $\gcd(n, q) = 1$. □

3.2 Finding the Order

We can now calculate the number of invertible circulants in the group $\mathcal{C}_n^*(\mathbb{F}_q)$ when n and q are coprime. Suppose that $\gcd(n, q) = 1$. We know from Theorem 3.11 that:

$$x^n - 1 = f_1(x) \cdot f_2(x) \cdot \cdots \cdot f_m(x)$$

where $f_1(x), f_2(x), ..., f_m(x)$ are distinct irreducible factors of $x^n - 1$. Then $\langle x^n - 1\rangle = \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cap \cdots \cap \langle f_m(x)\rangle$ where $\langle f_1(x)\rangle, \langle f_2(x)\rangle, ..., \langle f_m(x)\rangle$ are coprime ideals of $\langle x^n - 1\rangle$. Therefore $\mathbb{F}_q[x]/\langle x^n - 1\rangle = \mathbb{F}_q[x]/(\langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cap \cdots \cap \langle f_m(x)\rangle)$. Thus by the Chinese Remainder Theorem:

$$\mathcal{C}_n(\mathbb{F}_q) \cong \mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \prod_{i=1}^{m} (\mathbb{F}_q[x]/\langle f_i(x)\rangle).$$

If we take the group of units of each side of the isomorphism, then we get the formula of the following theorem.

Theorem 3.12. *If* $\gcd(n,q)=1$*, then* $|\mathcal{C}_n^*(\mathbb{F}_q)| = \prod_{i=1}^{m}(q^{d_i}-1)$ *where the* d_i*'s represent the degrees of the* m *distinct irreducible factors of* x^n-1*.*

Proof. Let $\gcd(n,q)=1$. Then Theorem 3.11 states that $x^n-1 = f_1(x)\cdot f_2(x)\cdot\cdots\cdot f_m(x)$ where $f_1(x), f_2(x), ..., f_m(x)$ are distinct irreducible factors of x^n-1. Then Proposition 3.4 states that $\langle f_1(x)\rangle, \langle f_2(x)\rangle, ..., \langle f_m(x)\rangle$ are coprime ideals of $\langle x^n-1\rangle$, so $\langle x^n-1\rangle = \langle f_1(x)\rangle \cap \langle f_2(x)\rangle \cap \cdots \cap \langle f_m(x)\rangle$. Since each $f_i(x)$ is an irreducible factor, $\mathbb{F}_q[x]/\langle f_i(x)\rangle$ is a field with size q^{d_i} where d_i is the degree of the factor $f_i(x)$. But we want the group of units from this field, so we must remove the zero element, and its size is $q^{d_i}-1$. When we do this for each factor, we get $\mathcal{C}_n(\mathbb{F}_q) \cong \mathbb{F}_q[x]/\langle x^n-1\rangle \cong \prod_{i=1}^{m}(\mathbb{F}_q[x]/\langle f_i(x)\rangle)$, so $|\mathcal{C}_n^*(\mathbb{F}_q)| = \prod_{i=1}^{m}(q^{d_i}-1)$. □

Example 3.13. Let us calculate the number of invertible circulants in $\mathcal{C}_9^*(\mathbb{F}_{11})$. We can use the formula of Theorem 3.12 because $\gcd(9,11)=1$. We can use the computer program Mathematica or Magma to factor the polynomial x^9-1 into distinct irreducibles over the finite field $\mathbb{F}_{11}$. The factorization is:

$$x^9-1 = (x+10)(x^2+x+1)(x^6+x^3+1)$$

and thus, $d_1=1, d_2=2, d_3=6$. We then use the previous theorem to calculate the number of invertible circulants in the group $\mathcal{C}_9^*(\mathbb{F}_{11})$:

$$|\mathcal{C}_9^*(\mathbb{F}_{11})| = (11^1-1)(11^2-1)(11^6-1) \approx 2.1\times 10^9.$$

