THE DIFFIE-HELLMAN KEY EXCHANGE

IN MATRICES OVER A FIELD AND A RING

by

JOSHUA B. NELSON, B.A.

A THESIS

IN

MATHEMATICS

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for
the Degree of

MASTER OF SCIENCE

Approved

Accepted

Dean of the Graduate School

May, 2003

ACKNOWLEDGMENTS

First of all, I would like to thank Dr. Alex Wang for his unwavering support and expertise while I worked on my thesis. Without Dr. Wang's patience and guidance, I would have never have been able to complete this paper. I would also like to thank Dr. Mara Neusel for being on my committee. I am appreciative of Dr. Bennett for asking me to think about graduate school, and Dr. David Weinberg for helping me with problems I have encountered as a graduate student, and for keeping me in stitches.

I would also like to thank Zachary Kemp, Casey Hume, Nick Willis, Brian Tate, Nalo Lewis, Tracy Harris and Billy Duke for being such great friends to me during my tenure here at Tech. I would also like to thank Ian Martinez for teaching me how to type in this cursed Latex. I am so very grateful for the love and support of my family. Thank you so much, Mom and Dad, for instilling in me a drive for intellectual achievement and for your unconditional love. I would also like to thank Bonnie and Wayne Morris who have treated me like I was their own. Last, but by no means least, I would like to thank from the bottom of my heart my wife Shannon. Shannon, you never let me get down on myself, and you always made me feel like I was someone special. You are the most caring person I know, and the best wife possible. I love you so much!

CONTENTS

ABSTRACT

In this paper, we study the Diffie-Hellman key exchange on matrices over a field, $GL(n, q)$, and over a ring, $M_n(R)$. We show that Jordan Canonical form is not defined for a matrix $A \in M_n(R)$, and we present a cryptosystem capitalizing on this notion.

LIST OF FIGURES

CHAPTER I
INTRODUCTION

Before Whitfield Diffie and Martin Hellman introduced public key cryptography to the world in 1976, the major method of keeping information secure was by the use of a secret key. Indeed, one of the earliest cryptosystems based on a secret key encryption was the Caesar Cipher, which basically shifts each letter of the alphabet over n spaces. Caesar would send messages to his generals in the field encrypted using his Caesar Cipher, and hope that no member of the opposing army intercepted the message or the key. When an enemy did get hold of the key and the message, they knew all that the Roman army knew, and more.

Diffie and Hellman saw the inherent flaws in secret key cryptography, and proposed a method by which anyone could encrypt a message using someone's public key, but only that someone could decrypt the message. In order to accomplish this, the encryption must be relatively easy to do, but the decryption of the message must be based on a so-called "hard" problem. In fact, the basis for security in most public key schemes is integer factorization, and the discrete logarithm problem [4].

One such system that utilizes the discrete logarithm problem is the Diffie-Hellman key exchange. The Diffie-Hellman key exchange is a protocol whereby two users, Alice and Bob can, by a sequence of transmissions over a public channel, agree upon a secret cryptographic key. Alice and Bob first choose a (multiplicatively written) finite abelian group G and some element $\alpha \in G$. Alice then selects an integer a at random and transmits α^a to Bob. Bob chooses a random integer b and transmits α^b to Alice. Both Alice and Bob can then determine α^{ab}, which is their shared secret key [1].

An eavesdropper Oscar monitoring the transmissions between Alice and Bob would know G, α, α^a and α^b. Therefore the parameters G and α should be chosen so that it is computationally infeasible to determine the secret key α^{ab}. The problem of determining a given α and $\beta = \alpha^a$ is known as the discrete logarithm

problem. Numerous groups have been proposed for cryptographic use that capitilize on the difficulty of solving the discrete logarithm problem. One such group proposed is the group of non-singular matrices over a finite field, $GL(n, q)$ [6].

In 1998, Menezes and Wu showed how the discrete logarithm problem in $GL(n, q)$ could be reduced in probabilistic polynomial time to the logarithm problem in small extensions of the finite field $\mathbb{F}_q$ [2]. It has also been shown that the Index-Calculus method for determining the discrete logarithm in a finite field takes subexponential time [4]. Thus, the group $GL(n, q)$ offers no significant advantage over finite fields whose security is based on the difficulty of computing discrete logarithms in a group.

This thesis explores the Diffie-Hellman key exchange in $GL(n, q)$ and in $M_n(R)$. We present a cryptosystem capitilizing on the notion that Jordan Canonical form is not defined for a matrix over a ring, and thus the group of matrices over a ring $M_n(R)$ offers an advantage over the group $GL(n, q)$.

CHAPTER II

ALGEBRA AND LINEAR ALGEBRA

2.1 Finite Fields

In this section, we will review some definitions and properties of finite fields.

Definition 2.1.1 (Finite Field). *A finite field is a field $\mathbb{F}$ which contains a finite number of elements.*

Definition 2.1.2 (Characteristic of a Field). *The characteristic of a field $\mathbb{F}$ is the least positive integer n such that*

$$\underbrace{a + a + \cdots + a}_{n} = 0$$

for all $a \in \mathbb{F}$.

Proposition 2.1.1. *[3] If $\mathbb{F}_q$ is a finite field of order $q = p^m$, p prime, then the characteristic of $\mathbb{F}_q$ is p. Moreover, $\mathbb{Z}_p$ is a field and hence every finite field of order p is isomorphic to $\mathbb{Z}_p$.*

We will see later that the following representation of a finite field is very useful.

