Discrete Mathematics

Lecture 7

Introduction to Cryptography 1

Lecturer: Kahenya N.P

Introduction to lecture 7

Lecture 7 is a continuation of lecture on Number theory. This lecture will introduce the concept of cryptography, classical cryptography, and key terms in cryptography.

References

These lecture notes have been derived from the following sources (Koman et al., 2001; Rosen, 2011, 2012).

Intended Learning Outcomes

At the end of this lecture, you will be able to;

(i) Define cryptography.

(ii) Solve problems in shift ciphers.

Definition of Terms

Cryptography is the science that deals with the design and implementation of secrecy systems. It is a technique of securing data and communication during transmission such that only the authorized recipient of the data can comprehend it.

The prefix *crypt* means secret or hidden while the suffix *graphy* means writing. In cryptography, mathematical concepts or ideas and set of laws or rules known as algorithms are used to convert messages into a form that cannot be read or understood by unauthorized persons.

These algorithms are applicable in day-to-day activities such as digital signatures, verification processes to protect data privacy, protecting confidential conversations, chats, transactions among others.

Plaintext is a message that is to be altered into a secret form. Encryption is the process of altering a message into secret form. Ciphertext is the secret form of the message. Cipher is a method of altering a message into a secret message. The receiver needs to understand the encrypted message. Hence the message needs to be decrypted. Decryption is the process of changing a ciphertext back to a plaintext.

A cryptosystem is a 5-tuple (*p,c,k,e,d*) where p - the set of plaintext strings, c is the set of ciphertext strings, k is the set of possible keys, e is the set if encryption functions, and d is the set of decryption functions. We have public and private cryptosystems.

Cryptoanalysis is the discipline that deals with breaking such secrecy systems. It is the process of recovering plaintext from ciphertext without the knowledge of both the encryption method or the key. Cryptology is a combination of cryptography and cryptanalysis.

Features of cryptography

Key features of cryptography include;

a) Confidentiality: It is only the receiver who can only access the sent message.
b) Integrity: The message to be sent cannot be altered in transit between the sender and the receiver.
c) Non-repudiation: Sender cannot reject or deny their intentions in the transmission of the message later.
d) Authentication: The identity of both the sender and the receiver of the message is guaranteed as well as the origin and destination of the message.

Classical cryptography

Shift ciphers

The earliest known uses of cryptography was by Julius Caesar (Rosen, 2012). The Caesar cipher is a type of shift cipher. The method involved moving or shifting an alphabet a few letters or steps forward. For example, letter D is moved to letter G. This is what is called encryption. The Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer $\mathrm{p}, \mathrm{p} \leq 25$, the integer $\mathrm{f(p)} = \mathrm{c}$ in the set $\{0,1,2, \ldots ,25\}$, that is, integers modulo 26, $\mathbb{Z}_{26}$ by;

$$\mathrm{f(p)} = \mathrm{c} = (\mathrm{p} + 3) \bmod 26$$

For example, in an encrypted message the letter p is replaced with; $(\mathrm{p}+3)\mathrm{mod}\ 26$ where 3 is the shift key. The receiver of the message will use the decryption function $\mathrm{f(p)}^{-1}$ to change the ciphertext c to plaintext p. The decryption function is given as;

$$\mathrm{f(p)}^{-1} = \mathrm{p} = (\mathrm{c}-3)\mathrm{mod}\ 26$$

In general, the shift cipher with shift key k can be represented by the function

$$\mathrm{f(p)} = (\mathrm{p}+\mathrm{k})\mathrm{mod}\ 26$$

This function is the encrypting function, where p is the plaintext. To recover the plaintext, we use the inverse function $f(p)^{-1}$ i.e. $f(p)^{-1} = (p-k)mod\ 26$

This process of recovering the original message is called decryption. The inverse function is the decryption function.

Example 1: Otieno wants to send a secret message to Michael. He encrypts the plaintext using the shift cipher with key 3. Determine the secret message he will send for the message, 'MEET AFTER THE PARTY'.