Let us take as a baseline threshold that Eve cannot successfully brute force a system with at least $2^{80} \approx 1.2\times 10^{24}$ keys. This threshold is sometimes used as a low standard for the minimum number of necessary keys in an encryption procedure. This baseline threshold does not guarantee that an encryption procedure is not vulnerable to a brute force attack, but it is a starting point. If a key is eighty bits (or ten bytes) long, then the keyspace has 2^{80} keys, and this number estimates the minimum number of keys needed in the keyspace. The mathematics of the encryption procedure could also influence the minimum number of keys the cryptographer wants in the keyspace. We want to know when our procedure will likely not be vulnerable to a brute force attack, so we wish to find out when our keyspace has at least 2^{80} keys in it. We will first look at the number of invertible circulants in our procedure when q is constant at 2, and n is increased until $|\mathcal{C}_n^*(\mathbb{F}_2)| \geq 1.2\times 10^{24}$. When we carry out calculations as in Example 3.13, we get:

$$|\mathcal{C}_{81}^*(\mathbb{F}_2)| \approx 8.9\times 10^{23}$$

$$|\mathcal{C}_{83}^*(\mathbb{F}_2)| \approx 4.8\times 10^{24}$$

$$|\mathcal{C}_{85}^*(\mathbb{F}_2)| \approx 1.7\times 10^{25}.$$

We remind the reader that we cannot calculate $|\mathcal{C}_{82}^*(\mathbb{F}_2)|$ or $|\mathcal{C}_{84}^*(\mathbb{F}_2)|$ with our formula because $\gcd(82,2)=2\neq 1$ and $\gcd(84,2)=2\neq 1$. We can see that our procedure hits the threshold number of invertible circulants when $q=2$ and $n=83$, but what if the cryptographer does not want to work with 83×83 matrices in the encryption procedure? The cryptographer could increase the value of q to decrease the value of n and still hit the minimum number of keys in the procedure's

keyspace. We will now look at the number of invertible circulants in our procedure when $q = 16$ and $q = 64$ (both powers of 2) and n is increased until $|\mathcal{C}_n^*(\mathbb{F}_q)| \geq 1.2 \times 10^{24}$:

$$|\mathcal{C}_{19}^*(\mathbb{F}_{16})| \approx 7.0 \times 10^{22}$$

$$|\mathcal{C}_{21}^*(\mathbb{F}_{16})| \approx 1.6 \times 10^{25}$$

$$|\mathcal{C}_{23}^*(\mathbb{F}_{16})| \approx 4.6 \times 10^{27}$$

$$|\mathcal{C}_{13}^*(\mathbb{F}_{64})| \approx 3.0 \times 10^{23}$$

$$|\mathcal{C}_{15}^*(\mathbb{F}_{64})| \approx 1.2 \times 10^{27}$$

$$|\mathcal{C}_{17}^*(\mathbb{F}_{64})| \approx 5.0 \times 10^{30}.$$

We can see that our procedure hits the threshold number of invertible circulants when $q = 16$ and $n = 21$ and when $q = 64$ and $n = 15$, which are both much better than $n = 83$. But we still need to see how the number of invertible circulants in the group grows when we use a prime other than 2 and not just powers of the prime 2. Let's look at the number of elements in $\mathcal{C}_n^*(\mathbb{F}_q)$ when q is a constant and n is increased for $q = 41$ and $q = 101$:

$$|\mathcal{C}_{14}^*(\mathbb{F}_{41})| \approx 3.6 \times 10^{22}$$

$$|\mathcal{C}_{15}^*(\mathbb{F}_{41})| \approx 1.4 \times 10^{24}$$

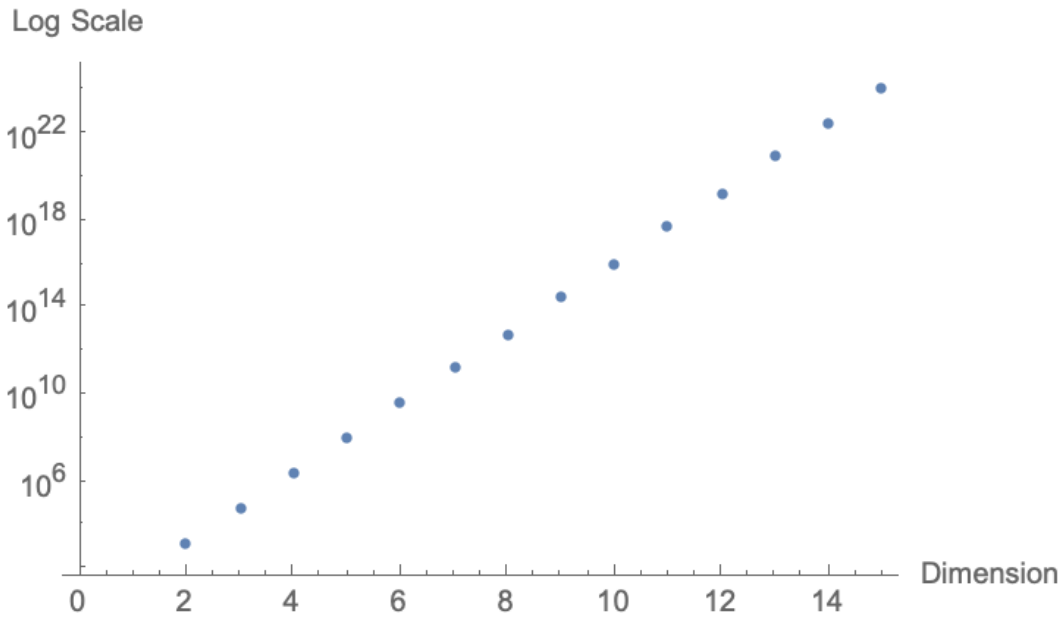
$$|\mathcal{C}_{16}^*(\mathbb{F}_{41})| \approx 5.2 \times 10^{25}$$

