University of Glasgow

QUANTUM TECHNOLOGY SCHOOL 20 21

ACADEMIC PACK

PART 1: CIPHERS

Dr Sarah Croke, School of Physics & Astronomy, University of Glasgow

Ciphers

This activity introduces ways of encoding sensitive information. These ideas are used in a multitude of applications from finance to defence to safeguarding personal information. We will introduce some of the earliest known methods as well as some provably secure methods.

Next week, we will see how these ideas are used in ***quantum key distribution***, which uses the physics of quantum mechanics to enable perfectly secure communication.

Technical terms: Cipher, key, one-time pad.

Task 1.1: Caesar cipher

The first example we will discuss dates from at least Roman times and is known as the Caesar cipher. It consists of replacing each letter of the text to be sent with one shifted a certain number of places down the alphabet.

The message to be sent is known as the **plaintext**, and the message with the shift applied is the **ciphertext**.

An example is shown in the table below, corresponding to a shift of +3 places.

Plain	a	b	c	d	e	f	g	H	i	j	k	l	m	n	o	p	q	r
Cipher	d	e	f	g	h	i	j	K	l	m	n	o	p	q	r	s	t	u

Plain	s	t	u	v	w	x	y	z
Cipher	v	w	x	y	z	a	b	c

Here is an example, using the +3 shift given in the previous table:

Plain text:

T O b e o r n o t t o b e

Cipher:

W r e h r u q r w w r e h

Exercises:

1.
    a. **If you are doing this in class:** your teacher should provide each table with a topic, and a set of names or phrases related to that topic. Take one per person and encrypt these using the cipher alphabet in the table above. When you have all finished pass the ciphertexts to another table.
    b. **If you are not working on these in class:** here is an encrypted set of words, encrypted using the cipher alphabet in the table above. Can you decrypt these? ***Encrypted words:*** GRF, VQHHCB, EDVKIXO, JUXPSB, VOHHSB.

2.
    a. **If you are doing this in class:** You should in turn have received a set of ciphertexts from another table. Decrypt these using the table above. Can you be the first team to decrypt and correctly guess the topic linking the decrypted names or phrases?
    b. **If you are not working on these in class:** the words you decrypted in Q1 are all linked by a common topic: can you find the topic linking them?

3. The following message has been encrypted using a Caesar cipher (but not the one given above). Can you decipher it?

K X K , V N N C V N J C N R P Q C - J U R L N

What shift did you have to apply? The shift is known as the **key**, and anyone who knows the key can decrypt an intercepted message.

4. Do you think the Caesar cipher is secure? Explain why / why not? If not, can you think of ways to improve on it?

Additional resources:

http://practicalcryptography.com/ciphers/caesar-cipher/

http://www.simonsingh.net/The_Black_Chamber/caesar.html

Task 1.2: Variable shift cipher

A more sophisticated version of the Caesar cipher is one in which we don't apply the same shift to each letter, but rather jumble up all the letters of the alphabet in a random order. Some of you may have made up your own such ciphers as children.

An example is shown below:

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
Cipher	b	h	t	z	k	m	e	d	n	w	x	c	y	q	a	p	f	j	l

Plain	t	u	v	w	x	y	z
Cipher	o	g	r	i	s	v	u

Here is an example, using the cipher alphabet given in the table:

Plain text:

T o b e o r n o t t o b e

Cipher:

O a h k a j q a o o a h k

Exercises:

1. Play a game of hangman with the person next to you (or alternatively, if you're working on these at home, try https://thewordsearch.com/hangman/). Discuss your strategy for winning. Why is hangman winnable?

Image from www.hangman.no

2. The following passage has been encrypted using a variable shift cipher (but not the one given above). Spend a few minutes trying to decrypt it:

EK SYLLRK HL XL HL HYK BLLI. EK SYLLRK HL XL HL

HYK BLLI VI HYVR CKSFCK FIC CL HYK LHYKD HYVIXR,

ILH QKSFTRK HYKA FDK KFRA, QTH QKSFTRK HYKA

FDK YFDC…

3. Do you think this encryption method is secure? Why/ why not?

Additional resources:

http://www.simonsingh.net/The_Black_Chamber/monoalphabetic.html

Task 1.3: One-time pad

We can improve security again by using a different randomly chosen shift for each letter of the message. An example is shown below:

Plain:	B	O	B	,	M	E	E	T		M	E		A	T
Shift:	17	13	2		4	7	13	16		4	20		3	8
Cipher:	S	B	D		Q	L	R	J		Q	Y		D	B

Plain:	E	I	G	H	T	-	A	L	I	C	E
Shift:	19	21	13	3	18		2	5	22	17	3
Cipher:	X	D	T	K	L		C	Q	E	T	H

Exercises:

1. Why is this more secure than the variable shift cipher discussed previously?
2. What is the key in this case?
3. Do you think this encryption method is secure? Why/why not?

