Maths Week Scotland

The Open University SCOTLAND

Create your own Cryptography Challenge

Are you ready to be a code setter? Create your own Cryptography Challenge using these five ciphers.

You can encrypt any words you want – why not try making them clues as part of a treasure hunt? Or each one a different word of a secret message?

Use accompanying sheet to write your encrypted words and challenge someone to crack the code.

Atbash Cipher

The Atbash cipher uses a reverse alphabet to create the code.

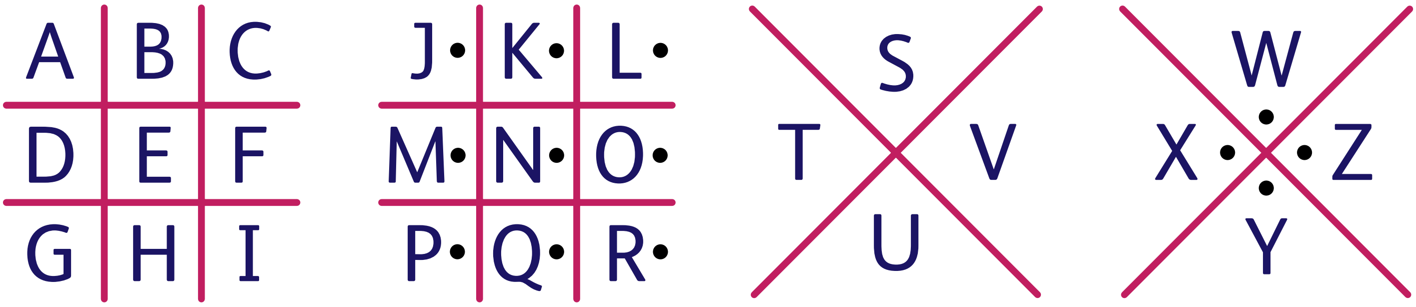
For example the word MATHS would be NZGSH.

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

This cipher gets its name from the Hebrew alphabet. The first letter of the Hebrew alphabet is “aleph”, which gets encrypted to the last letter, “taw”. The second letter of the Hebrew alphabet is “bet”, which gets encrypted to the second-last letter, “shin”. Putting these four letters together gives something which sounds like “atbash”.

Pigpen Cipher

Each letter is coded using the grid shape surrounding it. Here is the key:



A=┘ B=⊔ C=└ M=⊐ U=∧ etc.

This cipher is sometimes known as the “Freemason’s cipher” because it was often used by the Freemasons. You can see examples of this cipher on some tombstones of people who were Freemasons.

Polybius Square

Polybius square – Each letter is encoded as a pair of digits, using the square below. We always go **across first**, then **down second**. So the word “**EXAMPLE**” is coded as **23454224113123**.

E – 23

X – 45

A – 42

M – 24

P – 11

L – 31

E – 23

	1	2	3	4	5
1	P	O	L	Y	B
2	I/J	U	S	A	C
3	D	E	F	G	H
4	K	M	N	Q	R
5	T	V	W	X	Z

This cipher is named after the Ancient Greek historian, Polybius. You can see his name appearing as the “keyword” in the encryption square, but you can use any other word with no repeated letters. Can you make up your own cipher using your own secret keyword?

Digraph Cipher

Each pair of letters (a digraph) is encrypted using the table below. Don't forget to go **across first, then down!**

To encrypt the word EXAMPLE, we split the word into digraphs "**EX AM PL EX**". Note we add an extra letter "X" to the end to make sure we have pairs of letters. Using the table, we get: **EX** – GV and **AM** – VR and **PL** – UG and **EX** – GV. So "**EXAMPLE**" encrypts to "**GVVRUGGV**".

To decrypt this message, you need to do the opposite. Find the pairs of letters and then look **up first and across second**.