$$|\mathcal{C}_{12}^*(\mathbb{F}_{101})| \approx 1.1 \times 10^{24}$$

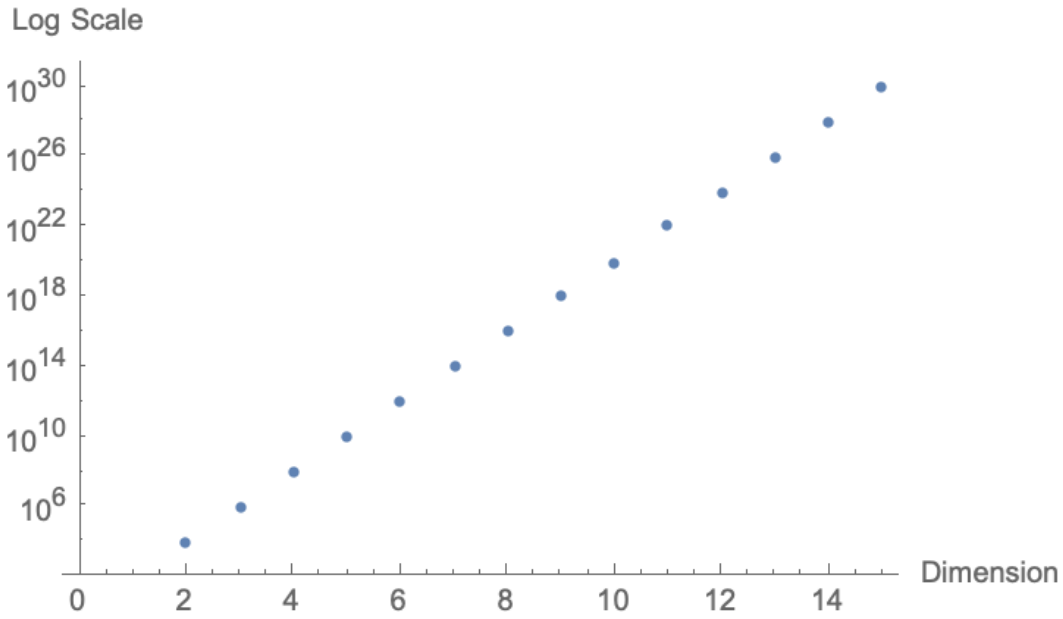
$$|\mathcal{C}_{13}^*(\mathbb{F}_{101})| \approx 1.1 \times 10^{26}$$

$$|\mathcal{C}_{14}^*(\mathbb{F}_{101})| \approx 1.1 \times 10^{28}.$$

We can see that our procedure hits the threshold number of invertible circulants when $q = 41$ and $n = 15$ and when $q = 101$ and $n = 13$. When we plot the number of invertible circulants versus the dimension of the circulants for $q = 41$ and $q = 101$, we see an interesting pattern appearing. For both plots, as the dimension of circulant matrices increases regularly, the number of invertible circulants increases linearly on a logarithmic scale; therefore, it increases exponentially on a linear scale. If this is true, then our procedure would be invulnerable to a brute force attack for a sufficiently large n because the number of invertible circulants for an eavesdropper to guess and check would increase exponentially.



