5. Classical Cryptographic Techniques from modular arithmetic perspective

By **classical cryptography** we mean methods of encipherment that have been used from antiquity through the middle of the twentieth century and that are generally based on pencil-and-paper work. The goal in all of these methods is to keep secret from intermediaries the content of messages in ordinary human language.

One of the essential ideals throughout the course is **modular arithmetic**, which we introduce in the context of shift ciphers. We illustrate how some forms of typographical transformations can be performed by calculations that use modular arithmetic. Broadly speaking, there are two basic approaches to cryptology: **substitution**, where plaintext symbols are replaced by other symbols to produce hypertexts, and **transposition**, where plaintext symbol are rearranged to produce ciphertext. We will encounter these basic ideas in various forms, separately and in combination.

- *Plaintext* will be written in lover case letters and *CIPHERTEXT* will be written in capital letters (expect in the computer problems).
- The letters of the alphabet are assigned numbers as follows:

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*

q	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
16	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*

Note that we start with *a=0*, so z is letter number 25.

- Spaces and punctuation are omitted. This is even more annoying, but is almost always possible to replace the possible to replace the spaces in the plaintext after decrypting. If spaces were left in, there would be two choices. They could be left as spaces; but this yields so much information on the structure of the message that decryption becomes easier. Or they could be encrypted; but then they would dominate frequency counts (unless the message averages at least eight letters per word), again simplifying decryption.

Note: In this chapter, we'll be using some concepts from number theory, especially modular arithmetic. If you are not familiar with congruence, you should read the first three section of chapter 3 before proceeding.

Shift Ciphers

One of the earliest cryptosystems is often attributed to Julius Caesar. Suppose Alice wanted to send a plaintext such as

attack

but she didn't want Oscar to read it. He shifted each letter by six places, so a become *G*, *b* became *Z*, *c* became *I*, and *K* because *Q*.

G Z Z G I Q

Decryption was accomplished by shifting back by seven spaces (and trying to figure out how to put the spaces back in).

We now give the general situation using *a modular arithmetic.*

Label the letters as integers from 0 to 25, the key is an integer k with $0 \leq k \leq 25$. The encryption process is

$$C = (p + k) \bmod 26$$

Decryption is $P= (c - k) \bmod 26$. For example, Caesar used $k=3$.

Let's see how the four types of attack work.

1. **Known ciphertext only:** Oscar has only the ciphertext. Her best strategy is an exhaustive search, since there are only 26 possible keys. The letter *e* occurs most frequently in most English text. Suppose the letter L appears frequently in the ciphertext. Since $e=4$ and L=11, a reasonable guess is that $k = 11 – 4 = 7$. However, for shift ciphers this method takes much longer than an exhaustive search, plus it requires many more letters in the message in order for it to work (anything short, such as this, might not contain a common symbol, thus changing statistical counts).

2. **Known plaintext:** If you know just one letter of the plaintext along with the corresponding letter of ciphertext, you can deduce the key. For example, if you know t ($P= 19$) encrypts to D ($C= 3$), then the key is $k \equiv 3 – 19 \equiv -16 \equiv 10 \pmod{26}$.

3. **Chosen plaintext:** Choose the letter a as the plaintext. The ciphertext gives the key. For example, if the ciphertext is *H*, then the key is 7.

4. **Chosen ciphertext:** choose the letter A as ciphertext. The plaintext is the negative of the key. For example, if the plaintext is h, the key is $– 7 \equiv 19 \pmod{26}$.

Affine Ciphers

The shift ciphers may be generalized and slightly strengthened as follows. Choose two integers α and β, with gcd (α, 26) = 1, and consider the function (called an *affine function*)

$$y= (\alpha x + \beta) \bmod 26; \qquad \alpha = P; \qquad y = C$$

For example, let $\alpha = 9$ and $\beta = 2$, so we are working with $9 p + 2$. take a plaintext letter such as h ($x = 7$). It is encrypted to $9 \cdot 7 + 2 \equiv 65 \equiv 13 \pmod{26}$, which is the letter N. Using the same function, we obtain

Affine → CVVWPM.

How do we decrypt? If we were working with rational number rather than mod 26, we find: $c - \beta = \alpha p$, $x = \alpha^{-1} (y - \beta)$ $p= \alpha^{-1}(c - \beta)$. In our example: $y = 9 p + 2$ and solve: $p = 1/9 (c – 2)$. But 1/9 needs to be reinterpreted when we work mod 26.since gcd (9, 26) = 1, there is a multiplicative inverse for 9 (mod 26) (if this last sentence doesn't make sense to you). In fact, $9 \cdot 3 \equiv 1 \pmod{26}$, so 3 is the desired inverse and can be used in place of 1/9. we therefore have

$$x \equiv 3 (c – 2) \equiv 3c – 6 \equiv 3y + 20 \pmod{26}.$$

Let's try this. The letter V (P=21) is mapped to $3.21 + 20 \equiv 83 \equiv 5 \pmod{26}$, which is the letter *f.* Similarly, we see that the ciphertext *CVVWPM* is decrypted back to *affine.*

Suppose we try to use the function 13P + 4 as our encryption function.

