RVPLBAYITDMULVNDAINITCBJNINNGZRSVWYHIMULRZ

David Jekel and Seongjin Cho (Josh)
Math 136
Prof. John Palmieri and Ian Zemke
May 30, 2012

Cryptography is the practice and study of techniques for secure communication in the presence of the third parties. Before the modern era, cryptography was concerned solely with encrypting messages to ensure secret communications from spies. However, moving toward the modern era, cryptography has become increasingly intricate. When new technologies, such as the internet, produced widespread communication over insecure channels, cryptography became a day-to-day activity for ordinary people (even if not many people realize it).

We will introduce the basic concepts of cryptography and modular matrix algebra through an exploration of the Hill Cipher. While the Hill Cipher comes nowhere near the complexity and security of computer-age coding systems, it is one of the best ciphers invented before the digital age. First, we will define cryptosystems and the Hill Cipher mathematically. Then because Hill Ciphers involve matrix multiplication using modular arithmetic, we will modify the normal tools used for working with real matrices to deal with modular matrices. We will apply our techniques to crack a Hill Cipher and then to make a more secure cipher. We assume the reader is familiar with real-numbered matrices, including matrix multiplication, elementary matrices, inverting matrices by row reduction, and computing determinants.

1 Introduction to Cryptosystems and the Hill Cipher

The fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure network in such a way that the third party, Oscar, cannot understand the conversation. Alice encrypts the plaintext, using the predetermined key, and sends the result ciphertext over the network. Oscar, although succeeded to intercept the ciphertext in the network by spying, cannot determine what the plaintext meant, but Bob who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext.

A formal definition of a cryptosystem, taken from Stinson, is as follows.

Definition 1 (Cryptosystem)**.** *A cryptosystem consists of five sets (P, C, K, E, D), where the following conditions are satisfied:*

1. *P is a finite set of possible plaintext elements.*
2. *C is a finite set of possible ciphertext elements.*
3. *K, the keyspace, is a finite set of possible keys.*
4. *For each $\kappa \in K$, there is an encryption rule $e_\kappa \in E$ and a corresponding decryption rule $d_\kappa \in D$. Each $e_\kappa : P \to C$ and $d_\kappa : C \to P$ are functions such that $d_\kappa(e_\kappa(x)) = x$ for every plaintext element $x \in P$.*

The interesting fact about property 4 is that clearly, each encryption function e_κ is an injective function; otherwise, decryption could be not be accomplished in an unambiguous manner. For example, if Alice sent an plaintext x_1 and x_2 through a encryption rule e_K such that

$$y = e_\kappa(x_1) = e_\kappa(x_2)$$

where $x_1 \neq x_2$, then Bob has no way of knowing whether y should decrypt to x_1 or x_2.

The mathematical definition of the Hill Cipher is as follows:

Definition 2 (Hill Cipher)**.** *Let n be a positive integer, let α be the number of characters in the alphabet, and let $\mathbb{Z}_\alpha$ be the set of integers 0 through $\alpha - 1$. The Hill Cipher cryptosystem is the cryptosystem where $P = C = \mathbb{Z}_\alpha^n$ (that is, the plaintext and ciphertext elements are strings of n letters represented by vectors in $\mathbb{Z}_\alpha^n$). K is the set of $n \times n$ invertible matrices over $\mathbb{Z}_\alpha$. E and D are both equal to the set of invertible linear transformations $\mathbb{Z}_\alpha^n \to \mathbb{Z}_\alpha^n$.*

For all $\mathbf{p} \in P$ and $\mathbf{c} \in C$ and $A \in K$,

$$\mathbf{e}_\kappa(\mathbf{p}) = A\mathbf{p} \quad \textit{and} \quad \mathbf{d}_\kappa(\mathbf{c}) = A^{-1}\mathbf{c}.$$

A Hill-2 Cipher, for instance, uses a 2×2 matrix. The letters of a plaintext are written as numbers, often as

$$\text{A} = 0, \text{B} = 1, \text{C} = 2, \ldots, \text{Z} = 25.$$

The plaintext is broken into pairs of numbers which are written as the columns of a matrix with two rows and as many columns are necessary. The plaintext matrix is left-multiplied by the key matrix. The numbers in the resulting matrix are turned back into letters and become the ciphertext. To make sure this resulting matrix has elements only consisting numbers 0 through 25, we use modular arithmetic, which we explain in the next section.

2 Modular Arithmetic for Matrices

As we will see, working with matrices using modular arithmetic can be challenging. We cannot count on the same assumptions as we did when working over fields like $\mathbb{R}$. Before we can work with modular matrices, we need to explain basic notation and theory in modular arithmetic.