Prime 41: Number of Invertible Circulants by Dimension of Circulants



Prime 101: Number of Invertible Circulants by Dimension of Circulants

It seems that the number of elements in $\mathcal{C}_n^*(\mathbb{F}_q)$ increases at least exponentially when q is constant and n increases, but we still need to prove this. And to do that we need to show that the formula's direct product of the factors of the polynomial $x^n - 1$ over $\mathbb{F}_q$ is at least exponential, if not more powerful. But we cannot predict the factorization of this polynomial for all values of n and q, so we will look at the sequence of the factors' degrees for various values of n and q. Each cell of the table below shows the degrees of the factors of $x^n - 1$ over the field $\mathbb{F}_q$ when $\gcd(n, q) = 1$:

	n=2	3	4	5	6	7	8
q=2	gcd $\neq 1$	(1,2)	gcd $\neq 1$	(1,4)	gcd $\neq 1$	(1,3,3)	gcd $\neq 1$
3	(1,1)	gcd $\neq 1$	(1,1,2)	(1,4)	gcd $\neq 1$	(1,6)	(1,1,2,2,2)
4	gcd $\neq 1$	(1,1,1)	gcd $\neq 1$	(1,2,2)	gcd $\neq 1$	(1,3,3)	gcd $\neq 1$
5	(1,1)	(1,2)	(1,1,1,1)	gcd $\neq 1$	(1,1,2,2)	(1,6)	(1,1,1,1,2,2)
7	(1,1)	(1,1,1)	(1,1,2)	(1,4)	(1,1,1,1,1,1)	gcd $\neq 1$	(1,1,2,2,2)
8	gcd $\neq 1$	(1,2)	gcd $\neq 1$	(1,4)	gcd $\neq 1$	(1,1,1,1,1,1,1)	gcd $\neq 1$
9	(1,1)	gcd $\neq 1$	(1,1,1,1)	(1,2,2)	gcd $\neq 1$	(1,3,3)	(1,1,1,1,1,1,1,1,1)

Let's look at the cells in which $x^n - 1$ factors into distinct linear factors over the finite field, which are highlighted in yellow. In all of these cases, because the degrees of all of the factors are 1, the formula for the number of elements in $\mathcal{C}_n^*(\mathbb{F}_q)$ is $(q-1)(q-1)\cdots(q-1) = (q-1)^n$ because the sum of the individual degrees must be the original degree n. Then the number of invertible circulants increases exponentially with respect to n, so these are the cases in which we know that the factorization is exponential. It seems that this is the case not only when $n = q-1$, but also when $n|q-1$, but we need to prove this. And to do that, we need to use the following proposition:

Proposition 3.14. *A finite subgroup of the multiplicative group of a field is cyclic. In particular, if $\mathbb{F}$ is a finite field, then the multiplicative group $\mathbb{F}^*$ of nonzero elements of $\mathbb{F}$ is a cyclic group.*

For a proof of this proposition, refer to [1, Section 9.5, Proposition 18].

Proposition 3.15. *If $\gcd(n,q) = 1$ and $n|q-1$, then $|\mathcal{C}_n^*(\mathbb{F}_q)| = (q-1)^n$.*

Proof. Suppose that $n|q-1$ or $q-1 = nk$ for some positive integer k. According to Proposition 3.14, the subgroup $\mathbb{F}_q^*$ of the multiplicative group of $\mathbb{F}_q$ is cyclic and has $q-1$ elements. Therefore, $\mathbb{F}_q^*$ has a generator α, so that all of the elements of $\mathbb{F}_q^*$ are in the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$. Every element of $\{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ is a solution to $x^{q-1} - 1 = 0$ by Lagrange's Theorem. Let's now look at who solves $x^n - 1 = 0$. One can check directly that the set $\{1, \alpha^k, \alpha^{2k}, \ldots, \alpha^{(n-1)k}\}$ solves this. So $x^n - 1 = 0$ has $\frac{q-1}{k} = n$ solutions that are distinct. Therefore, if $n|q-1$, then $|\mathcal{C}_n^*(\mathbb{F}_q)| = (q-1)^n$. □

We have now proved that in these cases, the formula from this factorization of $x^n - 1$ is exponential, but we still need to prove that in all other cases the formula from this factorization is at least exponential, if not even more fast-growing. And to do this, we will look at the minimum number of elements that can be obtained from the formula of Theorem 3.12.