Proposition 2.1.2. *Let $f(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree m. Then $\mathbb{Z}_p[x]/(f(x))$ is a finite field of order p^m. Addition and multiplication of polynomials is performed modulo $f(x)$.*

Definition 2.1.3 (Order of an element). *The order of an element $\alpha \in \mathbb{Z}_p[x]/(f(x))$ is the integer e such that $\alpha^e = 1 \mod f(x)$. If α is a primitive element of $\mathbb{Z}_p[x]/(f(x))$, the order of α is $p^m - 1$.*

2.2 Matrices

This section will review some basic definitions and properties of matrices. To begin with, we will denote $M_n(\mathbb{F}_q)$ to be the set of all $n \times n$ matrices with entries

from a finite field $\mathbb{F}_q$, and we will denote $M_n(R)$ to be the set of all $n \times n$ matrices with entries from a ring R. We will denote the rank of any matrix A by $r(A)$.

Definition 2.2.1 (General Linear Group). *The general linear group, denoted* $GL(n,q)$ *or* $GL(n,\mathbb{F}_q)$*, is the set of all non-singular* $n \times n$ *matrices over* $\mathbb{F}_q$ *under matrix multiplication.*

The order of $GL(n,q)$ is $\prod_{i=0}^{n-1}(q^n - q^i)$ [2].

Definition 2.2.2 (Characteristic Polynomial, Eigenvalues). *Let* $A \in M_n(\mathbb{F}_q)$*. The characteristic polynomial of* A *is* $p_A(x)$*, where* $p_A(x) = \det(A - Ix)$*;* $p_A(x)$ *is a polynomial of degree* n *in* $\mathbb{F}_q[x]$*. Let* E *denote the splitting field of* $p_A(x)$ *over* $\mathbb{F}_q$*. The roots* $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ *of* $p_A(x)$ *in* E *are the eigenvalues of* A*.*

Definition 2.2.3 (Eigenvector). *Let* λ *be an eigenvalue of* A*. A nonzero vector* u *is called a generalized eigenvector of rank* t *corresponding to* λ *if* $(A - \lambda I)^t u = 0$ *and* $(A - \lambda I)^{t-1} u \neq 0$*.*

2.3 Jordan Canonical Form

In this section we review the Jordan Canonical form of a matrix. It is important to note that any matrix with coefficients in an algebraically closed field can be put into Jordan Canonical form [3].

Definition 2.3.1 (Jordan Block). *A Jordan block of order* d *corresponding to* λ *is a* $d \times d$ *upper-triangular matrix of the form*

$$J_d(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}$$

A Jordan matrix is a direct sum of Jordan blocks.

Proposition 2.3.1. *[5] For every matrix $A \in M_n(\mathbb{F}_q)$ there exists a matrix $Q \in GL(n, E)$ such that $Q^{-1}AQ = J_A$, where*

$$J_A = J_{n_1}(\lambda_1) \oplus \cdots \oplus J_{n_s}(\lambda_s)$$

is a Jordan matrix, $\lambda_1, \lambda_2, \ldots, \lambda_s$ are the eigenvalues of A (not necessarily distinct), and $\sum_{i=1}^{s} n_i = n$.

The Jordan matrix J_A is unique up to rearrangement of the component Jordan blocks and is called the Jordan Canonical form of A.

Proposition 2.3.2. *[2] Let λ be an eigenvalue of $A \in GL(n, q)$ of multiplicity m.*

1. *If c is the smallest positive integer for which $rank(A - \lambda I)^c = rank(A - \lambda I)^{c+1}$, then the number of Jordan blocks corresponding to λ is $n - rank(A - \lambda I)$, and c is the size of the largest such block.*

2. *The number of Jordan blocks of size at least k in J_A corresponding to λ is $rank(A - \lambda I)^{k-1} - rank(A - \lambda I)^k$.*

3. *The number of Jordan blocks of size exactly k in J_A corresponding to λ is $rank(A - \lambda I)^{k+1} - 2rank(A - \lambda I)^k + rank(A - \lambda I)^{k-1}$.*

The following theorems provide us with a way to determine the order of a matrix $A \in GL(n, q)$. This will be useful to us later.

Theorem 2.3.1. *[2] The order of the Jordan block $J = J_d(\lambda)$ is $ord(\lambda)p\{d\}$, where $p\{d\}$ denotes the smallest power of p greater than or equal to d.*

Proof. [2] Let $s = ord(\lambda)$ and $u = p\{d\}$. Because $ord(\lambda) = p^m - 1$ for some m and $u = p\{d\}$ is a power of p, then $\gcd(s, u) = 1$. It can be shown that J^l is an upper-triangular matrix with (i, j)-entry equal to $\lambda^{l-j+1}\binom{l}{j-i}$ for $1 \leq i \leq j \leq d$. Thus $J^l = I$ if and only if $\lambda^l = 1$ and $\binom{l}{k} \equiv 0 \pmod{p}$ for each $1 \leq k \leq d - 1$. Now,

since u is a power of the characteristic p, $(1+x)^{su} = (1+x^u)^s$ in $\mathbb{Z}_p[x]$. Computing coefficients of x^k yields $\binom{su}{k} \equiv 0 \pmod{p}$, for each $1 \leq k \leq u-1$. Since $\lambda^{su} = 1$, it follows that $J^{su} \equiv I$ and so $ord(J)|su$. Suppose now that $ord(J) = sw$, where w is a divisor of u, $w < u$. Since $J^{sw} \equiv I$, we have $\binom{sw}{k} \equiv 0 \pmod{p}$ for each $l \leq k \leq d-1$. In particular, $\binom{sw}{w} \equiv 0 \pmod{p}$ since $w \leq d-1$. But equating coefficients of x^w in $(1+x)^{sw} = (1+x^w)^s$ yields $\binom{sw}{w} \equiv s \pmod{p}$ where $s \neq 0 \pmod{p}$, thus contradicting the previous statement. We conclude that $ord(J) = su$, as required. □

