UNIT 16 *Modern Encryption* Teacher Resource Material

Key Stage: *3 (or 4)*

Target: *Year 8 (gifted) or Year 9*

This is not difficult but it is complex! You actually use *four* operations in order to get the final code. So it is not the unit that you should tackle first! Pupils need to be familiar with the Caesar ciphers in Unit 1 before embarking on this unit. A great deal of work is entailed but you could make it easier by using a shorter message (e.g. 9 letters in a 3×3 matrix).

Solutions and Notes

Exercise 1 PHHW PH KHUH DW QLQH

Exercise 2 PHDH PHQW ULHH QHKW

Exercise 3 D.P. NVOI LUQQ TMNR

Exercise 4 KIBO KU?L XXTT _D_U

Exercise 5 QS_U XI,G XFFO IILW

Exercise 6 FDWB UDVJ OQQX RRWL

Exercise 7 FRQJ UDWX ODWL RQVB

Exercise 8 CONGRATULATIONS!

Activity 1 Step 1: add key

K	K	X	_
I	U	X	D
B	?	T	_
O	L	T	U

+

O	E	T	T
U	C	M	I
R	R	E	N
S	E	E	G

$$= \begin{bmatrix} 01011 + 01111 & 01011 + 00101 & 11000 + 10100 & 00000 + 10100 \\ 01001 + 10101 & 10101 + 00011 & 11000 + 01101 & 00100 + 01001 \\ 00010 + 10010 & 11101 + 10010 & 10100 + 00101 & 00000 + 01110 \\ 01111 + 10011 & 01100 + 00101 & 10100 + 00101 & 10101 + 00111 \end{bmatrix}$$

$$= \begin{bmatrix} 00100 & 01110 & 01100 & 10100 \\ 11100 & 10110 & 10101 & 01101 \\ 10000 & 01111 & 10001 & 01110 \\ 11100 & 01001 & 10001 & 10010 \end{bmatrix}$$

=

D	N	L	T
.	V	U	M
P	O	Q	N
.	I	Q	R

UNIT 16 *Modern Encryption* Teacher Resource Material (continued)

Activity 1

Step 2: column transformation

This is easier to calculate with the binary form.

The first column becomes

11100	+	10000	+	11100	=	10000 (P)
00100	+	10000	+	11100	=	01000 (H)
00100	+	11100	+	11100	=	00100 (D)
00100	+	11100	+	10000	=	01000 (H)

Calculating each column in a similar way gives

P	P	U	Q
H	H	L	H
D	Q	H	K
H	W	H	W

Step 3: row shift

P	P	U	Q
H	H	H	L
H	K	D	Q
W	H	W	H

Step 4: Caesar shift

M	M	R	N
E	E	E	I
E	H	A	N
T	E	T	E

i.e. MEET ME HERE AT NINE