Definition 3 (Congruence and mod)**.** *Suppose a and b are integers, and m is a positive integer. Then a mod m is the remainder when a is divided by m. To "reduce a mod m" simply means to find a mod m. The expression $a \equiv b \pmod m$ is called a "congruence." It is read "a is congruent to b modulo m." It means that a mod $m = b$ mod m, or equivalently $b - a$ is evenly divisible by m.*

Definition 4. *Suppose A and B are matrices. Then A mod m is matrix we get by reducing each element of A mod m. A and B are called congruent ($A \equiv B$) if the corresponding elements of A and B are congruent.*

Definition 5 (Modulus)**.** *The modulus $\mathbb{Z}_m$ is the set of integers 0 through m. (Sometimes, m is called the modulus as well.) The modulus has two operations, addition and multiplication; they are computed the same as integer addition and multiplication except that every answer is reduced mod m. They satisfy the following properties:*

1. *$\mathbb{Z}_m$ is closed under addition.*
2. *addition is commutative, i.e. $a + b = b + a$ for $a, b \in \mathbb{Z}_m$*
3. *addition is associative, i.e. $(a + b) + c = a + (b + c)$, $\forall\ a, b, c \in \mathbb{Z}_m$*
4. *0 is the additive identity, i.e. $a + 0 = 0 + a = a$, $\forall\ a \in \mathbb{Z}_m$*
5. *every element has an additive inverse, i.e. given $a \in \mathbb{Z}_m$, $\exists\ b \in \mathbb{Z}_m$ s.t. $a + b = 0$*
6. *$\mathbb{Z}_m$ is closed under multiplication, i.e. $a, b \in \mathbb{Z}_m$ implies that $a \cdot b \in \mathbb{Z}_m$*
7. *multiplication is commutative, i.e. $ab = ba$ $\forall\ a, b \in \mathbb{Z}_m$*
8. *multiplication is associative, i.e. $(ab)c = a(bc)$, $\forall\ a, b, c \in \mathbb{Z}_m$*
9. *1 is the multiplicative identity, i.e. $a \cdot 1 = 1 \cdot a = a$, $\forall\ a \in \mathbb{Z}_m$*

10. *multiplication distributes over addition, i.e.* $a(b+c) = ab + ac$ *and* $(b+c)a = ba + ca$, $\forall$ $a, b, c \in \mathbb{Z}_m$

In other words, the modulus $\mathbb{Z}_m$ satisfies all the properties of a field except one: not every number has a multiplicative inverse. For a given $a \in \mathbb{Z}_m$, there does *not necessarily* exist an $a^{-1} \in \mathbb{Z}_m$ satisfying $aa^{-1} = a^{-1}a = 1$. The first thing we can observe about $\mathbb{Z}_m$ is that matrix addition, multiplication, and determinants will work over $\mathbb{Z}_m$ just the same as they do over $\mathbb{R}$. These matrix operations are defined in terms of scalar addition and multiplication of the elements of matrices; we can perform all those operations over a modulus just as well as over a field. The following example illustrates matrix multiplication in $\mathbb{Z}_{26}$ as well as the basic idea of a Hill Cipher.

Example 1. *Use a Hill Cipher with the matrix* $\begin{pmatrix} 13 & 1 \\ 2 & 1 \end{pmatrix}$ *to encrypt the message "UNTITLED."*

Solution. Write the first message in a matrix:

$$\begin{pmatrix} \text{U} & \text{T} & \text{T} & \text{E} \\ \text{N} & \text{I} & \text{L} & \text{D} \end{pmatrix} \Longrightarrow \begin{pmatrix} 20 & 19 & 19 & 4 \\ 13 & 8 & 11 & 3 \end{pmatrix}$$

Now multiply by the code matrix:

$$\begin{pmatrix} 13 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 20 & 19 & 19 & 4 \\ 13 & 8 & 11 & 3 \end{pmatrix} = \begin{pmatrix} 13 & 21 & 24 & 3 \\ 1 & 20 & 23 & 11 \end{pmatrix} \Longrightarrow \begin{pmatrix} \text{N} & \text{V} & \text{Y} & \text{D} \\ \text{B} & \text{U} & \text{X} & \text{L} \end{pmatrix} \Longrightarrow \text{NBVUYXDL}$$

□

As we said before, not every number has a multiplicative inverse. This is an important difference: in order to decipher messages encoded with a Hill Cipher, we need to find the inverse of the key matrix, and if we are going to invert matrices, either by row reduction or cofactor expansion, we need multiplicative inverses of numbers. The following theorem, which we state without proof, establishes the condition for a number to have a multiplicative inverse in a modulus.