Theorem 2.3.2. *[2] Let $A \in GL(n,q)$. Let the distinct eigenvalues of A in E be $\lambda_1, \lambda_2, \ldots, \lambda_n$. Then the order of A is*

$$ord(A) = lcm(ord(\lambda_1), ord(\lambda_2), \ldots, ord(\lambda_n))p\{t\}$$

where t is the size of the largest Jordan block in J_A.

Proof. [2] Let the Jordan Canonical form of A be $J_A = J_1 \oplus J_2 \oplus \cdots \oplus J_s$, and let $Q \in GL(n,E)$ be a matrix such that $Q^{-1}AQ = J_A$. Then $ord(A) = ord(J_A) = lcm(ord(J_1), ord(J_2), \ldots, ord(J_s))$. The result now follows from theorem 2.3.1. □

CHAPTER III
PUBLIC-KEY CRYPTOGRAPHY

3.1 The Diffe-Hellman Key Exchange

Suppose users Alice and Bob want to exchange information over a non-secure channel. Alice and Bob can use the Diffie-Hellman key exchange to agree upon a secret cryptographic key.

The method is as follows. Alice and Bob first choose a finite abelian (multiplicatively written) group G, and some element $\alpha \in G$. Alice then selects a random integer a and transmits α^a to Bob. Then Bob selects a random integer b and sends α^b to Alice. Now, both Alice and Bob can determine their shared secret key, α^{ab}.

The Diffie-Hellman key exchange is presented in the figure below.

Step 1: Alice chooses an integer a at random.
Step 2: Alice computes α^a and sends it to Bob.
Step 3: Bob chooses an integer b at random.
Step 4: Bob computes α^b and sends it to Alice.
Step 5: Alice computes

$$(\alpha^b)^a = \alpha^{ab}.$$

and Bob computes

$$(\alpha^a)^b = \alpha^{ab}.$$

Thus α^{ab} is their shared secret key.

Figure 3.1: Diffie-Hellman key exchange [4]

Suppose that Oscar is monitoring the transmissions between Alice and Bob. Oscar then knows G, α, α^a and α^b. Therefore, the parameters G and α should be chosen so that it is computationally infeasible for Oscar to then determine α^{ab} [1].

However, determing α^{ab} reduces to determining a or b. But, the problem of finding a, for example, given α and $\beta = \alpha^a$, is the Discrete Logarithm Problem which will be described in the next section.

We will now provide a trivial example of the Diffie-Hellman Key Exchange.

Example 3.1.1. *Let $G = \mathbb{Z}_5^*$ and let $\alpha = 3 \in \mathbb{Z}_5^*$. Suppose Alice chooses a random integer $a = 74$ and transmits*

$$\alpha^a = 3^{74} \mod 5 = 4 \mod 5$$

to Bob. Bob selects a random integer $b = 55$ and transmits

$$\alpha^b = 3^{55} \mod 5 = 2 \mod 5$$

to Alice. To find their shared key, Alice computes

$$\alpha^{ab} = \alpha^{ba} = (\alpha^b)^a = (2)^{74} \mod 5 = 4 \mod 5$$

and Bob computes

$$\alpha^{ab} = (\alpha^a)^b = (4)^{55} \mod 5 = 4 \mod 5.$$

Thus,

$$\alpha^{ab} = 4$$

is their shared secret key.

3.2 Discrete Logarithm Problem

Many public-key cryptosystems are based on the difficulty of the discrete logarithm problem, denoted DLP. The following figure describes the problem (Figure 3.2).

Problem Instance: G is a finite group, $\alpha \in G$, $\beta \in <\alpha>$.

Objective: Find an integer a, such that

$$\alpha^a = \beta.$$

We will denote this integer a by $\log_\alpha \beta$.

Figure 3.2: Discrete Logarithm Problem [1]

There currently is no polynomial-time algorithm for the DLP over $\mathbb{Z}_p^*$, but in order to prevent known attacks, p should have at least 150 digits, and $p-1$ should have at least one large prime factor [1].

As is the case for the DLP in $\mathbb{Z}_p^*$, if the group G is chosen carefully, the DLP is an extremely difficult problem to solve. However, the DLP for $\mathbb{F}_q^*$ can be solved in subexponential time using the Index Calculus method [4]. Over the years, numerous groups have been suggested as possible candidates to make the DLP difficult to solve. One such group is the group of non-singular matrices over a finite field, $GL(n, q)$.

CHAPTER IV

THE DIFFIE-HELLMAN KEY EXCHANGE IN $GL(n, q)$

4.1 Reduction to Jordan Canonical Form

As stated earlier, any matrix with entries from an algebraically closed field can be reduced to Jordan Canonical Form. The following algorithm reduces a matrix $A \in GL(n, q)$ to Jordan Canonical Form.

