Cryptography – Introductory Exercises

Cryptography – Mathematical techniques used to code messages to obscure their meaning, such that only the intended recipient of a message can understand it.

In these exercises we will look at some substitution ciphers.

You may find it useful to review modular arithmetic from the group theory session.

1. Caesar Cipher

The simplest example of a cipher is a Caesar cipher.

We choose a value k and shift every letter in our message by k places in the alphabet.

k is called the *key*.

e.g. for $k = 4$

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
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
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

So the message HELLO becomes LIPPS.

If the recipient of our message knows the value of k they can decrypt the message by shifting each letter k places in the opposite direction.

Encryption: Shift each letter along k places.
Decryption: Shift each letter back k places.

Assign each letter in the alphabet a number:

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

Now a Caesar cipher is just adding k to the numbers corresponding to each letter in our message. Similarly, we can decipher by subtracting k.

If we shift Z=25 by 4 we get to D=3 – this is like modular arithmetic modulo 26!
We will come back to this later.

Exercises

a) Encipher the following message using a Caesar cipher with $k = 16$:
WHY IS IT CALLED A CAESAR CIPHER

b) Decipher the following message which was encrypted using a Caesar cipher with $k = 7$:
QBSPBZ JHLZHY BZLK PA

2. Vigenère Cipher

A Vigenère cipher is much like a Caesar cipher, but we shift each letter of our message by a different number of places. This makes it much harder to crack.

We do this by choosing a word as our key. Lets see how this works with an example.

Example

Suppose our key is "DOGS" and we have the message "WHO ATE MY HOMEWORK".

We write out our message and underneath we write out the key repeated:

W	H	O	A	T	E	M	Y	H	O	M	E	W	O	R	K
D	O	G	S	D	O	G	S	D	O	G	S	D	O	G	S

Recall the numbering of the alphabet:

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

D is number 3, so any letter in our message written above D we will shift by 3 places. Then we get:

W	H	O	A	T	E	M	Y	H	O	M	E	W	O	R	K
↓				↓				↓				↓			
Z				W				K				Z			

O is number 14, so any letter in our message written above O is shifted 14 places.

W	H	O	A	T	E	M	Y	H	O	M	E	W	O	R	K
↓	↓			↓	↓			↓	↓			↓	↓		
Z	V			W	S			K	C			Z	C		

G is number 6, so again we shift all letters above a G 6 places.

W	H	O	A	T	E	M	Y	H	O	M	E	W	O	R	K
↓	↓	↓		↓	↓	↓		↓	↓	↓		↓	↓	↓	
Z	V	U		W	S	S		K	C	S		Z	C	X	

Finally, S is number 18 so our final cipher is:

W	H	O	A	T	E	M	Y	H	O	M	E	W	O	R	K
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Z	V	U	S	W	S	S	Q	K	C	S	W	Z	C	X	C

If the person receiving the message knows the key word, they can decode the message the same way they decode a Caesar cipher by shifting backwards the right number of spaces for each letter.

Encryption: Shift each letter of the message along k spaces according to the number k of the corresponding letter in the key word.

Decryption: Shift each letter of the message back k spaces according to the number k of the corresponding letter in the key word.

Exercises

a) Encipher the following message using a Vigenère cipher with key word CODE

DID VIGENERE INVENT IT

b) Decipher the following message which was also encrypted using the key CODE

PC LX YOV FGZOEUC

Hint: You don't need to fit a whole number of the key word into the message. You can use the first few letters of the key word for the last letters of your message.

---

3. Affine Cipher

The final cipher we will look at is called the affine cipher. We will need our numerical version of the alphabet again.

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

Remember we are working in a system modulo 26. When we add values on to our numbers we loop back around when we get to 26.

Both of the previous ciphers have used addition and subtraction on the integers modulo 26 to substitute the letters in our message. We can also use more complicated operations.

An affine transformation is one of the form

$$y = ax + b$$

for constants a and b.

The affine cipher uses this as follows:

Encryption:

1. Choose keys a and b.
2. Convert all the letters in our message to numbers (as above)
3. Find $y = ax + b$ for each number x of the letters in our message.
4. Convert y back to a letter using the numerical alphabet.
5. Our cipher consists of all of these mappings for each letter in our message.

To decrypt, if someone knows the values of a and b they can apply the inverse operation:

$$x = a^{-1}(y - b)$$

where a^{-1} is the inverse of a modulo 26.