Theorem 1 (Multiplicative Inverses in $\mathbb{Z}_m$)**.** *$a \in \mathbb{Z}_m$ has a multiplicative inverse if and only if a and m are relatively prime, that is, $gcd(a, m) = 1$. Multiplicative inverses are unique within the modulus.*

From this theorem we can see that if m is prime, every nonzero number in $\mathbb{Z}_m$ has a multiplicative inverse (and $\mathbb{Z}_m$ is therefore a field). However, when m is not an prime number, not many elements in $\mathbb{Z}_m$ have a multiplicative inverse. For example, in $\mathbb{Z}_{26}$, only $1, 3, 5, 7, 11, 17, 25$ are relatively prime to 26, and their inverses are: $1^{-1} = 1$, $3^{-1} = 9$, $5^{-1} = 21$, $7^{-1} = 15$, $11^{-1} = 19$, $17^{-1} = 23$, and $25^{-1} = 25$. (One efficient way to compute inverses is the Extended Euclidean Algorithm. We do not have time to explain it here, but the reader may consult Stinson 163-166.)

Now that we understand inverses of numbers, we can move on to inverses of matrices:

Definition 6 (Inverses)**.** *Let A be a matrix over $\mathbb{Z}_m$. B is called a left inverse of A if $BA = I$ working modulo m, or equivalently $BA \equiv I \pmod m$. B is called a right inverse of A if $AB = I$. B is called an inverse of A if it is both a left and a right inverse.*

Theorem 2 (Conditions for Invertibility over a Modulus)**.** *A square matrix A is invertible over $\mathbb{Z}_m$ if and only if its determinant has a multiplicative inverse in $\mathbb{Z}_m$. If A is invertible, then A^{-1} is unique within the modulus. If A has a left inverse or a right inverse, then it is an inverse.*

Proof. Suppose a matrix A is invertible. Then

$$AA^{-1} = I \quad \text{and} \quad \det(A)\det(A^{-1}) = 1,$$

so the determinant of A has a multiplicative inverse.

If on the other hand the determinant of A has a multiplicative inverse, then the cofactor formula for the inverse will give us A^{-1} without using any multiplicative inverses other than the inverse of the determinant. We have not proven that a right inverse for A in a modulus is necessarily a left inverse for A, so we should verify that the inverse matrix given by this method is both a right and a left inverse for A.

We will use the cofactor formulae for the determinant and the inverse of an $n \times n$ matrix A as stated and proved by Treil (88-91), with slight changes in notation. Let $a_{i.j}$ be the entry of A in the i^{th} row and j^{th} column. Let $A_{i,j}$ be the matrix formed by removing row i and column j from A. Let $C_{i,j} = (-1)^{i+j}\det(A_{i,j})$. For any row i in A,

$$\det(A) = \sum_{j=1}^{n} a_{i,j}C_{i,j}$$

For any column j,

$$\det(A) = \sum_{i=1}^{n} a_{i,j}C_{i,j}$$

Let C be the matrix formed by putting the cofactors $C_{i,j}$ of A in row i and column j. Then

$$A^{-1} = (\det(A))^{-1}C^T$$

To show that this is a left inverse, compute $C^T A$. The i, i entry of $C^T A$ is,

$$\sum_{j=1}^{n} C_{j,i}a_{j,i} = \det(A)$$

The i, k entry of $C^T A$, $i \neq k$ is

$$\sum_{j=1}^{n} C_{j,i}a_{j,k}$$

which is the determinant for a matrix that is like A but with column i replaced by column k. This matrix has two columns which are the same, so its determinant is zero. Thus, all the non-diagonal entries of $C^T A$ are zero and all the diagonal entries are $\det(A)$. So $(\det(A))^{-1}C^T A = I$, and $(\det(A))^{-1}C^T$ is a left inverse for A. The proof that it is a right inverse is similar, and it is given by Treil. It follows that a matrix whose determinant has a multiplicative inverse modulo m is invertible modulo m.

Let N be the cofactor inverse $(\det(A))^{-1}C^T$. We will show that every left inverse and every right inverse of A is equal to N. Suppose B is a left inverse of A. Then, working modulo m,

$$BAN = (BA)N = IN = N \quad \text{and} \quad BAN = B(AN) = BI = B$$

Thus, $B = N$. Now suppose C is a right inverse for A. Then,

$$NAC = N(AC) = NI = N \quad \text{and} \quad NAC = (NA)C = IC = C,$$

so $C = N$. This proves that the inverse of A is unique modulo m. Also, every left or right inverse must be an inverse, since it is equal to N, which is an inverse. □

Now we can tell whether a matrix has an inverse over $\mathbb{Z}_m$. In order compute the inverse, we know we can use the cofactor formula, but even though this works well for 2×2 matrices, for large matrices it is extremely inefficient. Row reduction is a much better method in general, but in a modulus like $\mathbb{Z}_{26}$ where not every number has a multiplicative inverse, row reduction can have serious pitfalls, as the following example demonstrates.