Solution: We first replace the letters with numbers. Note the alphabet numeral equivalent in the table below.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

The plaintext or message that Otieno want to encrypt is 'MEET AFTER THE PARTY' is coded as;

Plaintext P	**M**	**E**	**E**	**T**	**A**	**F**	**T**	**E**	
	12	4	4	19	0	5	19	4	
$(\mathrm{p}+3)\mathrm{mod}\ 26$	15	7	7	22	3	8	22	7	
Ciphertext	P	H	H	W	D	I	W	H	
Plaintext	**R**	**T**	**H**	**E**	**P**	**A**	**R**	**T**	**Y**
	17	19	7	4	15	0	17	19	24
$(\mathrm{p}+3)\mathrm{mod}\ 26$	20	22	10	7	18	3	20	22	1
ciphertext C	U	W	K	H	S	D	U	W	B

The encrypted message sent is *PHHWDIWHUWKHSDUWB.*

Example 2: Juma wants to send a secret message to Mutiso. The secret message is to be encrypt with the shift cipher with key $k = 7$. Determine the ciphertext for the plaintext;

TWO ZEBRA GRAZING ALONG THE HIGHWAY

Solution: We can organize the work in a table.

p	T	W	O	Z	E	B	R	A	G	R	A	Z	I	N	G
	19	22	14	25	4	1	17	0	6	17	0	25	9	13	6
(p + 7)mod26	0	3	21	6	11	8	24	7	13	24	7	6	16	20	13
c	*A*	*D*	*V*	*G*	*L*	*I*	*Y*	*H*	*N*	*Y*	*H*	*G*	*Q*	*U*	*N*
p	A	L	O	N	G	T	H	E	H	I	G	H	W	A	Y
	0	11	14	13	6	19	7	4	7	8	6	7	22	0	24
(p + 7)mod26	7	18	21	20	13	0	14	11	14	15	13	14	2	7	5
c	H	S	V	U	N	A	O	L	O	P	N	O	C	H	F

The ciphertext sent is *ADVGLIYHNYHGQUNHSVUNAOLOPNOCHF*

Example 3: Akot sent a decrypted message *XFDSTYTQFENSJXX* to his friend Akur. He had encrypted the plaintext message using the encrypting function $\mathrm{f(p)} = (\mathrm{p} + 5)\mathrm{mod}\ 26$. Help Akur determine the plaintext message.

Solution: The decryption function is $\mathrm{f(p)}^{-1} = (\mathrm{p} - 5)\mathrm{mod}\ 26$

Ciphertext C	X	F	D	S	T	Y	T	Q	F
	23	5	3	18	19	24	19	16	5
(C − 5)mod 26	18	0	24	13	14	19	14	11	0
Plaintext P	S	A	Y	N	O	T	O	L	A
Ciphertext	**E**	**N**	**S**	**J**	**X**	**X**			
	4	13	18	9	23	23			
(C − 5)mod 26	25	8	13	4	18	18			
Plaintext P	Z	I	N	E	S	S			

The original message sent by Akot is SAY NO TO LAZINESS.

Example 4: Decrypt the ciphertext; PDWKV LVIXQ that was encrypted with the shift key k = 3.

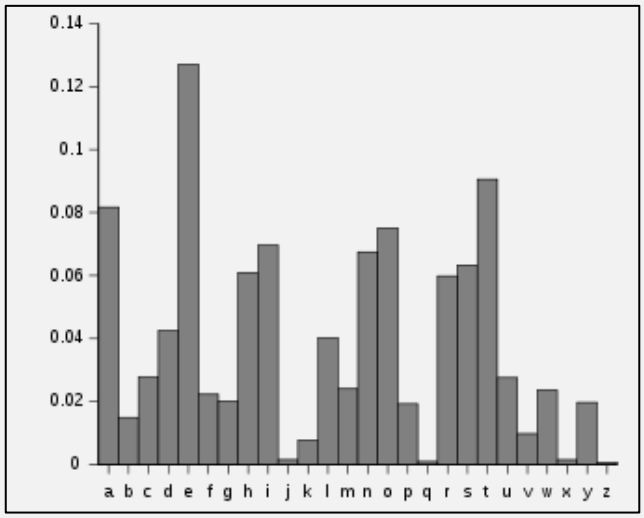
Solution: We apply the shift −k = −3mod 26.