We obtain

Input → *ERRER.*

If we alter the input, we obtain

Alter → *ERRER.*

Clearly this function leads to errors. It is impossible to decrypt, since several plaintexts yield the same ciphertext. In particular, we note that encryption must be one-to-one, and this fails in the present case.

What goes wrong in this example? If we select α=13; β =4 and solve y= 13x + 4, we obtain P=1⁄13 (C-4). But 1/13 does not exist mod 26 since gcd (13, 26) = 13 $\neq$ 1. more generally, it can be shown that $\alpha P + \beta$ is a one-to-one function mod 26 if and only if gcd (α, 26) = 1. In this case, decryption uses $x \equiv \alpha^* y - \alpha^* \beta \pmod{26}$, where $\alpha\alpha^* \equiv 1$ (mod26). So descryption is also accomplished by an affine function.

The key for this encryption method is the pair (α, β). There are 12 possible choices for α with gcd (α, 26) = 1 and there are 26 choices for β (since we are working mod 26, we only need to consider α and β between 0 and 25). Therefore, there are $12 \cdot 26 = 312$ choices for the key.

Let's look at the possible attacks.

1. **Ciphertext only:** An exhaustive search through all 312 keys would take longer than the corresponding search in the case of the shift cipher; however, it would be very easy to do on a computer. When all possibilities for the key are tired, a fairly short ciphertext , say around 20charecters, will probably correspond to only one meaningful plaintext, thus allowing the determination of the key. It would also be possible to use frequency counts, thought this would require much longer texts.

2. **Known plaintext:** With a little luck, knowing two letters of the plaintext and the corresponding letters of the ciphertext suffices to find the key. In any case, the number of possibilities for the key is greatly reduced and a few more letters should yield the key.

   For example, suppose the plaintext starts with *if* and the corresponding ciphertext is *PQ.* In numbers, this means that 8 (= *i*) maps to 15 (= P) and 5 maps to 16. therefore, we have the equations

   $$8\alpha + \beta \equiv 15 \text{ and } 5\alpha + \beta \equiv 16 \qquad \pmod{26}.$$

   Subtracting yields $3\alpha \equiv -1 \equiv 25 \pmod{26}$, which has the unique solution α =17. using the first equation, we find $8 \cdot 17 + \beta \equiv 15 \pmod{26}$, which yields $\beta = 9$.

   Suppose instead that the plaintext go corresponds to the ciphertext *TH.* We obtain the equations

   $$6\alpha + \beta \equiv 19 \text{ and } 14\alpha + \beta \equiv 7 \pmod{26}.$$

Subtracting yields -8 $\alpha \equiv 12 \pmod{26}$. Since gcd(-8,26) = 2, this has two solutions: α=5, 18. the corresponding values of β are both 15 (this is not a concidence; it will always happen this way). So we have two candidates for the key: (5, 15) and (18, 15). However, gcd (18, 26) $\neq$ 1 so the second is ruled out. Therefore, the key is (5, 15).

The preceding procedure works unless the gcd we get is 13 (or 26). In this case, use another letter of the message, if available.

If we know only one letter of plaintext, we still get a relation between α and β. For example, if we only know that g in plaintext corresponds to T in ciphertext, then we have $6\alpha + \beta \equiv 19 \pmod{26}$.there are 12 possibilities for α and each gives one corresponding β. There, an exhaustive search through the 12 keys should yield the correct key.

3. **Chosen plaintext:** Choose *ab* as the plaintext. The fist character of the ciphertext will be $\alpha \cdot 0 + \beta = \beta$, and the second will be $\alpha + \beta$. Therefore, we can find the key.

4.Chosen ciphertext: Choose AB as the ciphertext. This yields the decryption function of the form $x = \alpha_1 y + \beta_1$. We could solve for y and obtain the encryption key. But why bother? We have the decryption function, which is what we want.

Hill Cipher. The Hill cipher, which is a block cipher invented in 1929 by Lester Hill. It seems never to have been used much in practice. Its significance is that it was perhaps the first time that algebraic methods (linear algebra, modular arithmetic) were used in cryptography in an essential way. As we'll see in later chapters, algebraic methods now occupy a central position in the subject.
Chose an integer n, for example n=2. The key is an n x n matrix k. For example k is 2 x 2 matrix.