3.3 Universal Lower Bound on the Order

We cannot predict how the polynomial $x^n - 1$ factors over the finite field when $n \nmid q-1$, so we cannot predict the degrees of these factors to calculate the number of elements in this group. But we can prove inductively that the universal minimum of the order of this group grows exponentially for all values of n and q such that $\gcd(n,q) = 1$. As a consequence, if the smallest possible size of the group grows exponentially, then all possible sizes grow at least exponentially, if not more rapidly.

The following proposition is a result of the basic pattern found in Theorem 3.12

Proposition 3.16. *Let $n \geq 2$. Consider the product $\prod_{i=1}^{k}(q^{d_i} - 1)$ subject to the constraints $d_1 + d_2 + \cdots + d_k = n$ and $d_i \geq 1$. Then the minimum possible value of this product is $(q-1)^n$ occuring when $k = n$ and $d_1 = d_2 = \cdots = d_n = 1$.*

Proof. We will use a proof by induction. Let's look at the first case when $n = 2$, then there are two cases for the factorization of $(q-1)^2$: $d_1 = d_2 = 1$ or $d_1 = 2$. In the former case, $(q-1)^2 = (q-1)(q-1)$ since $d_1 = d_2 = 1$. In the latter case, $(q^2-1) = (q-1)(q+1)$ since $d_1 = 2$. The minimum of these two cases is in the first case because $q-1 < q+1$, so $(q-1)(q-1) < (q-1)(q+1)$ Thus, the proposition holds when $n = 2$.

Suppose that the proposition holds when $k = n$, then let's look at the case for $n+1$. We know that $d_1+d_2+\cdots+d_k = n+1$ and $d_i \geq 1$, so we set the product $P = (q^{d_1}-1)(q^{d_2}-1)\cdots(q^{d_k}-1)$. We wish to show that $P \geq (q-1)^{n+1}$. In the case when all $d_i = 1$, we have $P = (q-1)(q-1)\cdots(q-1) = (q-1)^{n+1}$. In all other cases, some $d_i > 1$.

Suppose that $d_1 > 1$, then $q-1$ is a factor of $q^{d_1}-1$. Then $q^{d_1}-1 = (q-1)(q^{d_1-1}+q^{d_1-2}+\cdots+q+1)$. Thus $P = (q-1)(q^{d_1-1}+q^{d_1-2}+\cdots+q+1)(q^{d_2}-1)\cdots(q^{d_k}-1)$. Let $T = \frac{P}{q-1} = (q^{d_1-1}+q^{d_1-2}+\cdots+q+1)(q^{d_2}-1)\cdots(q^{d_k}-1)$.

It must be true that $q^{d_1-1}+q^{d_1-2}+\cdots+q+1 > q^{d_1-1}-1$. So we have that $T > (q^{d_1-1}-1)(q^{d_2}-1)\cdots(q^{d_k}-1)$. But this falls into the case for $k = n$, so $T > (q-1)^n$ by the inductive hypothesis. If we multiply both sides by $q-1$, then we have $P = (q-1)T > (q-1)^{n+1}$. Thus, if the proposition holds for n, then it holds for $n+1$. Therefore, the proposition is true for all n such that $n \geq 2$. □

We have now proved that the number of invertible circulants increases at least exponentially, if not more rapidly, as n increases and q is constant. Thus, our procedure is not vulnerable to a brute force attack because it reaches the minimum number of keys in any keyspace without using extremely large values of n or q. This means that our procedure is not only mathematically possible, but it is also theoretically secure against a brute force attack. But before our procedure can be implemented in practice, there are some more questions that need to be answered:

- Can we calculate the number of elements in $\mathcal{C}_n^*(\mathbb{F}_q)$ when $\gcd(n,q) \neq 1$?
- Is the question of the conjugacy search problem actually impossible to answer or are there weaknesses in our procedure that we are overlooking?
- Can we determine the number of elements in each of the conjugacy classes? Do these conjugacy classes significantly reduce the number of effective keys in $\mathcal{C}_n^*(\mathbb{F}_q)$?
- Is our procedure vulnerable to other standard message attacks or to more complicated attacks, like a man-in-the-middle attack?

Any future research relating to this thesis would need to consider issues such as these.

References

[1] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR 2286236

[2] J.L. Massey and J.K. Omura, *Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission*, January 28 1986, US Patent 4,567,600.

[3] A. Myasnikov, V. Shpilrain, and A. Ushakov, *Group-based cryptography*, Advanced Courses in Mathematics CRM Barcelona, Birkhauser Verlag, 2008.