Science and Technology Facilities Council

Codes and Ciphers

How do we keep important data secure?

Updated May 2024 (daniel.westwood@stfc.ac.uk)

Why do we need encryption?

We need to encrypt sensitive information so it cannot be read by the wrong people:

- Passwords
- Bank Details
- Personal Information (Names, Addresses etc.)
- Medical Information

All of the above are considered sensitive types of information, which means they must not be shared in a way that **any party** can understand them, only the **intended party** with the right decryption information.

Letters to Numbers

A	1	G	7	M	13	S	19	Y	25
B	2	H	8	N	14	T	20	Z	26
C	3	I	9	O	15	U	21		
D	4	J	10	P	16	V	22		
E	5	K	11	Q	17	W	23		
F	6	L	12	R	18	X	24		

Cipher text: 8 5 12 12 15 5 22 5 18 25 15 14 5

Plain text: H E L L O E V E R Y O N E

- Easy to encode messages as numbers
- But also easy for anyone to decode, even people you don't want.
- We need something more sophisticated to encode our information

Science and Technology Facilities Council

Simple Caesar (Transposition) Cipher

- Shift letters by an agreed number when encoding.
- Simple to implement, difficult to decrypt quickly for humans.

Plaintext:
Our hidden message may contain sensitive information like my computer password which is hellomynameisdavid.

Shift by 3 letters

Ciphertext:
Rxu klgghq phvvdjh pdb frqwdlq vhqvlwlyh lqirupdwlrq olnh pb frpsxwhu sdvvzrug zklfk lv khoorpbqdphlvgdylg.

- Very easily broken by computers (or humans after a few minutes)

Vigenere (Substitution) Cipher – Harder to break

Uses a Keyword (agreed between parties) to encode data. Much harder to break with brute force because there are lots of different words that could fit.

- Pick a keyword (i.e ‘hidden message’ or a random jumble of letters.
- Write down your plain text to encode, and underneath write the keyword – repeating this word until you reach the length of the plaintext.

T	H	I	S	I	S	M	Y	P	L	A	I	N	T	E	X	T
H	I	D	D	E	N	M	E	S	S	A	G	E	H	I	D	D

Science and Technology Facilities Council

Vigenere (Substitution) Cipher – Harder to break

Uses a Keyword (agreed between parties) to encode data. Much harder to break with brute force because there are lots of different words that could fit.

- Use the alphabet to find the cipher letter, using your plain and key letters as **row** and **column** in the table.
- In our example, the plaintext ‘this is my plaintext’ gets encoded as ‘aplv mf yc hdaoramaw’

KEY \ -- PLAINTEXT --	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

Science and Technology Facilities Council

Activity

Split into two teams.

Try using a transposition or substitution cipher with your own shift/keyword.

Remember: The more you write down, the more vulnerable your code is!

Everyone in each team now writes a secret message (5-10 words) in your code. Make two copies and give one copy to the ‘enemy’ team. The other copy can be decoded by the rest of your team.

Can you decipher the enemies’ messages?

BONUS: Can you decode the following:

IGJRRR HMKAOTW VN FRWZUG OGNJIY, TRQK FURUW QAISTHG FL ZIOXOARK ERQHRD

Vigenere Cipher – Keyed Alphabet

As an added level of difficulty, you can also use alphabets from different languages, or a **keyed** alphabet, which takes a different keyword and shifts those letters to the front of the alphabet:

Abcdefghijklmnopqrstuvwxyz becomes:

Stfcabdeghijklmnopqruvwxyz with keyed alphabet (STFC)