Algorithm 4.1.1. *[2]*

Input: A matrix $A \in GL(n, q)$

Output: The Jordan Canonical form J_A *of* A

1. *Use the Hessenberg algorithm to find the characterisitc polynomial* $p_A(x)$ *of* A.

2. *Find the factorization of* $p_A(x)$ *over* $\mathbb{F}_q$ *using, for example, Ben-Or's algorithm:* $p_A(x) = f_1^{e_1} f_2^{e_2} \cdots f_s^{e_s}$, *where each* f_i *is an irreducible polynomial of degree* m_i. *Let the roots of* f_i *in* $\mathbb{F}_{q^{m_i}}$ *be* α_{ij}, $1 \leq j \leq m_i$. *Note that we may conveniently represent the field* $\mathbb{F}_{q^{m_i}}$ *as* $\mathbb{F}_q[x]/(f_i(x))$. *In this representation, we simply have* $\alpha_{i1} = x$, *and* $\alpha_{ij} = x^{q^{j-1}} \mod f_i(x)$ *for* $2 \leq j \leq m_i$.

3. *For* i *from* 1 *to* s, *do the following:*

   (a) *Set* $r_0 \longleftarrow n$

   (b) *Compute* $(A - \alpha_{i1} I)^a$ *and* $r_a = r(A - \alpha_{i1} I)^a$ *for* $a = 1, 2, \ldots, c, c+1$, *where* c *is the smallest positive integer such that* $r_c = r_{c+1}$

   (c) *Let* J_{i1} *be the direct sum of* $(r_{a+1} - 2r_a + r_{a-1})$ *Jordan blocks of order* a *corresponding to* α_{i1}, $1 \leq a \leq c$.

   (d) *Let* J_{ij} *be the same matrix as* J_{i1} *but with* α_{i1} *replaced by* α_{ij}, $2 \leq j \leq m_i$

   (e) *Set* $J_i \longleftarrow J_{i1} \oplus J_{i2} \oplus \cdots \oplus J_{im_i}$.

4. *Set* $J_A \longleftarrow J_1 \oplus J_2 \oplus \cdots \oplus J_s$.

Theorem 4.1.1. *[2] Algorithm 4.1.1 takes expected polynomial time.*

Proof. [2] Hessenberg's algorithm takes polynomial time while Ben-Or's algorithm takes expected polynomial time. In each iteration of Step 3, the computations are performed in the field $\mathbb{F}_{q^{m_i}}$. Since $m_i \leq n$, we have $\log q^{m_i} \leq n \log q$, and so each iteration of Step 3 takes polynomial time. Finally, since Step 3 is iterated s times, and $s \leq n$, we see that the expected running time of Algorithm 4.1.1 is bounded by a polynomial n and $\log q$. □

We will now present an example of such a reduction.

Example 4.1.1. *Let $\mathbb{F}_q$ be the finite field $\mathbb{Z}_{11}$, and let $A \in M_3(\mathbb{Z}_{11})$ such that*

$$A = \begin{pmatrix} 6 & 2 & 1 \\ 3 & 4 & 9 \\ 10 & 0 & 7 \end{pmatrix}.$$

First, we will use the Hessenberg algorithm to find the characteristic polynomial $p_A(x)$ of A, which is

$$p_A(x) = x^3 + 5x^2 + x + 9.$$

Next, we will use Ben-Or's algorithm to factor $p_A(x)$ over $\mathbb{Z}_{11}[x]$:

$$p_A(x) = (x^2 + 10x + 7)(x + 6).$$

Each of $x^2 + 10x + 7$ and $x + 6$ are irreducible polynomials of degree 2 and degree 1, respectively. Now, we find the roots of $x^2 + 10x + 7$ and $x + 6$ in $\mathbb{Z}_{11^2}$.
We do so by representing the field $\mathbb{Z}_{11^2}$ as $\mathbb{Z}_{11}/(x^2 + 10x + 7)$ and hence

$$\alpha_{11} = x, \alpha_{12} = x^{11} \mod x^2 + 10x + 7 = 10x + 1$$

are the roots of $x^2 + 10x + 7$. The root of $x + 6$ is $\alpha_{21} = -6 \mod 11 = 5 \mod 11$. Next, we set $r_0 = 3$ and then compute $(A - \alpha_{i1}I)^a$ and $r_a = r(A - \alpha_{i1}I)^a$ for $a = 1, 2, \ldots, c, c + 1$, where c is the smallest positive integer such that $r_c = r_{c+1}$

$$(A - \alpha_{11}I) = (A - xI) = \begin{pmatrix} 6-x & 2 & 1 \\ 3 & 4-x & 9 \\ 10 & 0 & 7-x \end{pmatrix}$$

where $r_1 = r(A - xI) = 2$, *and*

$$(A - \alpha_{11}I)^2 = (A - xI)^2 = \begin{pmatrix} (6-x)^2 + 16 & 20 - 4x & 31 - 2x \\ 120 - 6x & 6 + (4-x)^2 & 102 - 18x \\ 130 - 20x & 20 & 10 + (7-x)^2 \end{pmatrix}^2$$

such that $r_2 = r(A - xI)^2 = 2$.

Thus, for $\alpha_{11} = x$, $c = 1$, *and so we let* J_{11} *be the direct sum of*

$$(r_{a+1} - 2r_a + r_{a-1}) = (r_2 - 2r_1 + r_0) = 1$$

Jordan block of order 1 *corresponding to* α_{11}, *i.e.,* $J_{11} = [x]$.