We go over how to find inverses in the Group Theory session.

Example

We want to encode the message HELLO and we choose $a = 5$ and $b = 12$.

H is letter 7, so we find:

$$\begin{aligned} y &= (5 \times 7) + 12 \bmod 26 \\ &= 35 + 12 \bmod 26 \\ &= 47 \bmod 26 \\ &= 21 \end{aligned}$$

The letter of the alphabet corresponding to 21 is V, so we map H to V.

E is letter 4:

$$\begin{aligned} y &= (5 \times 4) + 12 \bmod 26 \\ &= 32 \bmod 26 \\ &= 6 \end{aligned}$$

6 corresponds to G, so we map E to G.

L is letter 11:

$$\begin{aligned} y &= (5 \times 11) + 12 \bmod 26 \\ &= 67 \bmod 26 \\ &= 15 \end{aligned}$$

So L maps to P.

Finally, O is letter 14:

$$\begin{aligned} y &= (5 \times 14) + 12 \bmod 26 \\ &= 82 \bmod 26 \\ &= 4 \end{aligned}$$

So O maps to E.

Therefore, our encrypted version of HELLO is VGPPE.

Now, how do we decrypt if we receive the message VGPPE and know that $a = 5$ and $b = 12$?

First we need to find the inverse of 5 modulo 26. Recall this is a number z such that $5 \times z \equiv 1 \bmod 26$. To find z, we use the Euclidean algorithm.

5 fits into 26 five times with 1 left over:

$$26 = 5 \times 5 + 1$$

Therefore:

$$1 = 26 - 5 \times 5$$

which modulo 26 means:

$$1 \equiv -5 \times 5 \bmod 26$$

Now we need to find $-5 \bmod 26$ which is 21.

So the inverse of 5 modulo 26 is 21.

Now we can decrypt the message using $x = a^{-1}(y - b)$ with $a^{-1} = 21$ and $b = 12$.

V is letter 21, so we find:

$$\begin{aligned} x &= 21 \times (21 - 12) \bmod 26 \\ &= 21 \times 9 \bmod 26 \\ &= 189 \bmod 26 \\ &= 7 \end{aligned}$$

We know that H is letter 7, so we decode V as H.

Now we do the same for the rest of the encrypted message.

G is letter 6:

$$\begin{aligned} x &= 21 \times (6 - 12) \bmod 26 \\ &= 21 \times -6 \bmod 26 \\ &= 21 \times 20 \bmod 26 \\ &= 420 \bmod 26 \\ &= 4 \end{aligned}$$

So G maps to letter 4, E.

P is letter 15:

$$\begin{aligned} x &= 21 \times (15 - 12) \bmod 26 \\ &= 21 \times 3 \bmod 26 \\ &= 63 \bmod 26 \\ &= 11 \end{aligned}$$

So P maps to letter 11, L.

Finally, E is letter 4:

$$\begin{aligned} x &= 21 \times (4 - 12) \bmod 26 \\ &= 21 \times -8 \bmod 26 \\ &= 21 \times 18 \bmod 26 \\ &= 378 \bmod 26 \\ &= 14 \end{aligned}$$

So E maps to O.

We can decode our message as HELLO!

Decryption:

1. Find a^{-1} mod 26.
2. Convert all the letters in the encrypted message to numbers (as above).
3. Find $x = a^{-1}(y - b)$ for each number y of the letters in the encrypted message.
4. Convert x back to a letter using the numerical alphabet.
5. Our message consists of all of these mappings for each letter in our message.

Exercises

a) Encipher the following message using an affine cipher with $a = 7$ and $b = 8$.

IN A WHILE

b) Decipher the following message which was also encrypted using $a = 11$ and $b = 2$.

YHAYAJMTU

Hint: The inverse of 7 mod 26 is 15. The inverse of 11 mod 26 is 19.

Extension

The following two questions will motivate our session. You don't need any solid answers, but if you have time have a think about how you might solve them!

1. Suppose two people are sharing a message using a Caesar cipher. You don't know the key, but you want to know what it says. How might you crack it? What about if they are using a Vigenère or affine cipher?

2. You want to share a message with a friend using a Caesar cipher. How do you tell them the value of k without anyone else finding out? How about the key for a Vigenère cipher, or a and b for an affine cipher?