Encrytion Algorithm is $y = e_k(X) = kX$

X is vector (1x n) obtained from plaintext letters numerical equivalents y is chiphertext letters numerical equivalents.

If $x_1, x_2, x_3, \dots x_{n-1}, x_n$ are the numerical equivalents of our n plaintext letters (n is seven), we breave plaintext each block to a vector of (1×n).

$(y_1\ \ y_2) = (x_1\ \ x_2)\ k \bmod 26$
$(y_3\ \ y_4) = (x_3\ \ x_4)\ k \bmod 26$
………
$(y_{n-1}\ \ y_n) = (x_{n-1}\ \ x_n)\ k \bmod 26$

Decryption algorithm is

$x = d_k(y) = y$
$(x_1\ x_2) = (y_1\ y_2)k^{-1} \bmod 26$
. . . .
$(x_{n-1}\ \ x_n) = (y_{n-1}\ \ y_n)k^{-1} \bmod 26$

Example :

n=2

x = july = ((9, 20), (11, 24)) $k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

$(y_1\ \ y_2) = (9, 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ mod 26 = (159 212) mod 26 = (3, 4)

$(y_3\ y_4) = (11, 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (11, 22)$ mod 26

y = ((3, 4), (11, 22)) = DELW ; y = DELW

In order to decrypt we need:

gcd (det (k), 26) = 1

Now that we have the ciphertext, how do we decrypt? Simply break the ciphertext into blocks of length n, change each to a vector, and multiply on the right by the inverse matrix *N*. In our preceding example, we have

$$y = DELW = ((3, 4), (11, 26)) \rightarrow (3, 4)\ k^{-1} = (3, 4) \begin{pmatrix} 7/53 & -8/53 \\ -3/53 & 11/53 \end{pmatrix} \bmod 26$$

= (9/53 20/53) mod 26 = (9, 20) = JULY

The Hill cipher can be implemented using key matrices with sizes other than 2 x 2 . ın the Exercises you have the opportunity to explore what happens with 3 x 3 key matrices.

Example 2

x = blockcipher. $k = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{vmatrix}$

This becomes (we add an x to fill the last space)

1 11 14 2 10 2 8 15 7 4 17 23

Now multiply each vector by *M*, reduce the answer mod 26, and change back to letters:

(1, 11, 14) *M* = (199, 183, 181) ≡ (17, 1, 25) (mod 26) = *RBZ*

(2,10, 2) *M* = (64, 72, 82) ≡ (12, 20, 4) (mod 26) = *MUE,* etc.

In our case, the ciphertext is: *RBZMUEPYONOM.*

It is easy to see that changing one letter of plaintext will usually change *n* letters of chiphertext. For example, if block is changed to clock, the fist three letters of ciphertext change from RBZ to SDC. This makes frequency counts less effective, though they are not impossible when n is small. The frequencies of two letter combinations, called **diagrams**, and three-letter combinations, **trigrams,** have been computed. Beyond that, the number of combinations becomes too large (though tabulating the results for certain common combinations would not to be difficult). Also, the frequencies of combinations are so low that it is hard to get meaningful data without a very large amount of text.

Cryptanalysis

1. Known plaintext

- Oscar knows m plaintexts $x_i \in (Z_{26})^m$ and (finds out) the corresponding ciphertexts $y_i,$ $1 \le \mathrm{i} \le m$
- Consider the matrices X, Y $\in (Z_{26})^{mxm}$ having the rows x_i's and y_i 's

-The equation $Y = Xk$ gives the key $K = X^{-1}Y$ (assumig X is invertible; if chosen plaintext, then Oscar will make sure of that)

Example: Assume m = 2 and the plaintext Friday is encrypted as PQCFKU, i.e., e_k (5, 17) = (15, 16), e_k (8, 3) = (2, 5), e_k (0, 24) = (10, 20). From the first two:

$$\begin{array}{ccc} P & = & C \\ \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} & = & \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} k \end{array}$$

$$k = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}$$

This can be verified by the third pair.

2. A chosen plaintext attack proceeds by the same strategy, but is a little faster. Again, if you do not know n, try various possibilities until one works. So suppose n is known. Choose the first block of plaintext to be *baaa* ... = 1000…, the second to be *abaa*... = 0100…, and continue through the *n*th block begin… *aaab* = 0001. the blocks of ciphertext will be the rows of the matrix *M.*

3. For a chosen ciphertext attack, use the same strategy as for chosen plaintext, where the choise now represent ciphertext. The resulting plaintext will be the rows of the invrse matrix *N.*

Claude Shannon, in one of the fundamental papers on the theorical foundation of cryptography, gave two properties that a good cryptosystem should have in order to prevent statistical analysis: **diffusion** and **confusion**.