Ciphertext C	P	D	W	K	V	L	V	I	X	Q
	15	3	22	10	21	11	21	8	23	16
(p − 3)mod 26	12	0	19	7	18	8	18	5	20	13
Plaintext P	M	A	T	H	S	I	S	F	U	N

The plaintext message is *MATHS IS FUN.*

Relative frequency of letters

The shift ciphers are weak and vulnerable to attacks. One can easily do an analysis of letters frequently appearing in a ciphertext to determine the key. In the English words the approximate relative frequency of letters put the most common letters as E (13%), T(9%), A (8%), O (8%), I (7%), S (7%) and so on (Rosen, 2012).



Source: Frequency analysis - Wikipedia:

The rarest are Z, Q, X, and J. The most common pairs of letters are TH, ER, ON and AN while SS, EE, TT, and FF are the most common repeats. These patterns pose areas of weakness that are exploited by ciphertext-only attacks.

Example 5: Decrypt the ciphertext;

YFXMPCESPZCJTDFDPQFWQZCPYNTASPCTYRXPDDLRPD

Solution: We want to use brute-force attack to determine the shift key that was used to encrypt this message.

First we determine the frequency of each letter.

Letter	Y	F	X	M	P	C	E	Z	J	T	D	Q	W	N	A	S	R	L
Frequency	3	3	2	1	7	4	1	2	1	3	5	2	1	1	1	2	2	1

In the ciphertext the most frequent letter is P. Hence we can assume P with a value of 15 is equivalent to E with a value of 4. E is the plaintext that was encrypted to P (the ciphertext). Taking our encrypting function to be $c = (p + k) \bmod 26$ where p is the plaintext and c the ciphertext, we have,

$$15 = (4+k) \bmod 26, \text{ thus } k = 11$$

Therefore, the encrypting function is; $c = (p + 11) \bmod 26$ and hence the decrypting function is;

$$p = (c - 11) \bmod 26$$

We can proceed to decrypt the message our *yfxmpcespzcjtdfdpqfwqzcpyntaspctyrxpddlrpd* to see if it makes sense. Otherwise, we proceed by assuming the most popular letter P is equivalent to the next most popular English alphabet T.

Ciphertext C	**Y**	**F**	**X**	**M**	**P**	**C**	**E**	**S**	**P**	**Z**	**C**	**J**	**T**	**D**
	24	5	23	12	15	2	4	18	15	25	2	9	19	3
$(p - 11) \bmod 26$	13	20	12	1	4	17	19	7	4	14	17	24	8	18
Plaintext P	N	U	M	B	E	R	T	H	E	O	R	Y	I	S
Ciphertext C	**F**	**D**	**P**	**Q**	F	W	Q	Z	C	P	Y	N	T	A
	5	3	15	16	5	22	16	25	2	15	24	13	19	0
$(p - 11) \bmod 26$	20	18	4	5	20	11	5	14	17	4	13	2	8	15
Plaintext P	U	S	E	F	U	L	F	0	R	E	N	C	I	P
Ciphertext C	**S**	**P**	**C**	**T**	**Y**	**R**	**X**	**P**	**D**	**D**	**L**	**R**	**P**	**D**
	18	15	2	19	24	17	23	15	3	3	11	17	15	3
$(p - 11) \bmod 26$	7	4	17	8	13	6	12	4	18	18	0	6	4	18
Plaintext P	H	E	R	I	N	G	M	E	S	S	A	G	E	S

The original message is NUMBER THEORY IS USEFUL FOR ENCIPHERING MESSAGES (Rosen, 2012).

Affine ciphers

The shift ciphers can easily be cracked by brute force attack, that is, a method that uses trial-error to determine the encrypting key. To improve on the shift ciphers, one can generalize them to a function of the form;

$$f(p) = c = (\alpha p + \beta) \bmod 26$$

with α and β are integer and are such that the function f is a bijection. A bijection is a one to one and onto mapping. The function f is a bijection if and only if α and 26 are relatively prime i.e., gcd(α, 26) = 1. This cipher is called affine cipher

Note that given that $\gcd(\alpha, 26) = 1$ then there exists 12 choices of α and 26 choices of β hence a total of $12 \times 26 = 312$ options for affine cipher.

