Writing Component Project

Learning Module Intro

to Shift, Substitution, and Vigenère Ciphers

Molly Morano
3-31-2023

Table of Contents

Class Notes

Intro to Cryptology

Activity 1.1

Opening Definition:

Cryptology – The science of securing information

What is in the field of cryptology?

Definitions within the field:

Plaintext – message that is in the vernacular of the language

Ciphertext – message has been changed based on the rules of the cipher

Decode – turning the ciphertext into the plaintext

Encode – turning the plaintext into the ciphertext

Key – private piece of information needed to decode a ciphertext

- ~~Select parties know~~

- ~~Code - set of rules~~

~~• NO KEY IS NEEDED~~Cipher - replace a piece of information with another object by a secret key known

What is a cipher?

only by select parties

Cipher vs. Code:

the information or key

that is uniform for

needed to decode

anyone that is using

and encode messages

the code

Importance of Cryptology

Cryptology is used to secure information on pencil and paper and across the internet. It keeps private information private. Without cryptology…

- Personal information over the internet would be available to the public
- Hiding sensitive information like military plans across paper correspondence would not be possible

Without cryptology… EVERYONE KNOWS EVERYTHING

A Bit of History

People have been hiding information in writing since humans began writing.

- Spartans used scytale cipher for military communication
- Caesar shift cipher used by Julius Caesar for military and political communication
- Arabs in 1412 used cryptanalysis to crack numerous ciphers including a shift, substitution and transposition cipher

As technology has evolved, computers are able to decrypt the ciphers. Because of this, modern cryptosystems often use computers because the complexity of the ciphers has to increase in order for other computers to not be able to decode secret messages. However, it is possible to encode and decode messages by hand!

Simpler ciphers that were done in the past can be encoded, decoded, and cracked by hand.

Shift Ciphers

Shift ciphers take the given alphabet of the plaintext and move the letters a set amount, which is the private key in this cipher.

First, you must number the letters within the alphabet. We will start with A being 0, ending with Z being 25.

[redacted]

0	1	2	3	4	5	6	7	8	9	10	11	12

[redacted]

13	14	15	16	17	18	19	20	21	22	23	24	25

Next the communicating parties must determine a secret key that is a whole number falling between 1 and 25. Classically, Julius Caesar encoded his military correspondence with a shift key of 3, so let's use this as an example.

Now with our key of 3, we add 3 to each of the values above.

[redacted]

3	4	5	6	7	8	9	10	11	12	13	14	15

[redacted]

16	17	18	19	20	21	22	23	24	25	26	27	28

Now we match the shifted value with the original alphabet numbers. So, A, now has a value of 3, D has a value of 3 in the original alphabet, so any A in our plaintext will be written as D in the ciphertext.

But as we face a problem near the end of the alphabet, X, Y and Z now have values that do not correspond to any letters in our original alphabet. To fix this problem, we work in modulus.

Modulus

First, we must understand that every division statement: ��/�� where q and p are both integers and p is not equal to zero, can be rewritten: �� = ���� + ��, where m and r are both integers and 0 ≤ �� < ��.

How about a few examples!

1. 14/3
   First, we know that p=14 and q=3
   14=3m+r
   Now, figure out the closest multiple of 3 that is less than or equal to 14.
   3*4=12 and 12<14
   So, 4 is going to be our m
   14=3(4)+r
   Now let’s figure out the value of r to make the equation true.
   14-(3*4)=r
   This means r in this case is 2.
   14=3(4)+2
2. 567/34
   567=34(16)+23
   p=567, q=34, m=16, r=23
3. 1024/2
   1024=2(512)+0
   p=1024, q=2, m=512, r=0

Let’s have some practice with this!

Activity 2.1

Now let’s continue to work with this equation. �� = ���� + ��

To fix the problem we have with shift ciphers, we are going to calculate, p mod q. But this equation is congruent to r! So, when working with modulus, you work with the remainder of ��/��. Therefore, every number that we work with is now going to be less than q.

�� ������ �� ≡ ��

Let's do a few more examples with modulus before we move onto some practice.

1. 45 mod 4

   We have to follow the same steps as before to find our r.

   p=45, q=4

   45=4m+r

   Now 4*11=44, which is the closest multiple of 4 that is less than or equal to 45. This means that m=11

   45=4(11)+r

   Finally calculate the value for r.