Example 2. *Suppose the message "RVPLBAYITDMU" was encrypted using the matrix* $\begin{pmatrix} 13 & 1 \\ 2 & 1 \end{pmatrix}$. *Use row reduction to invert the matrix, then decrypt the message.*

Solution. Row reduction can be tricky in modulus 26 because not all numbers have a multiplicative inverse. The noninvertible numbers do have numbers they can multiply to make zero (e.g. $2 \cdot 13 = 0$). We should not multiply a row by a number with no inverse. That would be the equivalent of multiplying by an elementary matrix which is not invertible. The result is often that we "lose" parts of the matrix we are trying to invert; we can turn an invertible matrix into a noninvertible matrix by multiplying by the wrong elementary matrices. Consider, for example, what happens when we multiply our matrix by two bad elementary matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 13 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 13 \end{pmatrix}$$

The last matrix is obviously not invertible because it has a zero column. We have just destroyed the matrix. These bad row operations have a similar effect to multiplying by zero. Therefore, before performing any row operation, make sure it is invertible.

With this caution, we will row reduce to find the inverse.

$$\left(\begin{array}{cc|cc} 13 & 1 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{array}\right)$$

It is not immediately clear how to proceed because neither 2 nor 13 has a multiplicative inverse mod 26. However, if we add the second row to the first, we get a 15, which has an inverse, 7.

$$\left(\begin{array}{cc|cc} 15 & 2 & 1 & 1 \\ 2 & 1 & 0 & 1 \end{array}\right)$$

This is an invertible operation because its matrix is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, which has inverse $\begin{pmatrix} 1 & 25 \\ 0 & 1 \end{pmatrix}$. In general, we can always invert row operations of the third kind because inverting their elementary matrices does not require a multiplicative inverse for the non-diagonal entry, only an additive inverse.

Now multiply the first row by 7. This operation is invertible because 7 has a multiplicative inverse.

$$\left(\begin{array}{cc|cc} 1 & 14 & 7 & 7 \\ 2 & 1 & 0 & 1 \end{array}\right)$$

Then, add 24 of row 1 to row 2, to zero the non-pivot entry in the first column.

$$\left(\begin{array}{cc|cc} 1 & 14 & 7 & 7 \\ 0 & 25 & 12 & 13 \end{array}\right)$$

Proceeding similarly, we complete the row reduction.

$$\left(\begin{array}{cc|cc} 1 & 0 & 19 & 7 \\ 0 & 1 & 14 & 13 \end{array}\right)$$

You can verify by multiplication that this is the inverse of the encoding matrix.

Now, to decode the message. The first 12 letters of the message are as follows

$$\begin{pmatrix} 19 & 7 \\ 14 & 13 \end{pmatrix} \begin{pmatrix} 17 & 15 & 1 & 24 & 19 & 12 \\ 21 & 11 & 0 & 8 & 3 & 20 \end{pmatrix} = \begin{pmatrix} 2 & 24 & 19 & 18 & 18 & 4 \\ 17 & 15 & 14 & 24 & 19 & 12 \end{pmatrix} \implies \text{CRYPTOSYSTEM}$$

The full title, with spaces inserted, reads:
"CRYPTOSYSTEMS LINEAR ALGEBRA AND THE HILL CIPHER." □

As we saw, row reduction does not work over $\mathbb{Z}_{26}$ as well as it did over $\mathbb{R}$. It can be a pain to invert matrices by checking every row operation is invertible. Row reduction over a modulus with multiple prime factors is also harder to program on a computer. When we had a noninvertible number in every row, we used our human intuition to see that adding the rows together a certain way would produce an invertible number. But finding a linear combination of the numbers in a column to add up to an invertible number, short of using brute force, is computationally complex, especially for larger matrices. The next section establishes a better method for computing inverses.

3 Inverting Matrices by Factorization

The idea behind inverse by factorization is to decompose the problem into several smaller, easier problems. Instead of inverting the matrix over large composite modulus, we invert it over several smaller, prime moduli (which are fields). Then we find the inverse over the original modulus in terms of the other inverses. For instance, instead of inverting a matrix mod 26, we invert it mod 2 and mod 13, then combine the results for our answer. To do this, we will need the following theorem, which is similar to the Chinese Remainder Theorem, but for matrices. (For a statement and proof of the Chinese Remainder Theorem, see Stinson 119-122. We do not need to state it here because our theorem and its proof use the same principles).