Diffusion means that if we change a character of the plaintext, then several characters of the ciphertext should change, and similarly, if we change a character of the ciphertext, then several characters of the plaintext should change. We say that the Hill cipher has this property. This means that frequency statistic of letters, digrams, etc. in the plaintext are diffused over several characters in the ciphertext, which means that much more ciphertext is needed to do a meaningful statical attack.

Confusion means that the key does not relate in a simple way to the ciphertext. In particular, each character of the ciphertext should depend on several parts of the key. For example, suppose we have a Hill cipher with an n x n matrix, and suppose we have a plaintext-ciphertext pair of length n^2 with which we are able to solve for the encryption matrix. If we change one character of the ciphertext, one column of the matrix can change completely. Of course, it would be more desirable to have the entire key change. When a situation like that happens, the cryptanalyst would probably need to solve for the entire key simultaneously, rather than piece by piece.

The Vigenere and substitution ciphers do not have the properties of diffusion and confusion, which is why they are so susceptible to frequency analysis.

The concepts of diffusion and confusion play a role in any well-designed block cipher. Of course, a disadvantage (which is precisely the cryptographic advantage) of diffusion is error propagation: A small error in the ciphertext becomes a major error in the decrypted message, and usually means the decryption is unreadable.

Permutation Cipher:

Encryption: $e_\pi (x_1, \ldots , x_n) = (x_{\pi (1),} \ldots , x_\pi) = (y_1, y_{2, \ldots ,} y_n)$
Decryption: $d_\pi (y_{1, \ldots,} y_n) = (y_{\pi\text{-}1(1),} \ldots , y_{\pi\text{-}1(n)}) = (x_{1,} x_{2, \ldots,} x_n)$

Example: Suppose plaintext "she sells seas hells by these ashore"
n = 6 and $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$ for decryption $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 2 & 4 \end{pmatrix}$. We can then use π for encryption as below:

shesel	lsseas	hellsb	ythese	ashore	π
EESLSH	SALSES	LSHBLE	HSYEET	HRAEOS	π^{-1}

We show next that the permutation cipher is a particular case of Hill cipher. Given π we construct the matrix $K_\pi = (kij)$ by

$$K_{ij} = \begin{Bmatrix} 1 & if\ i = \pi \\ 0 & otherwise \end{Bmatrix}$$

It is easy to see that encrypting using π in the permutation cipher is the same as encrypting using K_π in Hill cipher. Moreover, $K\pi^{-1} = K_{\pi\text{-}1}$.

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

Viegener Cipher

$Z_1 = K$ ans $z_i = x_{i\text{-}1,}$ for $i \geq 2$
Encryption: $e_z (x) = (x + z) \bmod 26$
Decryption: $d_z(y) = (y - z) \bmod 26$

Example: suppose K = 8, we have the following encryption:

rendezvous
irendezvou
ZVRQHDUJIM

One- time pad:

Notice that the autokey cipher is a modified Vigenere cipher where the key is the plaintext itself shifted by a fixed amount. Vigenere was possible to break by finding the length of the key. In autokey the key has the same length as the plaintext. Still, because it is related to the plaintext statistical techniques can be still applied.

Ideally, the key should be of the same length as the plaintext but completely unrelated. This is done in the One-time pad cipher.

One-time pad

$n \geq 1$, $P = C = K = (Z_2)^n$

$e_k = (x_1 + k_{1,} \ldots\ldots\ldots\ldots x_4 + k_4) \bmod 26$
$d_k = (x_1 - k_{1,} \ldots\ldots\ldots\ldots x_4 - k_4) \bmod 26$

-advantage: implies that **one-time pad** is perfectly secure
-disadvantages:
-the key (which has to be securely communicated) is as least as big as the plaintext
-each key can be used only once
-Vulnerable against know- plaintext
-severe key management problems; not commercially used but diplomatically and military
-much used for the Moscow- Washington hot- line
-much used for the Russian agents operating in foreing countries

Invented in 1918, it was thought to be unbreakable for many years unit Shannon proved it unbreakable only in 1949

Example:

x = i m p o s s i b l e
x = 8, 12, 15, 14, 18, 18, 8, 1, 11, 4
k = (8,13, 24, 19, 9, 1, 0, 7, 20, 3) – random looking 10 numbers. here is given one example sender and receiver must agree a key in advance.
$e_k(z)$ = (16, 25, 13, 7, 1, 19, 8, 8, 5, 7)
$e_k(x)$ = (Q Z N H B T I I F H)