Doing the same for α_{12} *and* α_{21}, *we get* $J_{12} = [10x + 1]$ *and* $J_{21} = [5]$. *Thus the Jordan Canonical form of* A *is*

$$J_A = \begin{pmatrix} x & 0 & 0 \\ 0 & 10x+1 & 0 \\ 0 & 0 & 5 \end{pmatrix}.$$

4.2 Reduction of the DLP

In this section, we will examine the DLP in $GL(n, q)$. As we mentioned earlier, to decrypt a message sent using the Diffie-Hellman key exchange, we only need to find l given $B = A^l$ where $A, B \in GL(n, q)$. This DLP in $GL(n, q)$ can be reduced to the DLP in small extensions of $\mathbb{F}_q$.

The following algorithm does such a reduction.

Algorithm 4.2.1. *[2]*

Input: Matrices $A, B \in GL(n, q)$ *with*

Output: The integer l.

1. *Use the Hessenberg algorithm to find the characterisitc polynomial* $p_A(x)$ *of* A.

2. *Find the factorization of* $p_A(x)$ *over* $\mathbb{F}_q$ *using, for example, Ben-Or's algorithm:* $p_A(x) = f_1^{e_1} f_2^{e_2} \cdots f_s^{e_s}$, *where each* f_i *is an irreducible polynomial of degree* m_i. *Let the roots of* f_i *in* $\mathbb{F}_{q^{m_i}}$ *be* α_{ij}, $1 \leq j \leq m_i$. *Note that we may conveniently represent the field* $\mathbb{F}_{q^{m_i}}$ *as* $\mathbb{F}_q[x]/(f_i(x))$. *In this representation, we simply have* $\alpha_{i1} = x$, *and* $\alpha_{ij} = x^{q^{j-1}} \mod f_i(x)$ *for* $2 \leq j \leq m_i$.

3. *For* i *from* 1 *to* s, *do the following:*

   (a) *Compute* $(A - \alpha_{i1} I)^a$ *and* $r_a = r(A - \alpha_{i1} I)^a$ *for* $a = 1, 2, \ldots, c, c+1$, *where* c *is the smallest positive integer such that* $r_c = r_{c+1}$.

   (b) *Find an eigenvalue* μ_{i1} *corresponding to* α_{i1} *by solving* $(A - \alpha_{i1} I)y = 0$.

   (c) *Construct a matrix* $Q_{i1} \in GL(n, q^m)$ *whose first column is* μ_{i1}

   (d) *Compute* $D_{i1} \longleftarrow Q_{i1}^{-1} B Q_{i1}$

   (e) *The* $(1,1)$ *entry of* D_{i1} *is* α_{i1}^l, *and so one can find* l *modulo* $ord(\alpha_{i1})$ *by solving a discrete logarithm problem in* $\mathbb{F}_{q^{m_i}}$.

4. *Let* t *be the maxilmum of the* c *values found in step 3, part (a). If* $t > 1$, *then do the following:*

   (a) *Let* $\lambda \in \mathbb{F}_{q^m}$ *be an eigenvalue which has a corresponding Jordan block of size* t.

   (b) *Find a basis* B_1 *for* $N((A - \lambda I)^{t-1})$.

   (c) *Find a basis* B_2 *for* $N((A - \lambda I)^t)$.

   (d) *Hence find a vector* u *in* B_2 *which is not in the subspace spanned by* B_1. *(*u *is a generalized eigenvector of rank* t.*)*

   (e) *Set* $u_t \longleftarrow u$, *and* $u_j \longleftarrow (A - \lambda I)u_{j+1}$ *for* $j = t-1, t-2, \ldots, 2, 1$.

   (f) *Construct a matrix* $Q \in GL(n, q^m)$ *whose first* t *columns are* $u_1, u_2, \ldots, u_t$.

(g) *Compute* $Q^{-1}AQ$ *and* $D \longleftarrow Q^{-1}BQ$.

(h) *The* $(1,1)$ *entry of* D *is* λ^l *and the* $(1,2)$ *entry of* D *is* $l\lambda^{l-1}$. *If* $p\{t\} = p$, *then first compute* λ^{l-1} *as* λ^l/λ, *and then divide* $l\lambda^{l-1}$ *by* λ^{l-1} *to obtain* $l \mod p$.

(i) *If* $p\{t\} \geq p^2$ *then let* J *be the* $t \times t$ *Jordan block in the upper-left hand corner of* $Q^{-1}AQ$. *Set* $s \longleftarrow ord(\lambda)$, $l' \longleftarrow l \mod s$ *(which was computed in step 3), and compute* $J^{l'}, J^{l'+s}, J^{l'+2s}, \ldots$ *until* $J^{l'+js}$ *is equal to the* $t \times t$ *matrix in the upper left-hand corner of* D. *Then* $l \mod p\{t\} = j$.

5. *Find* $l \mod ord(A)$ *by using the generalized Chinese Remainder Theorem.*

Theorem 4.2.1. *[2] Algorithm 4.2.1 is an expected poynomial-time reduction of the discrete logarithm problem in* $GL(n,q)$ *to the discrete logarithm problem in* $\mathbb{F}_{q^{m_i}}$, $1 \leq i \leq s$.