Theorem 3 (Inverse by Factorization)**.** *Let A be a square integer matrix. Let m be an integer greater than 1. Let $m_1, m_2, \ldots m_n$ be relatively prime factors of m such that $m_1 m_2 \ldots m_n = m$.*

1. *A is invertible modulo m if and only if it is invertible mod m_k for each k.*
2. *If A is invertible modulo m, then*

$$A^{-1} = \sum_{k=1}^{n} b_k (A^{-1})_k,$$

where $(A^{-1})_k$ is the inverse mod m_k of A, and b_k is $\frac{m}{m_k}$ times the integer which is a multiplicative inverse modulo m_k of $\frac{m}{m_k}$. (This product is not *reduced modulo m_k.)*

Proof. As we showed earlier, A is invertible mod m if and only if its determinant has a multiplicative inverse mod m, which is true if and only if m and $\det(A)$ are relatively prime. This holds if and only if $\det(A)$ and m_k are relatively prime, which is equivalent to A being invertible mod m_k for each k.

To prove the second part of the theorem, we will need some lemmas.

Lemma 3.1. *A matrix $X \equiv Y \pmod{m}$ if and only if $X \equiv Y \pmod{m_k}$, where m_k as above.*

Proof. Congruence of two matrices is defined as congruence of corresponding entries, so it is sufficient to prove the lemma for integers. Suppose $a \equiv b \pmod{m}$. Then there exists an integer c such that $a = b + cm$. Take $\bmod m_k$ of each side, and $a \bmod m_k = b \bmod m_k + 0$. so $a \equiv b \bmod m_k$ for all k. That finishes the proof for the first direction. For the second direction, we will prove that if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, then $a \equiv b \pmod{m_1 m_2}$, and the full result will follow by induction. Suppose $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$. There exist integers c_1, c_2 such that $a = b + c_1 m_1$ and $a = b + c_2 m_2$. Obviously, $c_1 m_1 = c_2 m_2$. Thus, both m_1 and m_2 are factors of $c_1 m_1$. Since m_1 and m_2 are relatively prime by hypothesis, $m_1 m_2$ must be a factor of $c_1 m_1$. Therefore, there exists an integer c such that $a = b + c m_1 m_2$. This means $a \equiv b \pmod{m_1 m_2}$. □

Now we can complete the proof for the second part of the theorem. Suppose A is a matrix that is invertible mod m. By the first part of the theorem, $(A^{-1})_k$ exists for each k, and $A(A^{-1})_k \equiv I \pmod{m_k}$. If we could find a matrix B such that $B \equiv (A^{-1})_k \pmod{m_k}$ for all k, then $AB \equiv A(A^{-1})_k \equiv I \pmod{m_k}$. Then by Lemma 3.1, $AB \equiv I \pmod{m}$, and so $B = A^{-1} \pmod{m}$.

For each k, let b_k be the product of $\frac{m}{m_k}$ and the multiplicative inverse mod m_k of $\frac{m}{m_k}$. We assumed that m_k and m_i are relatively prime for all $i \neq k$. Thus, $\frac{m}{m_k}$ and m_k are relatively prime, which implies that $\frac{m}{m_k}$ has an inverse modulo m_k.

Now let

$$B = \sum_{k=1}^{n} b_k (A^{-1})_k,$$

We claim that for each k, $B \equiv A(A^{-1})_k \pmod{m_k}$. For each k,

$$B \bmod m_k = \sum_{i=1}^{n} b_i (A^{-1})_i \bmod m_k$$

For each $i \neq k$, $\frac{m}{m_i}$ is divisible by m_k, so b_i is divisible by m_k. Thus, $b_i \bmod m_k = 0$. If $i = k$, then $b_i \bmod m_k = b_k \bmod m_k$. b_k was the product of a number and its multiplicative inverse mod m_k, so $b_k \bmod m_k = 1$. When we substitute these values for b_i into the sum, it has only one term left, and

$$B \bmod m_k = \sum_{i=1}^{n} b_i (A^{-1})_i \bmod m_k = (A^{-1})_k \bmod m_k$$

Therefore, $B \equiv (A^{-1})_k \pmod{m_k}$ for all k, so $B \equiv A^{-1} \pmod{m}$. □

We apply this theorem as follows. Suppose we want to invert a matrix mod m. We write the prime factorization of m, and if there are repeated factors, we group them together, so that the list of factors is relatively prime. We let the list of factors be $m_1, \ldots, m_n$. They satisfy the hypotheses of the theorem. They also provide convenient moduli in which to invert matrices. They are often much smaller than m, which makes doing modular arithmetic easier. In addition, each modulus is either prime and therefore a field, or else it has only one prime factor, which means we only have to worry about multiples of that one number during row reduction. In fact, in every column of an invertible matrix in these moduli, there will be at least one number with a multiplicative inverse. If this were not the case, then all the numbers would be multiples of the prime factor of the modulus, and the matrix would have one column filled with multiples of this number. Its determinant, then, would be divisible by this number, which would be a factor of the main modulus, and so the matrix would not be invertible. This method makes row reduction computationally much simpler.