   45-44=1=r

   So, 45 ������ 4 ≡ 1

2. 234 mod 15

   p=234, q=15, m=15, r=9

   234 mod 15 ≡ 9

3. 3 mod 14

   p=3, q=14, m=0, r=3

   3 mod 14 ≡ 3

   Notice that when p<q, p=r.

Activity 2.2

Modulus has a cyclical nature, as every value is congruent to a number in the interval [0,q). Even negative numbers fall into this interval. Simply subtract the value from q and that is the equivalent value mod q.

There is much more with modulus that can be done and is used in more complex cryptography however it is not going to be needed for our learning at this time.

Shift Cipher Continued

Now that we have information on modulus let's go back to our new alphabet with a shift key of 3.

[redacted]

3	4	5	6	7	8	9	10	11	12	13	14	15

[redacted]

16	17	18	19	20	21	22	23	24	25	26	27	28

With the English alphabet we are going to work mod 26, meaning q=26 unless otherwise stated.

We need to determine new values for X, Y and Z as they do not line up with any letters from our original alphabet.

Starting with X, we need to calculate, 26 mod 26.

The r in this case is going to be 0, meaning the new value for X with a shift of 3 is 0.

Now, find Y and Z on your own.

Y: 27 mod 26≡1

Z:28 mod 26≡2

So, our final shifted alphabet looks like:

[redacted]

3	4	5	6	7	8	9	10	11	12	13	14	15

[redacted]

16	17	18	19	20	21	22	23	24	25	0	1	2

Every letter has a new value that corresponds to one from the original alphabet! Now let's try encoding something with our new alphabet.

Take the plaintext: Caesar and find the ciphertext using a shift cipher with a shift of 3. We start with the letter C.

C has a value of 5 in this new alphabet.

Going back to the original alphabet, we need to find the letter that has a value of 5. That letter is F. This means C in plaintext, is F in the ciphertext.

Now we repeat this process with the remaining letters.

This gives us the ciphertext: Fdhvdu

Great! Now anyone who knows our shift key will be able to easily get the plaintext. Let's practice decoding a message now. Using the same shift key of 3. I am going to give you a ciphertext of qeobb decode it to the plaintext.

To decode, we are going to find the number value in our shifted alphabet, starting with Q. In the shifted alphabet, Q=19. Then go back to the original alphabet to find the letter with the value of 19, which is T.

Repeating this process, we find the plaintext to be "three".

Another way to use the shift cipher, instead of values is to use a cipher wheel. Simply align a letter with A and encode and decode on the wheel. Or you can make a table for the original alphabet and cipher alphabet, a table like this is shown below.

[redacted]

	X Y Z					E			F			J	K	L					S					U	

The first line of this table is the plaintext alphabet, and the second row is the ciphertext alphabet. Each of these methods can work with a shift cipher, it is your opinion what technique you choose to use.

The shift cipher is seen as one of, if not, the most basic cipher there is. As there are only 26 options for the cipher, and one of those is simply the normal alphabet, with a shift of 0. Because of this, it is quite simple to brute force a way to crack the cipher without any explicit knowledge of the key. Simply guess what the key is and keep changing the shift until you find a shift that creates a message in English.

Activity 2.3

Substitution Cipher

A substitution cipher is when each letter of the plaintext alphabet is replaced with a different symbol. This symbol could be another letter, or it could be a random shape, however, each letter of the plaintext must be assigned a unique symbol to be able to decode the message.

We will be looking at a specific type of substitution cipher called an affine cipher. This is where each letter of the plaintext alphabet is substituted for a different letter in the plaintext alphabet. Though it sounds quite similar to the shift cipher, it is different due to

the letters of the cipher alphabet not needing to be in alphabetical order, which will always occur in a shift cipher.

In order to construct our affine cipher, we must again take a plaintext alphabet like the one formed in the shift cipher, with values of each letter from A=0 to Z=25.

[redacted]

0	1	2	3	4	5	6	7	8	9	10	11	12

[redacted]

13	14	15	16	17	18	19	20	21	22	23	24	25

Next, we need to determine two shift keys, instead of the one used in shift ciphers.

The first number we need to find let's call a. This number cannot be 0 and needs to be relatively prime to 26. This means the greatest common divisor of a and 26 must be 1. Also remember we are working modulo 26, so the number is going to be less than 26.