For decrypting we use the inverse function; $f(p)^{-1} = p = \overline{\alpha}(c - \beta) \bmod 26$

where $\bar{\alpha}$ is the multiplicative inverse of $\alpha \pmod{26}$ and $0 \leq c \leq 25$.

Example 1: Encrypt the following plaintext message *THE SILENT WHISPERING* using the affine cipher $f(p) = (3p + 5) \bmod 26$.

Solution:

Plaintext	**T**	**H**	**E**	**S**	**I**	**L**	**E**	**N**	**T**	**W**
	19	7	4	18	8	11	4	13	19	22
$(3p + 5) \bmod 26$	10	0	19	7	3	12	19	18	10	19
Ciphertext C	*K*	*A*	*T*	*H*	*D*	M	*T*	*S*	*K*	*T*
Plaintext	**H**	**I**	**S**	**P**	**E**	**R**	**I**	**N**	**G**	
	7	8	18	15	4	17	8	13	6	
$(3p + 5) \bmod 26$	0	3	7	24	17	4	3	18	23	
Ciphertext	*A*	*D*	*H*	*Y*	*R*	*E*	*D*	*S*	*X*	

The ciphertext is *KATHDMTSKTADHYTEDSX*

Example 2: Decrypt the message *KVFBYQBKVCHOWMBKZNYQBTFX* that the original message was encrypted with the function $c = (5p + 7) \bmod 26$.

Solution: The decrypting function is the inverse function $p = \overline{5}(c - 7) \bmod 26$.

We first need to find the inverse of 5 mod 26 (discussed in a previous lesson for week 5).

Let the inverse of 5 be x then $5x \equiv 1 \bmod 26 \Rightarrow \gcd(5,26) = 1$ that is;

$$26 = 5(5) + 1$$

$$\therefore 1 = 26 - 5(5)$$

Introducing mod 26 we get $26 \bmod 26 - 5 \cdot 5 \bmod 26 = 1 \bmod 26$

$$\Rightarrow -5 \cdot 5 \bmod 26 = 1 \bmod 26$$

$$(26 - 5)5 \bmod 26 \equiv 1 \bmod 26$$

$$21 \cdot 5 \bmod 26 \equiv 1 \bmod 26 \therefore \overline{5} = 21$$

Therefore, the decrypting function is;

$$p = 21(c - 7) \bmod 26$$

Ciphertext c	**K**	**V**	**F**	**B**	**Y**	**Q**	**B**	**K**	**V**	**C**	**H**	**0**
	10	21	5	1	24	16	1	10	21	2	7	14
$21(c-7)\text{mod } 26$	11	8	10	4	19	7	4	11	8	25	0	17
Plaintext p	*L*	*I*	*K*	*E*	*T*	*H*	*E*	*L*	*I*	*Z*	*A*	*R*
Ciphertext c	**W**	**M**	**B**	**K**	**Z**	**N**	**Y**	**Q**	**B**	T	F	X
	22	12	1	10	25	13	24	16	1	19	5	23
$21(c-7)\text{mod } 26$	3	1	4	11	14	22	19	7	4	18	10	24
Plaintext c	*D*	*B*	*E*	*L*	*O*	*W*	*T*	*H*	*E*	S	K	Y

The plaintext message is *LIKE THE LIZARD BELOW THE SKY.*

Theorem

Let a, b, c, d, e, f, and m be integers with $\text{m} \geq 0$ such that $(\Delta, \text{m}) = 1$ where $\Delta = \text{ad} - \text{bc}$ then the systems of linear congruences $\text{ax} + \text{by} = \text{e} \pmod{\text{m}}$, $\text{cx} + \text{dy} = \text{f} \pmod{\text{m}}$ has a unique solution modulo m given by; $\text{x} = \overline{\Delta}(\text{de} - \text{bf}) \text{mod m}$ and $\text{y} = \overline{\Delta}(\text{af} - \text{ce}) \text{mod m}$ where $\overline{\Delta}$ is the inverse Δ modulo m.