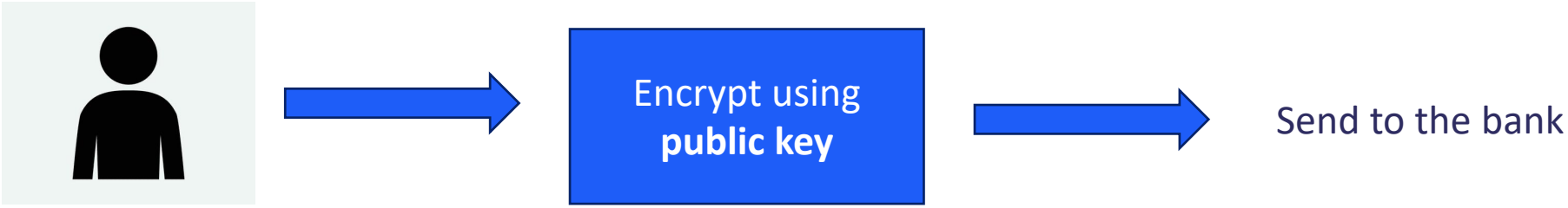
Try using this vigenere table to encode and decode messages, using your own keyword.

	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	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z
B	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s
C	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t
D	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f
E	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c
F	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a
G	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b
H	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d
I	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e
J	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g
K	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h
L	j	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i
M	k	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j
N	l	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k
O	m	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l
P	n	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m
Q	o	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n
R	p	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o
S	q	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p
T	r	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q
U	u	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r
V	v	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u
W	w	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v
X	x	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w
Y	y	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x
Z	z	s	t	f	c	a	b	d	e	g	h	i	j	k	l	m	n	o	p	q	r	u	v	w	x	y

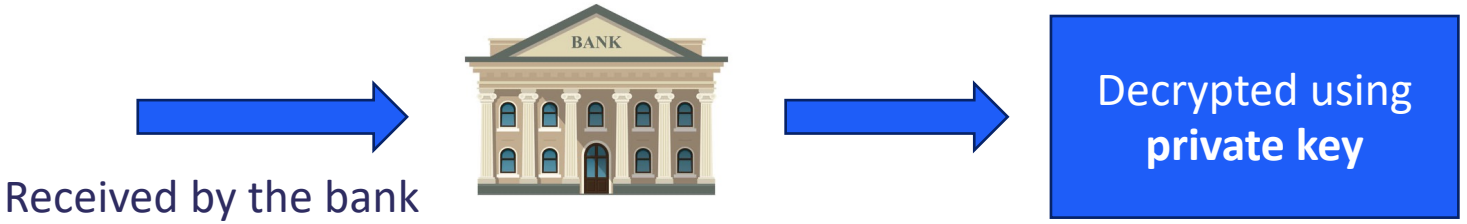
Science and Technology Facilities Council

Encryption used by Banks

Typically, banks will use something called **Public Key Cryptography** when sending and receiving information. The bank will make a **public key** available to everyone (via a website **SSL/TLS** certificate), which anyone can use to encrypt data. But the encryption is very hard to reverse if you only have the public key.



The bank holds what's called the **private key** which they keep hidden so no one else has access. When they receive some encrypted information they can decode it using their private key. The information can in fact **only** be decoded by the **private key**, so only the bank will be able to read the information.



Science and Technology Facilities Council

Quantum Encryption!

Quantum Key Distribution (QKD) relies on the weird science of **Quantum Mechanics** and can be used to solve certain problems with current encryption, as well as being much harder if not impossible to break!

- **Detect if someone else has viewed information:** On observing a quantum state, the state will change (wave function collapse) so it will be evident that someone peeked at the information.
- **Entanglement-based protocols:** Entanglement of two separate **qubits** can be used to determine if someone has intercepted some of the information, because measurement will affect the whole system.

Find out more about quantum technologies on the RAL Space/STFC websites:

https://www.ukri.org/councils/stfc/
https://www.ralspace.stfc.ac.uk/

UKRI Science and Technology Facilities Council

Science and Technology Facilities Council

Thank you

Facebook: Science and Technology Facilities Council

Twitter:@STFC_matters

YouTube: Science and Technology Facilities Council