So, which numbers can we use?

Well, the factors of 26 are: 2,13,26

So, anything that is divisible by these numbers is not able to be a.

That leaves us with the following numbers:

3,5,7,9,11,15,17,19,21,23,25

For the first example, let's have a=5.

Our next shift key let's call b, and b must be less than 26, and be a whole number. For this example, we are going to use b=7.

Our two shift keys are a=5, and b=7.

The formula to calculate the ciphertext alphabet is below:

Let x=plaintext letter numeric value

Let y=ciphertext letter numeric value

�� ≡ (���� + ��) ������ 26

For this example, our formula will be:

�� ≡ (5�� + 7) ������ 26

Using your knowledge of modulus, calculate the numeric values of the ciphertext alphabet.

[redacted] [redacted] 7 12 17 22 1 6 11 16 21 0 5 10 15

H	M	R	W	B	G	L	Q	V	A	F	K	P

[redacted] [redacted] 20 25 4 9 14 19 24 3 8 13 18 23 2

U	Z	E	J	O	T	Y	D	I	N	S	X	C

Next, we use the new values and create a ciphertext alphabet.

So the full table for these values is:

[redacted]

			H M R W B G L						A			P		Z		J	O			Y D I		N			C

To encode and decode, we use the same rules as the shift cipher, only with the ciphertext alphabet above.

Now for some practice!

Activity 3.1

Substitution ciphers can be quite simple, though they are more difficult to break than a shift cipher. Unlike having to try 26 different combinations, we instead can run a frequency analysis on the letters present within the message.

In every language, there are some letters that are repeated more than others, there are also some letter combinations that are commonly together. The knowledge of these will help us to crack the codes of these affine ciphers.

We are going to be looking at these distributions in English.

***Goes along with an example on activity

First look at the ciphertext that you have and count how many times each letter repeats. Then find the frequency in percent that the letter repeats within the ciphertext.

$* 100$

Formula:

Next, look at the charts provided and make some educated guesses about what these letters may be.

Vigenère Cipher

The final cipher we will be studying is the Vigenère Cipher, first developed in the 16th century. This is a polyalphabetic cipher, unlike the monoalphabetic ciphers we have learned about before. This cipher uses a 26x26 alphabet, that includes all the possible shift ciphers.

The first row of the table is simply the plaintext alphabet, and the next is a shift cipher alphabet with a shift of 1, and each row then increases the shift by 1.

Thus, creating a table like the one below.

Unlike the past 2 ciphers, the secret key within this cipher is a word.

To encode, choose a key and have your plaintext. The plaintext is going to use the horizontal alphabet on the top of the table, the key will use the vertical alphabet on the left side of the table.

Find the first letter of the plaintext on the top line, and the first letter of the key on the first column. Then find where they intersect with each other on the table, this intersection is the first letter of the ciphertext.

Continue this process, repeating the key until the plaintext is completely encoded.

To decode, you take the ciphertext across the top, and the key once again along the side. Find the intersection and decode just as you encoded.

Activity 4.1

This cipher was known as the unbreakable until the late 19th century, hundreds of years after it was introduced. It can be broken if the length of the key can be determined. It can be done, especially if patterns are able to arise in longer messages. However, the work goes to in depth and will not be looked at in this lesson.

The Vigenère cipher is much more difficult to crack than shift or substitution ciphers, as it is difficult to find a series of steps to solve it without the key being known.

Resource Packet

Name:

Resource Packet

Alphabet Frequency Chart: In percent

[redacted]

8.55	1.6	3.16	3.87	12.1	2.18	2.09	4.96	7.33	.22	.81	4.21	2.53

[redacted]

7.17	7.47	2.07	.1	6.33	6.73	8.94	2.68	1.06	1.83	.19	1.72	.11

Common English Words: In percent

[redacted]

[redacted]

WAS	.88	FROM	.47	OR	.3

Alphabet Original Values:

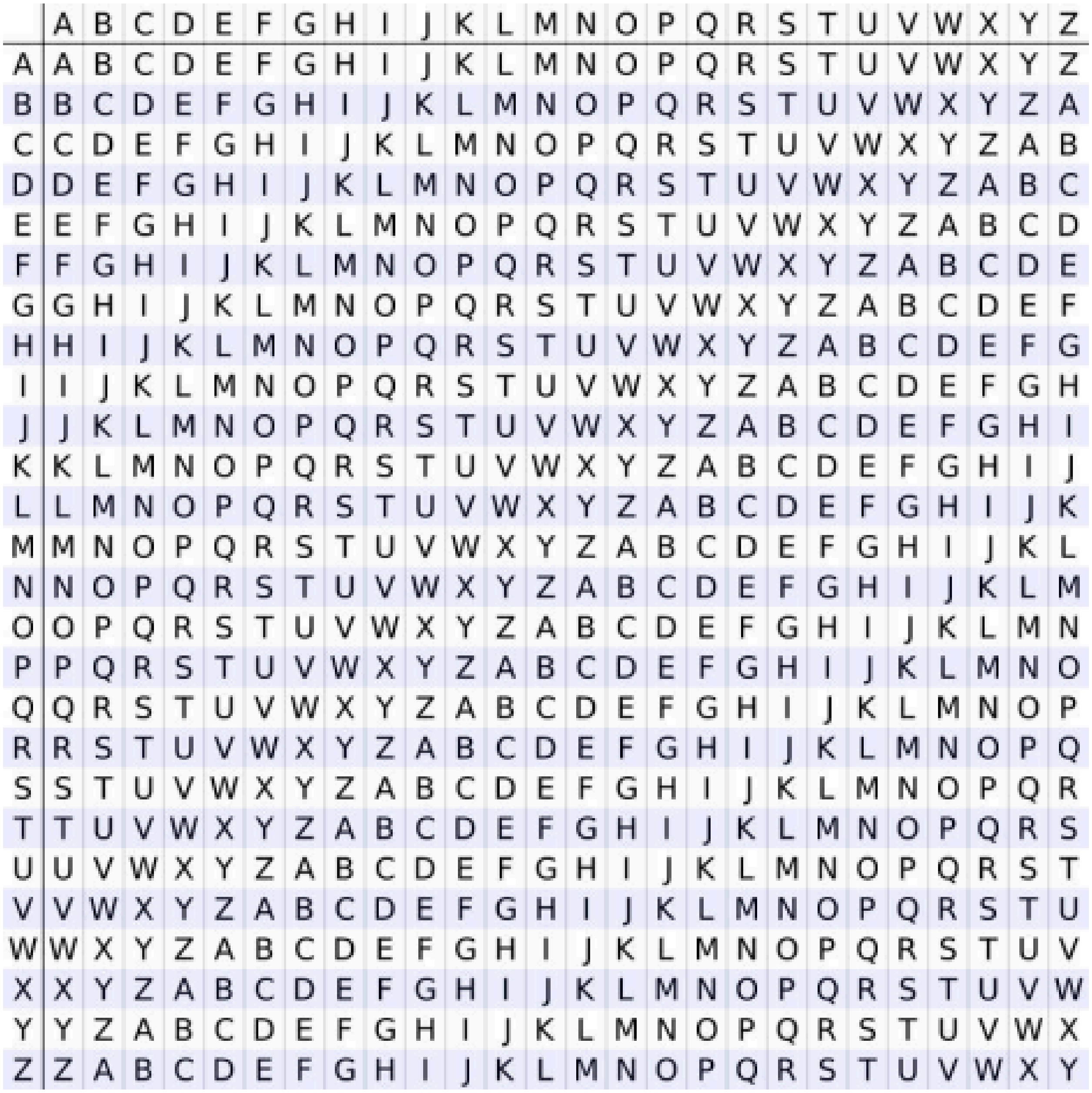
[redacted]

0	1	2	3	4	5	6	7	8	9	10	11	12

[redacted]

13	14	15	16	17	18	19	20	21	22	23	24	25

Vigenère Chart:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Activity 1.1

Name:

What do I know?

Let's determine what your knowledge of Cryptology is before we begin.
Answer these questions to the best of your ability, even if you need to guess!

I think Cryptology is…

I think Cryptology is used in…

Words I think of when I hear Cryptology:

Activity 2.1

Name:

Activity 2.1

Let's practice finding the values in a division equation. Do all the work by hand.

1. 102 ÷ 97

p=______________ q=______________

m=_____________ r =______________ 2.

176/71

p=______________ q=______________

m=______________ r =______________ 3.

95/65

p=______________ q=______________

m=______________ r =______________ 4.

