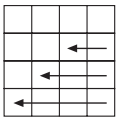
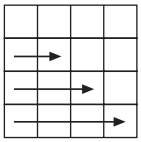
Codes and Ciphers	**UNIT 16** *Modern Encryption* Lesson Plan 1	*Encryption*
Activity		***Notes***
		T: Teacher P: Pupil Ex.B: Exercise Book
1	**Introduction** T: With the advent of powerful and cheap computers, software allows us to encrypt quickly and easily. Here is an example, called Rijndael also known as Advanced Encryption Standard (AES) This is often used for internet security. We'll go through the method together; it has four steps: • substitution (we'll use a Caesar substitution) • row shift • column transformation • add key T: It looks complex although it is really straightforward, but much quicker for a computer than for us! *5 mins*	Discussion about security and, in particular, internet security used for international companies. T should find out if Ps have any direct knowledge of systems, and build on their experiences. T writes the information on the board.
2	**Caesar substitution** T: We start with a plaintext message HI HERE IS A MESSAGE T: How many letters in this message? *(16)* T: We can put this in a 4×4 grid, writing the message down the columns. Who would like to do this? P_1 (on board): H R A S I E M A H I E G E S S E T: Look at your copy of the Caesar substitution we are going to use. What is the shift? *(By 3)* T: What else do you notice? *(Some punctuation marks are included as well as letters)* T: What does the message now become? P_2 (on board): K U D V L H P D K L H J H V V H T: Now encrypt OUR SECRET MESSAGE in the same way. *15 mins*	Ps should be familiar with this concept but might need reminding of the technique. This part of the lesson should be as interactive as possible, with Ps working at the board. **OS 16.1** should be shown or a grid drawn on the board. A copy of **OS 16.2** is given to each P. Volunteer P at board. T gives Ps a few minutes to complete this. They could use a copy of **OS 16.1**. Interactive review of answers; T must ensure that all Ps have understood.

Codes and Ciphers	**UNIT 16** *Modern Encryption* Lesson Plan 1	*Encryption*
Activity		***Notes***
3	**Row shift** T: The next step involves shifting the rows of the grid: first row – no shift second row – shift left by 1 third row – shift left by 2 fourth row – shift left by 3 We can show this by  What does our message become? P_3 (on board): K U D V H P D L H J K L H H V V T: Now it's your turn; continue with your example.	Interactive introduction with T making sure that Ps understand the concepts. T chooses a P (or volunteer) to work at the board; other Ps help if there is confusion. Ps have a few minutes for this; T monitors progress. Review, with T sorting out any misconceptions.
	20 mins	
4	**Column transformation** T: Here we make a transformation; for each column – A → B+C+D B → A+C+D C → A+B+D D → A+B+C and for this to make sense, we add letters by putting them into binary. T: Look at your copy of the binary code. Are all possible codes used? *(Yes, all 32)* T: For addition, we use the rules $0+0=1$ $0+1=1$ $1+0=1$ $1+1=0$ (This is called 'exclusive OR-ing' and is extensively used in computing) T: How can we write H + H ? *(01000 + 01000)* T: Good. Now add the corresponding binary digits. *(00000)* T: What about H + H + H ? *(00000 + 01000)* T: And what is that? *(01000)* T: In letters? *(H)* T: Now try K + H + H. P_1 (on board): $K + H + H = 01011 + (01000 + 01000)$ $= 01011 + 00000$ $= 01011$ (K)	This is more difficult – the explanation is straightforward but it is easy to make errors in the actual calculations. Each P has a copy of **OS 16.2**. It is important that Ps appreciate these rules and can use them without problems. **OS 16.4** can be used by T or each P can be given a copy. This is not easy to explain unless Ps are very flexible and able; T might need to go through several examples or use **OS 16.1** where letters are converted to their binary codes – there is no need to go back to letters at the end of this step. The 'sums' can be done in any order; e.g. $(01011 + 01000) + 01000$ $= 00011 + 01000$ $= 01011$
(continued)		