Example 1: Solve the system of linear congruences

$$19 = (24\text{x} + \text{y}) \text{mod } 26$$
$$22 = (13\text{x} + \text{y}) \text{mod } 26$$

Solution: Recall from previous lecture that $\text{a} \equiv \text{b} \bmod \text{m}$ is the same as $\text{b} \equiv \text{a} \bmod \text{m}$. Hence we can have;

$$24\text{x} + \text{y} \equiv 19 \text{mod } 26 \cdots \text{(i)}$$
$$13\text{x} + \text{y} \equiv 22 \text{mod } 26 \cdots \text{(ii)}$$

Note that $\Delta = \text{ad} - \text{bc} = 24 - 13 = 11$ and $(\Delta, \text{m}) = (11,26) = 1$ implying that the system has a unique solution.

Subtracting (ii) from (i) we have; $11\text{x} \equiv -3 \bmod 26 = 23 \bmod 26$

Let another parameter t be such that;

$$11\text{t} = 1 \bmod 26 \Rightarrow 11\text{tx} = 23\text{t} \bmod 26 \therefore \text{x} = 23\text{t} \text{mod} 26 \cdots \text{(iii)}$$

From $11\text{t} = 1 \bmod 26$ we have;

$$26 = 2(11) + 4$$
$$11 = 2(4) + 3$$

$$4 = 1(3) + 1$$

Hence

$$1 = 4 - 1(3) = 4 - 1[11 - 2(4)] = 3(4) - 1(11) = 3[26 - 2(11)] - 1(11)$$

$$\therefore 1 = 3(26) - 7(11)$$

Introducing mod 26 we have;

$$-7(11) \equiv 1 \; mod \; 26$$

$$15 \cdot 11 \equiv 1 \; mod \; 26 \therefore 11^{-1} = 15 = t$$

Therefore equation (iii) becomes $x = 23 \times 15 \; mod \; 26 = 7$

Next we determine y by multiplying equation (i) and (ii) by 13 and 24 respectively (to eliminate x) and subtracting to get;

$$\begin{array}{r} 312\mathrm{x} + 13\mathrm{y} = 247 \bmod 26 \\ \underline{312\mathrm{x} + 24\mathrm{y} = 528 \bmod 26} \\ 11\mathrm{y} = 281 \bmod 26 \cdots (\mathrm{iv}) \end{array}$$

Again, we introduce a parameter t such that $11\mathrm{t} = 1 \bmod 26$.

Thus equation (iv) becomes $11ty = 281t \; mod \; 26 \Rightarrow y = 281t \; mod \; 26$

From the previous working $t = 15$ and therefore;

$$y = 281 \times 15 \; mod \; 26 = 4215 \; mod \; 26 = 3$$

Example 2: Decrypt the message below given that an affine cipher of the form $\mathrm{C} = (\mathrm{aP} + \mathrm{b}) \bmod 26$ was used with $(a, 26) = 1, 0 \leq b \leq 25$.

*RVRQQCBERFRWRYJ **WA**BGORBFW**LY**KW*

*ABYNYWPHPOOPVRY **WA**BLSW**BO**YP**PY***

Solution: Make a frequency table for the ciphertext

	R	V	Q	C	B	E	F	W	Y	J	A	G	O	L	K	N	P	H	S
	7	2	2	1	6	1	2	7	7	1	3	1	4	2	1	1	5	1	1

R, W, Y, and B have high frequency. We must determine which will assume the values E, T, A, O, I, N etc.

Recall that The most common pairs of letters are TH, ER, ON and AN.

In our ciphertext the common pair is WA with 2 counts and BO and PY with 1 count each.

We can let W= T and A=H we can also let B = E (the pair ER correspond to BO). Also, O = R (R is a popular element).

