UNIT 12 *One-Time Pads* Teacher Resource Material

Key Stage: *3 or 4*

Target: *High-achieving Year 7/8, mainstream Y9, coursework for GCSE*

Teaching Notes

Teaching Notes

We explain the secure cryptography of one-time pads, pointing out how a secure scheme can be compromised by bad practice.

Exercise 4 shows students that the cipher text can be decrypted to anything and there is no way to recover the 'true' message.

In *Activity 3*, students should find that they can get no further than the first six letters since the pad is truly random in this case. This demonstrates that one-time pads are secure against knowing part of the plaintext, if properly chosen.

Solutions and Notes

Exercise 1
a) DSNAP FOJLW KI
b) AOPLC JSANN PQSFG

Exercise 2
a) XYRIN VUVLM GO
b) UUTTA ZYMND LWYBQ

Exercise 3
a) SNAP CRACKLE POP
b) STOP LOOK LISTEN
c) WHO DARES WINS

Activity 1

	F	X	I	P	U	F	⇒	6	24	9	16	21	6
–	S	E	C	R	E	T		– 19	5	3	18	5	20
	M	S	F	X	P	L	⇐	13	19	6	24	16	12

Encrypted message: MSFXPL

Exercise 4
a) YOU NEVER HAD IT SO GOOD
b) FEW DIE AND NONE RESIGN

Activity 2
a) 1 2 3 4 5 6
b) 7 8 9 ... ; SECRET YOUR PHONE HAS BEEN TAPPED

Activity 3
a) PEYTRF
b) No; there is no structure to the key so you cannot deduce the rest of it from the first 6 letters.