Example 3. *Invert the matrix* $\begin{pmatrix} 2 & 20 & 5 \\ 8 & 33 & 42 \\ 51 & 15 & 34 \end{pmatrix}$ *in mod 60 using factorization.*

Solution. The prime factorization of 60 is $2 \times 2 \times 3 \times 5$, so our factors are 4, 3, and 5. In mod 4, the matrix becomes

$$\begin{pmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \\ 3 & 3 & 2 \end{pmatrix}$$

By switching the rows to avoid 0s and 2s, we can row reduce to find the inverse mod 4:

$$\left(\begin{array}{ccc|ccc} 3 & 3 & 2 & 0 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 2 & 2 & 1 & 1 & 0 & 0 \end{array}\right) \Longrightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 2 & 0 & 0 & 3 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{array}\right) \Longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 3 & 3 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{array}\right)$$

The reduction in mod 3 is even easier:

$$\left(\begin{array}{ccc|ccc} 2 & 2 & 2 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \Longrightarrow \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 2 & 0 & 0 \\ 0 & 1 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \Longrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

Finally, row reduce mod 5:

$$\left(\begin{array}{ccc|ccc} 2 & 0 & 0 & 1 & 0 & 0 \\ 3 & 3 & 2 & 0 & 1 & 0 \\ 1 & 0 & 4 & 0 & 0 & 1 \end{array}\right) \implies \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & 0 & 0 \\ 0 & 3 & 2 & 1 & 1 & 0 \\ 0 & 0 & 4 & 2 & 0 & 1 \end{array}\right) \implies \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 4 \\ 0 & 0 & 1 & 3 & 0 & 4 \end{array}\right)$$

Now we need to write the linear combination of the inverse matrices specified in the theorem. The first coefficient is $\frac{60}{4} = 15$, times its multiplicative inverse mod 4, which is 3 because $3 \cdot 15 = 45 \equiv 1 \pmod 4$. The second is $\frac{60}{3} = 20$, times its multiplicative inverse mod 3, which is 2. The third is $\frac{60}{5} = 12$, times its multiplicative inverse mod 5, which is 3. Now take the linear combination of the inverse matrices, adding the results mod 60:

$$\begin{pmatrix} 2 & 20 & 5 \\ 8 & 33 & 42 \\ 51 & 15 & 34 \end{pmatrix}^{-1} = 45 \begin{pmatrix} 0 & 3 & 3 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} + 40 \begin{pmatrix} 0 & 2 & 0 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} + 36 \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 4 \\ 3 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 48 & 35 & 15 \\ 50 & 37 & 44 \\ 33 & 0 & 34 \end{pmatrix}$$

□

4 Cracking a Hill Cipher

In general, there are four types of attacks on a cryptosystem, defined by the type of information available to the attacker.

1. Ciphertext only attack:
   The opponent possesses a string of ciphertext, y.

2. Known plaintext attack:
   The opponent possesses a string of plaintext, x, and the corresponding ciphertext, y.

3. Chosen plaintext attack:
   The opponent has obtained temporary access to the encryption machinery. Hence he can choose a plaintext string, x, and construct the corresponding ciphertext string, y.

4. Chosen ciphertext attack:
   The opponent has obtained temporary access to the decryption machinery. Hence he can choose a ciphertext string, y, and construct the corresponding plaintext string, x.

The Hill Cipher can be difficult to break with a ciphertext-only attack, but it succumbs easily to a known plaintext attack (or a chosen plaintext or chosen ciphertext attack). Of course, if the interceptor has only ciphertext, but he has enough of it, he can find common sets of n letters and use letter and n-graph frequency analysis to make reasonable guesses about what the corresponding plaintext is. He then will know some of the plaintext and will be able to make a known-plaintext attack.