161/122

p=______________ q=______________

m=______________ r =______________ 5.

59 ÷ 29

p=______________ q=______________

m=______________ r =______________

Use this space to show your work.

Activity 2.1 - Key

Name:

Activity 2.1

Let’s practice finding the values in a division equation. Do all the work by hand.

6. 102 ÷ 97 p= 102 q= 97

m= 1

r = 5

7. 176/71

p= 176

q= 71

m= 2

r = 34

8.

p= 95

q= 65

m= 1

r = 30

9. 161/122

p= 161

q= 122

m= 1

r = 39

10. 59 ÷ 29

p= 59

q= 29

m= 2

r = 1

Use this space to show your work.

Activity 2.2

Name:

Activity 2.2

Let’s get some practice working with modulus. Find the congruence of each equation. Notice, when working in modulo, we don’t use the equal sign, we add an extra line and make it a congruence statement. If you can figure out these equations without using the p = q�� + ��, you are welcome to, however, still show supporting work.

1. 21 mod 2

2. 48 mod 45

3. 41 mod 19

4. 48 mod 9

5. 50 mod 56

6. 100 mod 82

7. 45 mod 8

8. 83 mod 56

Activity 2.2 - Key

Name:

Activity 2.2

Let's get some practice working with modulus. Find the congruence of each equation. Notice, when working in modulo, we don't use the equal sign, we add an extra line and make it a congruence statement. If you can figure out these equations without using the �� = ���� + ��, you are welcome to, however, still show supporting work.

1. 21 mod 2≡1

2. 48 mod 45≡3

3. 41 mod 19≡3

4. 48 mod 9≡3

5. 50 mod 56≡50

6. 100 mod 82≡18

7. 45 mod 8≡5

8. 83 mod 56≡27

Name:

Activity 2.3

Let's do some practice with the Caesar cipher. Encoding, decoding and breaking the cipher will all be performed in this worksheet.

Section 1: Encoding

First, choose a key that you are going to use, pick a number between 4 and 24.

Key=__________________

Now make your new alphabet. Fill out the table below to make your shift cipher.

[redacted]

[redacted]			
Z			

Remember:

Ciphertext value = plaintext value + key

Next using your shift cipher, encode the following phrase:

The cow jumped over the moon

Ciphertext:

Now encode a sentence for some practice!

________ Section 2: Decoding

Now, you are going to decode a message I am sending to you. The key for this message is 14.

Ciphertext: vojsoufsohrom

**notice, there are no spaces to make the message more secure, you will need to determine the spaces that are needed while decoding.

[redacted]

[redacted]

Z			

What is the plaintext?

Section 3: Breaking the Cipher

Below is a ciphertext, decode the ciphertext without knowing the key to it. There are only 25 ciphers to try, so use trial and error to find something that makes sense in English!

Ciphertext: ymjvz njygw tbskt cozru xtajw ymjqf editl

*there is a table but you do not need to use it

[redacted]	[redacted]	[redacted]	
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
Z			

What is the plaintext?

____

Activity 2.3 - Key

Name:

Key - Activity 2.3

Let’s do some practice with the Caesar cipher. Encoding, decoding and breaking the cipher will all be performed in this worksheet.

Section 1: Encoding

First, choose a key that you are going to use, pick a number between 4 and 24.

Key=__________________

Now make your new alphabet. Fill out the table below to make your shift cipher.

Plaintext Plaintext Value Ciphertext

Value

[redacted]

[redacted]

Ciphertext

Z			

Remember:

Ciphertext value = plaintext value + key

Next using your shift cipher, encode the following phrase:

The cow jumped over the moon

Ciphertext: -

____

________ Now encode a sentence for some practice!

____

________ Section 2: Decoding

Now, you are going to decode a message I am sending to you. The key for this message is 14.

Ciphertext: vojsoufsohrom

**notice, there are no spaces to make the message more secure, you will need to determine the spaces that are needed while decoding.

Plaintext Plaintext Value Ciphertext Ciphertext
Value

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

Z	25	13	N

What is the plaintext?

Have a great day

Section 3: Breaking the Cipher

Below is a ciphertext, decode the ciphertext without knowing the key to it. There are only 25 ciphers to try, so use trial and error to find something that makes sense in English!