Proof. [2] Hessenberg's algorithm takes polynomial time, while Ben-Or's algorithm takes expected polynomial time. Each iteration of Step 3 involves linear algebra over $\mathbb{F}_{q^{m_i}}$ where $m_i \leq n$. Since $\log q^{m_i} \leq n \log q$ and $s \leq n$, Step 3 is a polynomial time reduction. Finally, Step 4 involves linear algebra over $\mathbb{F}_{q^m}$, where $m \leq n$. If $p\{t\} \geq p^2$, then $p\{t\} < n^2$, and so the process of computing $J^{l'+js}$ in Step 4, part (i) is iterated at most n^2 times. This proves the statement of the theorem. □

We will now provide an example of the reduction of the DLP in $GL(n,q)$ to the DLP in small extensions of $\mathbb{F}_q$.

Example 4.2.1. *Let* $\mathbb{F}_q = \mathbb{Z}_{11}$ *and let*

$$A = \begin{pmatrix} 6 & 2 & 1 \\ 3 & 4 & 9 \\ 10 & 0 & 7 \end{pmatrix}$$

$$B = \begin{pmatrix} 3 & 8 & 8 \\ 4 & 2 & 10 \\ 8 & 8 & 8 \end{pmatrix}$$

where $A, B \in GL(3, \mathbb{Z}_{11})$, *and* $B = A^l$.

Our goal is to determine l. *As in example 4.2.1, we find the characteristic polynomial of* A *to be*

$$p_A(x) = x^3 + 5x^2 + x + 9 = (x^2 + 10x + 7)(x + 6)$$

and we find the roots of $x^2 + 10x + 7$ *to be* $\alpha_{11} = x$ *and* $\alpha_{12} = 10x + 1$, *and the root of* $x + 6$ *to be* $\alpha_{21} = 5$.

Now we find an eigenvector μ_{11} *corresponding to* α_{11} *by solving* $(A - xI)y = 0$, *i.e.,*

$$\begin{pmatrix} 6-x & 2 & 1 \\ 3 & 4-x & 9 \\ 10 & 0 & 7-x \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This is done much in the same way as would be done in $M_3(\mathbb{Z})$. *First, we reduce the matrix* $(A - \alpha_{11}I) = (A - xI)$ *using Gaussian elimination, keeping in mind that all calculations are done in* $\mathbb{Z}_{11}[x]/(x^2 + 10x + 7)$. *Hence*

$$A = \begin{pmatrix} 6-x & 2 & 1 \\ 3 & 4-x & 9 \\ 10 & 0 & 7-x \end{pmatrix}$$

reduces to

$$A = \begin{pmatrix} 1 & 0 & x+4 \\ 0 & 1 & 5x+7 \\ 0 & 0 & 0 \end{pmatrix}.$$

Then we solve for $\begin{pmatrix} u \\ v \\ w \end{pmatrix}$ *and get* $\mu_{11} = \begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} 10x+7 \\ 6x+4 \\ 1 \end{pmatrix}$.

The eigenvalues corresponding to $10x + 1$ *and* 5 *are found in the same manner and are* $\mu_{12} = \begin{pmatrix} x+6 \\ 5x+10 \\ 1 \end{pmatrix}$ *and* $\mu_{21} = \begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix}$, *respectively.*

Next, we construct a non-singular matrix $Q_{11} \in GL(3, \mathbb{Z}_{11^2})$ *whose first column is* μ_{11}*:*

$$Q_{11} = \begin{pmatrix} 10x+7 & x+6 & 0 \\ 6x+4 & 2x & 5 \\ 1 & 9x+7 & x \end{pmatrix}$$

where

$$Q_{11}^{-1} = \begin{pmatrix} 10 & x & 6 \\ 6x+1 & 3x+6 & 9x+9 \\ 5x & x+6 & x+5 \end{pmatrix}.$$

Doing the same for μ_{12} *and* μ_{21}*, we get*

$$Q_{12} = \begin{pmatrix} x+6 & 2x & 1 \\ 5x+10 & 3x+9 & x+2 \\ 1 & 8x+1 & 5 \end{pmatrix}, Q_{12}^{-1} = \begin{pmatrix} 2x+9 & x+1 & x+8 \\ 9x+5 & x+2 & 6x+4 \\ 4x+10 & 8x+4 & 9x+10 \end{pmatrix}$$

and

$$Q_{21} = \begin{pmatrix} 2 & 7 & 10 \\ 4 & 1 & 0 \\ 1 & 4 & 3 \end{pmatrix}, Q_{21}^{-1} = \begin{pmatrix} 6 & 5 & 2 \\ 9 & 3 & 3 \\ 8 & 9 & 3 \end{pmatrix}.$$

Now, we compute $D_{11} = Q_{11}^{-1}BQ_{11}$*,* $D_{12} = Q_{12}^{-1}BQ_{12}$ *and* $D_{21} = Q_{21}^{-1}BQ_{21}$*, but we are only concerned with the* $(1,1)$ *entry of each of these three matrices, which is* $\alpha_{11}^l = 7x+8$*,* $\alpha_{12}^l = 4x+4$ *and* $\alpha_{21}^l = 1$*, respectively.*

Next, we must compute the order of the roots x*,* $10x+1$*, and* 5*. These are* 120*,* 120*, and* 10*, respectively.*

Thus, we can find l *modulo* $ord(\alpha_{ij})$ *by solving discrete logarithm problems in* $\mathbb{Z}_{11}[x]/(x^2+10x+7)$ *and* $\mathbb{Z}_{11}$*.*