Consider the following scenario for example:

Example 4. *You intercept the message "SONAFQCHMWPTVEVY," which you know was enciphered using a Hill 2-cipher. An earlier statistical analysis of a long string of intercepted ciphertext revealed that the most frequently occurring ciphertext digraphs were "KH" and "XW" in that order. You take a guess that those digraphs correspond to "TH" and "HE," respectively, since those are the most frequently occurring digraphs in most long plaintext messages on the subject you think is being discussed. Find the deciphering matrix, and read the message.*

Solution. Let C be the 2×2 encoding matrix for the Hill Cipher. To decrypt the message, we need to find C^{-1}.

Through a previous analysis of ciphertext, we determined that C sends "TH" to "KH" and "HE" to "XW." That is

$$C\begin{pmatrix}19\\7\end{pmatrix} = \begin{pmatrix}10\\7\end{pmatrix} \quad \text{and} \quad C\begin{pmatrix}7\\4\end{pmatrix} = \begin{pmatrix}23\\22\end{pmatrix}$$

Combine these equations, and we have

$$C\begin{pmatrix}19 & 7\\7 & 4\end{pmatrix} = \begin{pmatrix}10 & 23\\7 & 22\end{pmatrix}$$

Since C has to be invertible, we can left-multiply by C^{-1}:

$$\begin{pmatrix}19 & 7\\7 & 4\end{pmatrix} = C^{-1}\begin{pmatrix}10 & 23\\7 & 22\end{pmatrix}$$

The matrix on the right is invertible (its determinant is 7), so we can right-multiply by its inverse to make the equation yield C^{-1}.

$$\begin{pmatrix}19 & 7\\7 & 4\end{pmatrix}\begin{pmatrix}10 & 23\\7 & 22\end{pmatrix}^{-1} = C^{-1}$$

To compute the inverse, we will use factorization. First, invert the matrix modulo 2 and modulo 13, then take the linear combination specified by the theorem. Inverting the matrix modulo 2 is trivial:

$$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}^{-1} = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$$

Now invert it modulo 13:

$$\left(\begin{array}{cc|cc}10 & 10 & 1 & 0\\7 & 9 & 0 & 1\end{array}\right) \Longrightarrow \left(\begin{array}{cc|cc}1 & 1 & 4 & 0\\0 & 2 & 11 & 1\end{array}\right) \Longrightarrow \left(\begin{array}{cc|cc}1 & 0 & 5 & 6\\0 & 1 & 12 & 7\end{array}\right)$$

Now take the linear combination to find the inverse of the matrix modulo 26, using the technique from the previous theorem and example. The first coefficient is $\frac{26}{2}$ times its multiplicative inverse modulo 2, which is 1. The second is $\frac{26}{13}$ times its multiplicative inverse modulo 13, which is 7. Add the multiples of the matrices together, working modulo 26:

$$(13)(1)\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} + (2)(7)\begin{pmatrix}5 & 6\\12 & 7\end{pmatrix} = \begin{pmatrix}18 & 19\\25 & 20\end{pmatrix}$$

Returning to our earlier equation for C^{-1},

$$C^{-1} = \begin{pmatrix}19 & 7\\7 & 4\end{pmatrix}\begin{pmatrix}18 & 19\\25 & 20\end{pmatrix} = \begin{pmatrix}23 & 7\\18 & 5\end{pmatrix}$$

To decode the message "SONAFQCHMWPTVEVY," we find its matrix, then multiply its matrix by the decoder:

$$\text{SONAFQCHMWPTVEVY} \Longrightarrow \begin{pmatrix}18 & 13 & 5 & 2 & 12 & 15 & 21 & 21\\14 & 0 & 16 & 7 & 22 & 19 & 4 & 24\end{pmatrix}$$

$$\begin{pmatrix}23 & 7\\18 & 5\end{pmatrix}\begin{pmatrix}18 & 13 & 5 & 2 & 12 & 15 & 21 & 21\\14 & 0 & 16 & 7 & 22 & 19 & 4 & 24\end{pmatrix} = \begin{pmatrix}18 & 13 & 19 & 17 & 14 & 10 & 17 & 1\\4 & 0 & 14 & 19 & 14 & 1 & 8 & 4\end{pmatrix}$$

The last matrix is the decoded message: "SENATORTOOKBRIBE." □

5 A More Complex Hill Cipher

As we saw, a simple Hill-2 Cipher in mod 26 is not hard to break if we have enough ciphertext. However, there are ways to make Hill Ciphers much more difficult to break.

Hill Ciphers do not have to use mod 26. If the set of keys includes non-alphabetic characters like punctuation marks, we could easily work modulo 27, modulo 28, modulo 29, etc. In fact, working modulo 29 has distinct advantages. Since over half of the numbers in modulus 26 do not have multiplicative inverses, a random matrix will more likely not be invertible. In modulus 29, however, most matrices are invertible. That means we are working with a larger set of keys in our cryptosystem. The code is thus harder to break.