	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	JR	JS	JT	JU	JV	JW	JX	JY	JZ	JA	JB	JC	JD	JE	JF	JG	JH	JI	JJ	JK	JL	JM	JN	JO	JP	JQ
B	KR	KS	KT	KU	KV	KW	KX	KY	KZ	KA	KB	KC	KD	KE	KF	KG	KH	KI	KJ	KK	KL	KM	KN	KO	KP	KQ
C	LR	LS	LT	LU	LV	LW	LX	LY	LZ	LA	LB	LC	LD	LE	LF	LG	LH	LI	LJ	LK	LL	LM	LN	LO	LP	LQ
D	MR	MS	MT	MU	MV	MW	MX	MY	MZ	MA	MB	MC	MD	ME	MF	MG	MH	MI	MJ	MK	ML	MM	MN	MO	MP	MQ
E	NR	NS	NT	NU	NV	NW	NX	NY	NZ	NA	NB	NC	ND	NE	NF	NG	NH	NI	NJ	NK	NL	NM	NN	NO	NP	NQ
F	OR	OS	OT	OU	OV	OW	OX	OY	OZ	OA	OB	OC	OD	OE	OF	OG	OH	OI	OJ	OK	OL	OM	ON	OO	OP	OQ
G	PR	PS	PT	PU	PV	PW	PX	PY	PZ	PA	PB	PC	PD	PE	PF	PG	PH	PI	PJ	PK	PL	PM	PN	PO	PP	PQ
H	QR	QS	QT	QU	QV	QW	QX	QY	QZ	QA	QB	QC	QD	QE	QF	QG	QH	QI	QJ	QK	QL	QM	QN	QO	QP	QQ
I	RR	RS	RT	RU	RV	RW	RX	RY	RZ	RA	RB	RC	RD	RE	RF	RG	RH	RI	RJ	RK	RL	RM	RN	RO	RP	RQ
J	SR	SS	ST	SU	SV	SW	SX	SY	SZ	SA	SB	SC	SD	SE	SF	SG	SH	SI	SJ	SK	SL	SM	SN	SO	SP	SQ
K	TR	TS	TT	TU	TV	TW	TX	TY	TZ	TA	TB	TC	TD	TE	TF	TG	TH	TI	TJ	TK	TL	TM	TN	TO	TP	TQ
L	UR	US	UT	UU	UV	UW	UX	UY	UZ	UA	UB	UC	UD	UE	UF	UG	UH	UI	UJ	UK	UL	UM	UN	UO	UP	UQ
M	VR	VS	VT	VU	VV	VW	VX	VY	VZ	VA	VB	VC	VD	VE	VF	VG	VH	VI	VJ	VK	VL	VM	VN	VO	VP	VQ
N	WR	WS	WT	WU	WV	WW	WX	WY	WZ	WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ
O	XR	XS	XT	XU	XV	XW	XX	XY	XZ	XA	XB	XC	XD	XE	XF	XG	XH	XI	XJ	XK	XL	XM	XN	XO	XP	XQ
P	YR	YS	YT	YU	YV	YW	YX	YY	YZ	YA	YB	YC	YD	YE	YF	YG	YH	YI	YJ	YK	YL	YM	YN	YO	YP	YQ
Q	ZR	ZS	ZT	ZU	ZV	ZW	ZX	ZY	ZZ	ZA	ZB	ZC	ZD	ZE	ZF	ZG	ZH	ZI	ZJ	ZK	ZL	ZM	ZN	ZO	ZP	ZQ
R	AR	AS	AT	AU	AV	AW	AX	AY	AZ	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ
S	BR	BS	BT	BU	BV	BW	BX	BY	BZ	BA	BB	BC	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ
T	CR	CS	CT	CU	CV	CW	CX	CY	CZ	CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ	CK	CL	CM	CN	CO	CP	CQ
U	DR	DS	DT	DU	DV	DW	DX	DY	DZ	DA	DB	DC	DD	DE	DF	DG	DH	DI	DJ	DK	DL	DM	DN	DO	DP	DQ
V	ER	ES	ET	EU	EV	EW	EX	EY	EZ	EA	EB	EC	ED	EE	EF	EG	EH	EI	EJ	EK	EL	EM	EN	EO	EP	EQ
W	FR	FS	FT	FU	FV	FW	FX	FY	FZ	FA	FB	FC	FD	FE	FF	FG	FH	FI	FJ	FK	FL	FM	FN	FO	FP	FQ
X	GR	GS	GT	GU	GV	GW	GX	GY	GZ	GA	GB	GC	GD	GE	GF	GG	GH	GI	GJ	GK	GL	GM	GN	GO	GP	GQ
Y	HR	HS	HT	HU	HV	HW	HX	HY	HZ	HA	HB	HC	HD	HE	HF	HG	HH	HI	HJ	HK	HL	HM	HN	HO	HP	HQ
Z	IR	IS	IT	IU	IV	IW	IX	IY	IZ	IA	IB	IC	ID	IE	IF	IG	IH	II	IJ	IK	IL	IM	IN	IO	IP	IQ

Rail-fence Cipher

Take the sentence: **I AM A CODEBREAKER**
Then write the letters on alternate lines to make your "rail-fence":

I		M		C		D		B		E		K		R	
	A		A		O		E		R		A		E		A

Note that we have added an extra letter "A" to make sure that all the rows are filled.

We now get the encrypted message **IMCDBEKRAAOERAEA** by reading along the top line, and then the bottom line.

To break the code we just **split the ciphertext in two halves** and reverse the process.

Write the first half of the ciphertext along the top row, leaving a space after each letter. Then write the second half of the ciphertext along the bottom row, in the alternate spaces. You should be able to read the message diagonally down and up. Think carefully about how you would do this with the example before tackling the challenge below!

You can use this grid to help you build your "rail-fence":

The rail-fence cipher is a simple system for sending encrypted messages that first appeared in the US Civil War. It gets its name from the old-fashioned American fence built without the use of nails. Looked at from above, the fence looked like a zigzag. These examples only used two rows, but you can extend the rail-fence to three, four, or any number of rows. Whoever wants to decrypt the message needs to know how many rows there are, so keep that secret as your decryption key!

Now you know five different ways to encrypt a word. Create your own encrypted words on the accompanying sheet.

Codes and cryptography play a part in all our lives: in credit cards, national security and protection of online data. Problem-solving skills and knowledge of the underpinning mathematics are essential for modern cryptography and data science.

To find out more about the mathematics behind codes and cryptography, check out the Open University's wide range of mathematics and data science qualifications at undergraduate and postgraduate levels. Search for "OU mathematics" or "OU data science" to learn more!

To find more Maths Week Scotland events and activities head to **www.mathsweek.scot**.

Find more codes to crack on the **Open University Codebreak app**. Suitable for a range of ages to complete as a group or interdependently.

www.mathsweek.scot/activities.