Ciphertext: ymjvz njygw tbskt cozru xtajw ymjqf editl

*there is a table but you do not need to use it

Plaintext Plaintext Value Ciphertext Ciphertext
Value

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

Z	25	4	E

What is the plaintext?

The quick brown fox jumps over the lazy dog

Activity 3.1

Name:

Assignment 3.1

Now some practice with the affine cipher. We will work on encoding, decoding and breaking the cipher with no knowledge of the key.

Section 1: Encoding

Time to encode with an affine cipher. Fill out the table below using the following values: a=7

b=20

[redacted]

[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
Z			

Now try encoding the plaintext: cryptology is fun

____

Section 2: Decoding

Given the ciphertext: yhsej htsee gnyfb pdfzn egnyf bpjhtse

a=15 b=5

Use the table below to help discover the plaintext

[redacted]	[redacted]		
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
[redacted]			
Z			

What is the plaintext?

____

Section 3: Breaking the Cipher

Use the charts in your packet to try and decode the following plaintext. nsydo

zuiru mdzbs zydoz uieoig

What is the plaintext?

____

Activity 3.1 - Key

Name:

Assignment 3.1

Now some practice with the affine cipher. We will work on encoding, decoding and breaking the cipher with no knowledge of the key.

Section 1: Encoding

Time to encode with an affine cipher. Fill out the table below using the following values: a=7

b=20

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

Z	25	13	N

Now try encoding the plaintext: cryptology is fun

ijgvxotokgyqdeh

Section 2: Decoding

Given the ciphertext: yhsej htsee gnyfb pdfzn egnyf bpjhtse a=15

b=5

Use the table below to help discover the plaintext

What is the plaintext?

Don’t count the days make the days count

Section 3: Breaking the Cipher

Use the charts in your packet to try and decode the following plaintext. nsydo zuiru mdzbs zydoz uieoig

What is the plaintext?

Do what is right, not what is easy

Activity 4.1

Name:

Activity 4.1

We are going to work with the Vigenère cipher for this activity. You are going to encode and decode some text. For this activity be sure to have your Vigenère table out!

Section 1: Encoding

First, encode the plaintext with the given keyword.

Plaintext: vigenere

Keyword: trade

Ciphertext: ____

Now encode a few words you want with the same keyword from above.

Section 2: Decoding

Given the ciphertext, decode using the keyword.

Ciphertext: obbw fobml jwbz

Keyword: entry

Plaintext:

____

Activity 4.1 - Key

Name:

Activity 4.1

We are going to work with the Vigenère cipher for this activity. You are going to encode and decode some text. For this activity be sure to have your Vigenère table out!

Section 1: Encoding

First, encode the plaintext with the given keyword.

Plaintext: vigenere

Keyword: trade

Ciphertext: crgbjlae

Now encode a few words you want with the same keyword from above.

Section 2: Decoding

Given the ciphertext, decode using the keyword.

Ciphertext: obbw fobml jwbz

Keyword: entry

Plaintext:

Sounds of chaos

Test

Name:

Complete every section to the best of your ability. You have learned everything that you need to in order to complete this exam.

Section 1: Definitions

Use the word box to fill in the definitions below.

decode key cryptography cryptanalysis
plaintext ciphertext encode
cipher

1. The regular language text, before any cipher changes the letters.

____

2. The study of ciphers when knowledge of how to break the code is present.

____

3. The process of taking plaintext into a ciphertext.

____

4. The thing needed in order to move between the plaintext and ciphertext.

____

5. Breaking ciphers without knowing the secret information.

____

6. The letters that are not in language that you can read.

____

7. Moving from the ciphertext to the plaintext.

____

8. ____________________________ replace a piece of information with another object by a secret key known only by select parties.

Section 2: Modulus

Complete the modulus equations. 1.

34 mod 3

2. 72 mod 5

3. 13 mod 4

4. 16 mod 11

5. 48 mod 5

6. 29 mod 5

7. 130 mod 15

8. 456 mod 24

9. 89 mod 65

10. 96 mod 9

Section 3: Encoding

Given the cipher, encode the message. You will need to use your resource packet for this.

1. Use the affine cipher with values of a=5 and b=8 to encode the plaintext.
   Plaintext: thirty five people

   [redacted]

[redacted]

Z			

The ciphertext is:

____

2. Encode the plaintext using the keyword of: crypto

Plaintext: people are walking

Ciphertext: ____

Section 3: Decode

Decode the given ciphertext.