It is even better to use multiple Hill Ciphers. Of course, if we used two ciphers that used matrices of the same size over the same modulus, we could multiply them together to make one matrix, and our code would not be any harder to break. Using two matrices over different moduli, however, is much more difficult. If we multiplied our text by A modulo 26 and then by B modulo 29, the encryption function cannot written as a matrix. In fact, it is not a linear transformation. A few calculations with numbers (which are 1×1 matrices) will show this is the case.

$$6(5(14+13) \bmod 26) \bmod 29 = 1$$

while

$$6(5(14) \bmod 26) \bmod 29 + 6(5(13) \bmod 26) \bmod 29 = 21 + 20 = 41$$

41 and 1 are not congruent modulo 26 or modulo 29. Further examples would show that there is no modulus in which the two answers would be congruent for all inputs. Since the function is not a linear transformation, it cannot be represented by a matrix.

For a cipher with a single $n \times n$ matrix, we only need n linearly independent plaintext-ciphertext pairs to crack the code. But when two matrices are applied working in two different moduli, knowing n linearly independent pairs will not yield the decoding matrices. The two ciphers have to be cracked separately, and this is difficult because to crack either one the spy would have to know some of the text in the intermediate step, after the first matrix is applied, but before the second is applied. Presumably, he would never be given the chance to intercept this. Of course, with enough ciphertext, he could use n-graph frequency to find out what the encryption function does to each n-graph. But this is considerably more work than simply inverting a matrix as we did in the last example.

Example 5. *In order to increase the difficulty of breaking your cryptosystem, you decide to encipher your messages using a Hill 2-cipher by first applying the matrix* $\begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix}$ *working modulo 26 and then applying the matrix* $\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix}$ *working modulo 29. Thus, while your plaintexts are in the usual 26 letter alphabet, your ciphertexts will be in the alphabet with 0-25 as usual and blank=26, ?=27, and !=28. Encipher the message "SEND" and decipher "ZMOY."*

Solution. Let A be the first encoding matrix and B be the second one. To avoid the confusion of working with two different moduli at once, we will perform the encoding in two steps. First, multiply "SEND" by A mod 26, then multiply the result by B mod 29. First, in mod 26,

$$\text{SEND} \implies \begin{pmatrix} 18 & 13 \\ 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 3 & 11 \\ 4 & 15 \end{pmatrix} \begin{pmatrix} 18 & 13 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 20 & 20 \\ 2 & 19 \end{pmatrix}$$

Second, multiply this result by B *modulo 29*,

$$\begin{pmatrix} 10 & 15 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 20 & 20 \\ 2 & 19 \end{pmatrix} = \begin{pmatrix} 27 & 21 \\ 2 & 10 \end{pmatrix} \implies \text{?CVK}$$

Decryption with this ciphers is a similar two step process. We must reverse the encoding process by undoing each of the steps, and undoing them *in reverse order*. First multiply by B^{-1} modulo 29, then multiply by A^{-1} modulo 26. Inverting the matrices by the technique explained in the previous example will yield

$$A^{-1} = \begin{pmatrix} 15 & 15 \\ 22 & 3 \end{pmatrix} \text{ modulo } 26, \quad B^{-1} = \begin{pmatrix} 18 & 28 \\ 19 & 20 \end{pmatrix} \text{ modulo } 29$$

For the first step, multiply "ZMOY" by B^{-1} on the left, modulo 29. The result should contain only numbers 0 through 25.

$$\text{ZMOY} \implies \begin{pmatrix} 25 & 14 \\ 12 & 24 \end{pmatrix} \qquad \begin{pmatrix} 18 & 28 \\ 19 & 20 \end{pmatrix} \begin{pmatrix} 25 & 14 \\ 12 & 24 \end{pmatrix} = \begin{pmatrix} 3 & 25 \\ 19 & 21 \end{pmatrix}$$

For the second step, multiply the result by A^{-1} modulo 26.

$$\begin{pmatrix} 15 & 15 \\ 22 & 3 \end{pmatrix} \begin{pmatrix} 3 & 25 \\ 19 & 21 \end{pmatrix} = \begin{pmatrix} 18 & 14 \\ 19 & 15 \end{pmatrix} \implies \text{STOP}$$

□

References:

Herstein, I.N. *Abstract Algebra.* Prentice-Hall, Inc. 1996.

Stinson, Douglas R. *Cryptography: Theory and Practice.* CRC Press. 1995.

Treil, Sergei. *Linear Algebra Done Wrong.* Brown University. 2009.