Codes and Ciphers	**UNIT 16** *Modern Encryption* Lesson Plan 1	*Encryption*
Activity		***Notes***
4 *(continued)*	T: So we have the first column. Now it's your turn to complete the other columns.	Ps have about 10 minutes tor this exercise; it will take them time to understand the process. T should monitor progress, check and review each column in turn.
	35 mins	
5	**Add key** T: Our message is now H R Y V K W Y L K M V L K O K V T: To this we add our (secret) KEY. We will use CRYPTOVARIABLEXX So our message is now H R Y V / K W Y L / K M V L / K O K V + C T R L / R O I E / Y V A X / P A B X = ? T: What is H + C ? Write it on the board, please. P_1 (on board): H + C 01000 + 00011 = 01011 ⇒ K P_2 (on board): K + R 01011 + 100010 = 11001 ⇒ Y P_3 (on board): K + Y 01011 + 11001 = 10010 ⇒ R etc. T: Complete the final message. T: Answer? P_4 (on board): K F K Z Y X P I R , W T , N I N	Either the letters or, more efficiently, their binary representations, can be used at this stage. Ps should understand that only the message sender and receiver know this key. Volunteer Ps work at the board – perhaps 2 or 3 at a time. The class check the answers and then have 4 or 5 minutes to complete the final column. T monitors progress. Final answers are checked interactively with whole class.
	45 mins	
	Homework Complete the final two stages of your example OUR SECRET MESSAGE	

Codes and Ciphers	**UNIT 16** *Modern Encryption* Lesson Plan 2	*Decryption*
Activity		***Notes***
1	**Step 1: Key** T: Here we have our received message, in groups of 4 characters. 'FRA WYHB ,TC, BLUO To decrypt the message, we simply work backwards through the 4 steps, reversing them. T: What do we do first? *(Put in the* 4×4 *grid)* P_1 (at board): ' W , B F Y T L R H C U A B , O T: Well done; what next? *(Subtract the key)* T: Yes – but this is the same as ... what? *(Adding)* T: OK. Who will start this off? P_2: What is the key? T: OURTOPSECRETKEYX ; what is the sum? P_3: ' W , B + O O C K = F Y T L U P R E R H C U R S E Y A B , O T E T X T: Each of you can do one sum and put in your answer. Ps: Q X X I S I F I _ , F L U G O W *15 mins*	T can use either the received message from the encryption example in Lesson Plan 1, or this new message. T might need to justify the methods but it is sometimes enough just to see the method working. This stage might need more explanation. As with the encryption, T can work with the binary representation, using **OS 16.4**. Assign one sum to each P; use other Ps to check the work, in pairs, etc. T should check each answer as it is presented.
2 *(continued)*	**Step 2: column transformation** T: As with the key, the column transformation is also 'self inverse' – to reverse it, we do the same thing again! T: What happens to the first column? Q → S+_+U S → _ → U → Who can complete the next three rows? Q → S+_+U S → Q+_+U _ → Q+S+U U → Q+S+_ T: Good. And the next stage? *(Work out these sums)* etc.	The first part might need more explanation; it works because the 'addition' values are also self inverse. As with encryption, T can either use the binary representations (and use **OS 16.4**) or use the letters and binary as in the plan.

Codes and Ciphers	**UNIT 16** *Modern Encryption* Lesson Plan 2	*Decryption*
Activity		***Notes***
2 *(continued)*	P_1: S + _ + U $\Rightarrow$ 10011 + 00000 + 10101 = 00110 $\Rightarrow$ F P_2: Q + _ + U $\Rightarrow$ 10001 + 00000 + 10101 = 00100 $\Rightarrow$ D, etc. T: Now complete the other column transformations. T: This is the new message: F U O R P D Q R W V Q W B J X L *30 mins*	Ps will need time to complete this. T should monitor progress; then review and correct mistakes. It is very easy to make a mistake!
3	**Step 3: row shift** T: How do we do this? *(Shift in opposite direction)* T: Well done! We can summarise this as  T: I need three volunteers to do this on the board: Ps: F U O R / P D Q R / W V Q W / B J X L → F U O R / R D D Q / Q W W V / J X L B *35 mins*	Interactive discussion on method, with Ps at board completing the shift. T should ensure that all Ps have understood.
4	**Step 4: Caesar substitution** T: What next? (Reverse the shift of 3 letters) T: OK – it's your turn now. T: Who has the message? *(CONGRATULATIONS!)* *45 mins*	Hopefully, Ps will see what to do; T makes sure that they have understood and encourages Ps to work as fast as possible to determine the message. Praise for those who are successful.
	Homework Decrypt the message K F K Z Y X P I R , W T , N I N with the original key.	