University of Glasgow

Binary digits:

In most modern devices – computers, phones, etc, information is stored as binary digits or **bits**. A bit can have the value "0" or "1", and is so commonly used because in this case the physical architecture need have only two distinguishable states. This means that everything you input is first transformed to a sequence of zeroes and ones.

Accompanying this worksheet you will find a table with one widely used encoding, known as ASCII.

Exercise:

1. Assuming your mobile phone operating system uses ASCII encoding, how is the name Bob stored in binary by your phone?

For bits we can only shift by zero (do nothing) or by one (flip the bit from 0 to 1 or from 1 to 0). A method of encryption then is to randomly choose whether or not to flip each bit. The list of choices of which bits to flip then forms the key. This is known as the **one-time pad** or **Vernam cipher**.

An example is given below – anywhere a "1" appears in the key, the plaintext bit in the same position is flipped to form the cipher.

Plain	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1
Key	1	0	0	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0
Cipher	1	0	0	0	0	1	1	0	1	1	1	1	1	0	1	0	0	1

Exercises:

1. In the example above, anyone who has the key should be able to decode the message. How would you do this?

2. Below is an example of a sequence of three ASCII characters that have been encrypted using a one-time pad. The key is given – can you find the characters?

Cipher	1	0	0	1	1	1	0	0		0	1	1	1	0	1	1	1	
Key	1	0	1	0	0	1	1	0		0	1	0	1	1	0	1	0	
Plain																		

Cipher	0	1	1	1	0	1	0	0
Key	0	1	0	1	1	1	0	1
Plain								

Characters:

Additional resources:

https://www.random.org/bytes/ (for generating random keys)

University of Glasgow

ASCII to binary table:

ASCII CHARACTER	Binary		ASCII CHARACTER	Binary
NUL	00000000		space	00100000
SOH	00000001		!	00100001
STX	00000010		"	00100010
ETX	00000011		#	00100011
EOT	00000100		$	00100100
ENQ	00000101		%	00100101
ACK	00000110		&	00100110
BEL	00000111		'	00100111
BS	00001000		(	00101000
HT	00001001		)	00101001
LF	00001010		*	00101010
VT	00001011		+	00101011
FF	00001100		,	00101100
CR	00001101		-	00101101
SO	00001110		.	00101110
SI	00001111		/	00101111
DLE	00001000		0	00110000
DC1	00010001		1	00110001
DC2	00010010		2	00110010
DC3	00010011		3	00110011
DC4	00010100		4	00110100
NAK	00010101		5	00110101
SYN	00010110		6	00110110
ETB	00010111		7	00110111
CAN	00011000		8	00111000
EM	00011001		9	00111001
SUB	00011010		:	00111010
ESC	00011011		;	00111011
FS	00011100		<	00111100
GS	00011101		=	00111101
RS	00011110		>	00111110
US	00011111		?	00111111

ASCII CHARACTER	Binary		ASCII CHARACTER	Binary
@	01000000		`	01100000
A	01000001		a	01100001
B	01000010		b	01100010
C	01000011		c	01100011
D	01000100		d	01100100
E	01000101		e	01100101
F	01000110		f	01100110
G	01000111		g	01100111
H	01001000		h	01101000
I	01001001		i	01101001
J	01001010		j	01101010
K	01001011		k	01101011
L	01001100		l	01101100
M	01001101		m	01101101
N	01001110		n	01101110
O	01001111		o	01101111
P	01010000		p	01110000
Q	01010001		q	01110001
R	01010010		r	01110010
S	01010011		s	01110011
T	01010100		t	01110100
U	01010101		u	01110101
V	01010110		v	01110110
W	01010111		w	01110111
X	01011000		x	01111000
Y	01011001		y	01111001
Z	01011010		z	01111010
[	01011011		{	01111011
\	01011100		|	01111100
]	01011101		}	01111101
^	01011110		~	01111110
_	01011111		DEL	01111111