We can find l *for* $7x+8 = x^l \mod 11$*,* $4x+4 = (10x+1)^l \mod 11$*, and* $1 = 5^l \mod 11$ *using a variety of methods, including the Index-Calculus algorithm and the Brute force method to name a couple. We use brute force to find that*

$$20 = l \mod 120$$

$$20 = l \mod 120$$

$$10 = l \mod 10.$$

Finally, we find $l \mod ord(A)$ *using the Generalized Chinese Remainder Theorem. Hence*

$$l = 20.$$

This is the integer we are looking for as we can see when we let $l = 20$ *in our original problem* $A^l = B$.

$$A^{20} = \begin{pmatrix} 6 & 2 & 1 \\ 3 & 4 & 9 \\ 10 & 0 & 7 \end{pmatrix}^{20} = \begin{pmatrix} 3 & 8 & 8 \\ 4 & 2 & 10 \\ 8 & 8 & 8 \end{pmatrix} = B$$

CHAPTER V

THE DIFFIE-HELLMAN KEY EXCHANGE IN $M_n(R)$

5.1 Jordan Form

As we have stated before, any matrix with coefficients in an algebraically closed field can be reduced to Jordan Canonical form. So, what about a matrix $A \in M_n(R)$, where R is a ring? Can we reduce A to Jordan Canonical form using traditional methods or the algorithm described in Section 4.1?

Eigenvalues are not defined for a matrix $A \in M_n(R)$, where R is a ring. Since there is no definition of eigenvalue for a matrix A, then characteristic polynomial is not defined for A. As a result of this, Algorithm 4.1.1 and Algorithm 4.2.1 cannot be implemented, as the first step in both algorithms involve finding the characteristic polynomial of a matrix.

Now, we will provide an example which illustrates how a matrix over a ring cannot be reduced to Jordan Canonical form using Algorithm 4.1.1 or traditional methods.

Example 5.1.1. *Let $R = \mathbb{Z}_6$ and let*

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Hence the characteristic polynomial $p_A(x)$ of A is

$$p_A(x) = (x-2)(x-3).$$

Setting $p_A(x) = 0$ gives the eigenvalues of A: $x = 3, x = 2$. However, if we expand $(x-2)(x-3)$, we get

$$(x-2)(x-3) = x^2 - 5x + 6.$$

Alas, $x^2 - 5x + 6$ modulo 6 is $x^2 - 5x$, and setting $x^2 - 5x = 0$ yields $x^2 - 5x = x(x-5) = 0$. Thus, $x = 0$ and $x = 5$ are also eigenvalues of A.

But, as eigenvalues are defined, there should only be $n = 2$ eigenvalues for the matrix A. Thus, we can conclude that the eigenvalues for the matrix A are undefined.

As the reduction of a matrix A to Jordan Canonical form is based on finding eigenvalues for the matrix A, we can conclude that the reduction of a matrix $A \in M_n(R)$ cannot be done using Algorithm 4.1.1 or traditional methods.

5.2 Cryptosystem

In this section, we will present a public-key cryptosystem which makes use of the Diffie-Hellman key exchange in matrices over a ring.

This cryptosystem's security is based on the difficulty involved in reducing a matrix with ring entries to Jordan Canonical form. During the Diffie-Hellman key exchange over matrices in $M_n(R)$, if Oscar cannot reduce a matrix to Jordan Canonical form, then he cannot obtain the secret cryptographic key. Thus any cryptosystem which uses the secret key during encryption and decryption will be sufficiently difficult to break.

The cryptosystem is as follows.

Step 1: Alice and Bob use the Diffie-Hellman key exchange to find the shared secret cryptographic key $A^{ab} = B \in M_n(R)$.

Step2: Alice and Bob map B into a group G which gives an element $B_g \in G$ (An example of this mapping will be described later.) The group G is public information.

Step 3: Alice encrypts a message $M \in G$ by multiplying M and B_g ,i.e. $M * B_g = Y$ and sends Y to Bob.

Step 4: To decrypt the message, Bob computes the inverse of B_g and recovers the message M by computing $Y * B_g^{-1} = M$

5.2.1 Example

Now, we will provide an example of the cryptosystem.

Example 5.2.1. *Alice and Bob perform the Diffie-Hellman key exchange over* $M_3(\mathbb{Z}_{10})$.

Let

$$A = \begin{pmatrix} 6 & 2 & 1 \\ 3 & 4 & 9 \\ 9 & 0 & 7 \end{pmatrix}.$$

Alice sends Bob

$$A^a = A^6 = \begin{pmatrix} 9 & 8 & 6 \\ 4 & 8 & 5 \\ 0 & 6 & 7 \end{pmatrix}.$$

Bob sends Alice

$$A^b = A^9 = \begin{pmatrix} 3 & 4 & 6 \\ 0 & 8 & 1 \\ 6 & 2 & 3 \end{pmatrix}.$$

Thus the shared secret cryptographic key is

$$A^{ab} = A^{54} = \begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix} = B.$$

The group G *is* $\mathbb{Z}_{11}^{*9} = \{(g_1, g_2, \ldots, g_9) | g_i \in \mathbb{Z}_{11}^*\}$ *with multiplication defined componen wise:*

$$(x_1, x_2, \ldots, x_9) * (g_1, g_2, \ldots, g_9) = (x_1 * g_1, x_2 * g_2, \ldots, x_9 * g_9),$$

and the map $\pi : M_3(\mathbb{Z}_{10}) \longrightarrow G$ *is defined by*

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \mapsto (\hat{a_{11}} + 1, \hat{a_{12}} + 1, \hat{a_{13}} + 1, \ldots \hat{a_{33}} + 1,)$$

where $\hat{a_{ij}}$ *is the same number in* $\mathbb{Z}_{11}$ *as* a_{ij} *in* $\mathbb{Z}_{10}$.