1. Ciphertext : pjhuk ljvkl jhlzh yjpwo lyz
   Shift cipher key of 7

[redacted]

Z			

The plaintext is:

____

Bonus Questions: Cracking the Code

Decode the ciphertext without knowledge of the key.

1. An affine cipher was used and produced the ciphertext:
   mdefu orere gwfde fmdoa dmwae vvejc uwpie ricfdw jregw mcqvl ugwvv euumw

wf

Test - Key

Name:

Complete every section to the best of your ability. You have learned everything that you need to in order to complete this exam.

Section 1: Definitions

Use the word box to fill in the definitions below.

decode key cryptography cryptanalysis
plaintext ciphertext encode
cipher

1. The regular language text, before any cipher changes the letters.

   plaintext

2. The study of ciphers when knowledge of how to break the code is present.

   cryptography

3. The process of taking plaintext into a ciphertext.

   encode

4. The thing needed in order to move between the plaintext and ciphertext. key

5. Breaking ciphers without knowing the secret information.

   cryptanalysis

6. The letters that are not in language that you can read.

   ciphertext

7. Moving from the ciphertext to the plaintext.

   decode

8. Ciphers replace a piece of information with another object by a secret key known only by select parties.

Section 2: Modulus

Complete the modulus equations. 1.

34 mod 3 1

2. 72 mod 5 2

3. 13 mod 4 1

4. 16 mod 11 5

5. 48 mod 5 3

6. 29 mod 5 4

7. 130 mod 15 10

8. 456 mod 24 0

9. 89 mod 65 24

10. 96 mod 9 6

Section 3: Encoding

Given the cipher, encode the message. You will need to use your resource packet for this.

1. Use the affine cipher with values of a=5 and b=8 to encode the plaintext.

Plaintext: thirty five people

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

Z	25	3	D

The ciphertext is:

zrwpzyhwjcfcaflc

2. Encode the plaintext using the keyword of: crypto

Plaintext: people are walking

Ciphertext: rvmee scicl tzmzlv

Section 3: Decode

Decode the given ciphertext.

1. Ciphertext : pjhuk ljvkl jhlzh yjpwo lyz
   Shift cipher key of 7

[redacted]	0 7 H	1 8 I	2 9 J	3

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

Z	25	6	G

The plaintext is:

I can decode Caesar ciphers

Bonus Questions: Cracking the Code

Decode the ciphertext without knowledge of the key.

1. An affine cipher was used and produced the ciphertext:
   mdefu orere gwfde fmdoa dmwae vvejc uwpie ricfdw jregw mcqvl ugwvv euumw wf

Plaintext:

What's in a name? That which we call a rose by any other name would smell as sweet

References:

Affine Cipher. cs.uri.edu/cryptography/classical-ciphers/affine/article.html. “Caesar Cipher in Cryptography.” GeeksforGeeks, 27 Mar. 2023, www.geeksforgeeks.org/caesar-cipher-in-cryptography. Accessed 31 Mar. 2023.

Caesar Cipher (Shift) - Online Decoder, Encoder, Solver, Translator. www.dcode.fr/caesar-cipher.

“Cryptography.” University of Rhode Island, cs.uri.edu/cryptography/classical ciphers/affine/article.html. Accessed 31 Mar. 2023.

“Cryptology | Definition, Examples, History, and Facts.” Encyclopedia Britannica, 26 July 1999, www.britannica.com/topic/cryptology/History-of-cryptology. GeeksforGeeks.

“Caesar Cipher in Cryptography.” GeeksforGeeks, 27 Mar. 2023, www.geeksforgeeks.org/caesar-cipher-in-cryptography.

“History of Cryptology.” Encyclopedia Britannica, 26 July 1999, www.britannica.com/topic/cryptology/History-of-cryptology. Accessed 31 Mar. 2023.

“Online Decoder, Encoder, Solver, Translator.” DCode, www.dcode.fr/caesar cipher. Accessed 31 Mar. 2023.

Practical Cryptography. www.practicalcryptography.com/cryptanalysis/letter frequencies-various-languages/english-letter-frequencies.

“The Story of Cryptography : Historical Cryptography.” GhostVolt, ghostvolt.com/articles/cryptography_history.html. Accessed 31 Mar. 2023.