We can then investigate the following;

$22 = (19a + b) \bmod 26;\ 1 = (4a + b) mod\ 26$
$0 = (7a + b) \bmod 26 \qquad 14 = (17a + b)m$

Suppose we solve the congruences;

$22 = (19a + b) \bmod 26$ and $1 = (4a + b) \bmod 26$

We can see that $\begin{matrix} 22 = 19a + b \cdots (i) \\ 1 = 4a + b \cdots (ii) \end{matrix}$

Subtracting (ii) from (i) we get $21 \bmod 26 \equiv 15a$

We let another parameter t such that $15t = 1 \bmod 26 \therefore a = 21t \bmod 26$

$$\Rightarrow 26 = 15(1) + 11$$
$$15 = 1(11) + 4$$
$$11 = 2(4) + 3$$
$$4 = 1(3) + 1$$

Therefore $1 = 7 \cdot 15\ mod\ 26 \Rightarrow t = 7 \therefore a = 21 \cdot 7\ mod\ 26 = 17$

From equations (i) and (ii) we can eliminate a to get $15b = 9 \bmod 26$

Again, we let a parameter t is such that $15t = 1 \bmod 26$ hence $b = 9t \bmod 26$. This congruence is the same as the above working and therefore;

$$t = 7 \Rightarrow b = 9 \cdot 7 \bmod 26 = 11$$

We now have our encrypting function $c = (17p + 11) \bmod 26$.

The decryption function is then $p = \overline{17}(c - 11) mod\ 26$

It can be shown that $\overline{17} = 23$

The decrypting function is $p = 23(c - 11) mod\ 26$

We next decrypt our message; *RVRQQCBERFRWRYJ**WA**BGORBFW**LY**KW*

*ABYNYWPHPOOPVRY**WA**BLSW**BO**YP**PY***

c	R	V	R	Q	Q	C	B	E	R	F	R
	17	21	17	16	16	2	1	4	17	5	17
P	8	21	8	11	11	1	4	21	8	18	8
C	I	W	I	L	L	B	E	V	I	S	I
C	W	R	Y	J	W	A	B	G	O	R	B
	22	17	24	9	22	0	1	6	14	17	1
	19	8	13	6	19	7	4	15	17	8	4
P	T	I	N	G	T	H	E	P	R	I	E
C	F	W	L	Y	K	W	A	B	Y	N	Y
	5	22	11	24	10	22	0	1	24	13	24
	18	19	0	13	3	19	7	4	13	20	13
P	S	T	A	N	D	T	H	E	N	U	N
C	W	P	H	P	O	O	P	V	R	Y	W
	22	15	7	15	14	14	15	21	17	24	22
	19	14	12	14	17	17	14	22	8	13	19
P	T	O	M	O	R	R	O	W	I	N	T
C	A	B	L	S	W	B	O	Y	P	P	Y
	0	1	11	18	22	1	14	24	15	15	24
	7	4	0	5	19	4	17	13	14	14	13
P	H	E	A	F	T	E	R	N	O	O	N

The plaintext message is *I WILL BE VISITING THE PRIEST AND THE NUN TOMORROW IN THE AFTERNOON*

Exercises

1) Encrypt the following using the function $c = (3p + 5) \bmod 26$

   TODAY IS THE LAST DAY FOR THE SPY TO CARRY THE QUEEN ZEBRA

2) Suppose the ciphertext below was produced by encrypting the plaintext with a shift cipher. Decrypt the text.

   Ercwyjjmgmirxpcehkyergihxiglrspskcmwmrhmwxmrkymwlefpijvsqqekmg

3) Decrypt the text, assume a shift cipher was used: *dycvoozzobmrkxmodynbokw*

4) Solve the following systems of linear congruences;

   a) $7 \bmod 26 = 16x + b$
      $10 \bmod 26 = 5x + b$

   b) $18 = (13x + b) \bmod 26$
      $7 = (18x + b) \bmod 26$

   c) $17 = (2x + b) \bmod 26$
      $12 = 23x + b) \bmod 26$

   d) $5 = (13x + b) \bmod 17$
      $16 = (7x + b) \bmod 17$

5) Decrypt the message below given that an affine cipher of the form $C = (aP + b) \bmod 26$ was used with $(a, 26) = 1, 0 \leq b \leq 25$.

   XSABQNKHXPIBXFFNSIPBZARNCEOZDCWDKKNARIANKVIMXKWIMADQN

6) Attempt exercise on (Rosen, 2012, p. 304).

References

Koman, B., Busby, R., & Ross, S. (2001). *Discrete Mathematical Structures*. Prentice-Hall.

Rosen, K. (2011). *Elementary Number Theory and Its Application* (6th ed.). Person.

Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.