Alice wants to send

$$M = (6, 7, 10, 4, 1, 5, 5, 2, 9) \in G$$

to Bob. She takes

$$B = \begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix}$$

and maps each element of B *to an element of* $\mathbb{Z}_{11}$ *via the mapping*

$$0 \mapsto 1, 1 \mapsto 2, \ldots, 10 \mapsto 11.$$

Thus B *becomes*

$$B_g = (8, 9, 9, 7, 9, 10, 5, 3, 10).$$

Now, Alice multiplies M *and* B_g *component-wise:*

$$\begin{aligned} &(6, 7, 10, 4, 1, 5, 5, 2, 9) * (8, 9, 9, 7, 9, 10, 5, 3, 10) \\ &= (6 * 8, 7 * 9, 10 * 9, 4 * 7, 1 * 9, 5 * 10, 5 * 5, 2 * 3, 9 * 10) \mod 11 \\ &= (4, 8, 2, 6, 9, 6, 3, 6, 2). \end{aligned}$$

Alice sends the encrypted message

$$Y' = (4, 8, 2, 6, 9, 6, 3, 6, 2)$$

to Bob.

Bob takes

$$B = \begin{pmatrix} 7 & 8 & 8 \\ 6 & 8 & 9 \\ 4 & 2 & 9 \end{pmatrix}$$

and maps it to

$$(8, 9, 9, 7, 9, 10, 5, 3, 10).$$

Bob then computes the inverses of each element in B_g *modulo* 11, *and gets*

$$(8, 9, 9, 7, 9, 10, 5, 3, 10)^{-1} = (7, 5, 5, 8, 5, 10, 9, 4, 10).$$

Finally, Bob multiplies this vector and the encrypted message M component-wise to get the original message:

$$(4, 8, 2, 6, 9, 6, 3, 6, 2) * (7, 5, 5, 8, 5, 10, 9, 4, 10) \mod 11$$

$$= (4 * 7, 8 * 5, 2 * 5, 6 * 8, 9 * 5, 6 * 10, 3 * 9, 6 * 4, 2 * 10)$$

$$= (6, 7, 10, 4, 1, 5, 5, 2, 9).$$

As one can see, this is the original message M that Alice encrypted.

CHAPTER VI
CONCLUSION AND FUTURE WORK

As the future of technology becomes a reality, the process of keeping information secure is becoming increasingly more difficult. It is for this reason that we have presented this cryptosystem. We have presented a cryptosystem that is more difficult to break than one whose security is based on the difficulty of solving the discrete logarithm in $GL(n, q)$.

This is accomplished by improving on an existing method. The Diffie-Hellman key exchange is not new by any means, and over the years, numerous mathematicians have proposed many groups for the exchange to take place in. Some of these groups have demonstrated strengths of the Diffie-Hellman key exchange, and some have demonstrated weaknesses. The group $GL(n, q)$ is an example of the latter.

In this paper, we have improved upon the central idea of suggesting the group $GL(n, q)$, i.e., matrix multiplication is a time-consuming process. This idea therefore makes it harder for an eavesdropper, Oscar, to find the secret key. We have shown that the group $M_n(R)$ satisfies the requirement that the calculations in G be difficult, because the group elements are matrices. More importantly, we have shown that an element of $M_n(R)$ cannot be reduced to Jordan Canonical form, thus making it extremely difficult for Oscar to find the key using the methods available to him.

As technology evolves, so too does cryptography. There are several options for future work relating to this paper. One area might include defining a protocol where the only information about the group that is sent, is sent during the Diffie-Hellman key exchange, i.e., if $M_n(\mathbb{Z}_{p-1})$ is the group used for the Diffie-Hellman key exchange, then the two users would know to switch to the group $M_n(\mathbb{Z}_p)$ without having to communicate this across the channel. This would make it even more difficult for an eavesdropper to decrypt the message. Also, the research could be expanded to include more cryptosystems that incorporate the basic idea of our cryptosystem.

BIBLIOGRAPHY

[1] Stinson D., *Cryptography: Theory and Practice*, CRC Press LLC, Boca Raton, FL, (1995), 116-188.

[2] Menezes A., Wu Y., "The discrete logarithm problem in $GL(n,q)$," *Ars Combinatoria* 6, 1998, 23-32.

[3] Hungerford T. W., *Algebra*, Holt, Rinehart and Winston, New York, (1974), 360.

[4] Menezes A., van Oorschat P., Vanstone S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, (1997), 45.

[5] Horn R., Johnson C., *Matrix Analysis*, Cambridge University Press, Cambridge, (1985), 385.

[6] Odoni R., Sanders R., Varadharajan V., "Public key distribution in matrix rings," *Electronic Letters* 20, 1984, 386-387.

PERMISSION TO COPY

In presenting this thesis in partial fulfillment of the requirements for a master's degree at Texas Tech University or Texas Tech University Health Sciences Center, I agree that the Library and my major department shall make it freely available for research purposes. Permission to copy this thesis for scholarly purposes may be granted by the Director of the Library or my major professor. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my further written permission and that any user may be liable for copyright infringement.

Agree (Permission is granted.)

_____ _____

Student Signature Date

Disagree (Permission is not granted.)

_____ _____

Student Signature Date