Please refer to the online lesson plan on the DT Hub to access all website links and additional resources.

## Learning hook

Show students the Cybersecurity jobs video as evidence that cryptographic jobs are in high demand.
Use the resource ‘*Caesar code activities*’ (XLS), issue the students a spreadsheet challenge.
First decide if a working spreadsheet is given to students with some parts to complete, or if students will work with the teacher in class to develop the formulas. (This second method is preferred.)
Tell students that they are going to design a spreadsheet to encode using the Caesar cypher.

**Teacher explanation of Caesar code spreadsheet**

* Activity A: Caesar shift of 3 uses the functions CHAR and CODE. This works except where an alphabet wrap around is needed.
* Activity B: Caesar shift is set in cell 14 solves this problem by introducing the MOD function. Each letter is given its ASCII value minus 65. This results in the letters of the alphabet being numbered 00 to 25.

Having students develop their own Caesar code spreadsheet introduces a number of the key features of spreadsheet formulas.

**Student activity**

*Students create their own Caesar Code encryption/decryption spreadsheet as follows:*

1. In Column A place the plaintext (message to be encoded) using uppercase, entering only one letter in each cell.
2. In Column B place the formula:
**=CHAR(CODE(A1)+n**   where n is the number of alphabetic positions to be advanced
(Analyse this formula with students)
3. **Fill down** column B using this formula. Show how the formula on each line becomes changed relative to that line.
4. Observe that the formula does not encrypt X, Y or Z. Discuss why this is so.
5. Ask for suggestions as to how this can be rectified. (Use a conditional formula to overcome this ‘over-run’ of the alphabet.)
6. **=IF((CODE(A1)+n)>90,CHAR(CODE(A1)+n-26),CHAR(CODE(A1)+n))**
(Analyse this formula with students)
7. Finally, address the inconvenience of entering the shift integer each time. How can this be overcome? (Designate a single cell in another part of the spreadsheet for this integer, eg D1, and replace n in the formula with D$1)
8. **=IF((CODE(A1)+D$1)>90,CHAR(CODE(A1)+D$1-26),CHAR(CODE(A1)+D$1))**
(Analyse this formula with students)

Demonstrate the online wartime Enigma machine at the Enigma simulation site and have students try using it.

## Learning map and outcomes

Protecting sensitive data is vital.

Encryption of data is a means of protecting data, one example being the use of secret and public keys. We examine cryptography and modern encryption methods for transmitting digital data securely.

## Learning input

1. Show students the YoungWonks page and the video three-quarters down: *Public and Private Key encryption explained.*
Three fictional characters, Alice (A), Bob (B) and Eve (‘Eavesdropper’) have traditionally been used to explain encryption methods. In the video, the narrator describes two types of keys: public keys and private keys.
	* Using these three characters and the mailbox example in the video, ask a student explain to class how public and private keys work.
2. Introduce cyphers and codes from an historical perspective.
	* In a class discussion decide what needs have existed for codes through history and collect examples.
	(Secrecy, privacy, belonging, communication, convenience, shorthand etc)
3. Optional student activity: Place the historical examples listed below on cards in a lucky dip. Ask students to select from these and present short explanations to the class after researching the origin, need, use and method for their example.

A selection of possible examples:
	* Aboriginal cave art
	* Early alphabets, Roman numerals, hieroglyphs
	* Early Christian communities (Ichthus – fish symbol)
	* Musical notation
	* Wartime: Enigma machine
	* Smoke signals, lights, flags
	* Morse code
	* Emoticons
	* URLs and DNS
	* Street slang
	* Pitman shorthand
	* Sign language
	* Braille
	* Algebra
	* Periodic table of elements
	* Iconography
	* Barcodes
	* QR codes
	* Binary
	* ASCII
	* UNICODE

## Learning construction

Explain that students will send coded messages to one another using the following two public-key simulation activities.
Explains modular arithmetic and in particular modular multiplication tables.

**Activity 1: using the M-product table to generate modular inverses**

1. Distribute the worksheet *Caesar code activities*(XLS) and conduct Activity 1.
First work through an example for students and answer any questions.
2. Have students encrypt, transmit and decrypt a secret message represented by an integer using a modular table. The steps are described on the worksheet.
3. Following practice completing a mod 5 multiplication table, students are provided with worksheets containing the following (uncompleted) M9 modular multiplication table (showing M-products).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 0 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |
| 3 | 0 | 3 | 6 | 0 | 3 | 6 | 0 | 3 | 6 |
| 4 | 0 | 4 | 8 | 3 | 7 | 2 | 6 | 1 | 5 |
| 5 | 0 | 5 | 1 | 6 | 2 | 7 | 3 | 8 | 4 |
| 6 | 0 | 6 | 3 | 0 | 6 | 3 | 0 | 6 | 3 |
| 7 | 0 | 7 | 5 | 3 | 1 | 8 | 6 | 4 | 2 |
| 8 | 0 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

* + Have students encrypt, transmit and decrypt a secret message represented by an integer between 1 and 8 using the modular 9 multiplication table provided.
	+ **Choosing the keys**:
	Their public key is determined by the modular multiplication table used, (here it is 9)
1. Pick two integers from the table whose mod product is 1.
	* **Encryption key** is the first integer.
	* **Decryption key**, or private key is the second integer.
	* Students can tell others their public and encryption keys but their decryption key is kept private!
2. **Encryption**: ask students to choose a message for transmission (here it needs to be restricted to an integer between 1 and 8). This is the encrypted secret message and is represented as an integer.
	* Using the modular multiplication table they find M-product of both the message integer and their encryption key.
	* The result is the encoded secret message.
3. **Decryption**: find M-product of decryption (private) key and the encrypted secret message.
This is the decrypted message, known only to those who have the private key.
4. Lead students in a discussion:
	* What kind of integer can we start with? (Only 1 to 8, others are off the table)
	* If someone wants to intercept the message and decrypt it how many possible keys do they need to try? (Only a few)

**Activity 2: using an arithmetic technique for generating modular inverses**

1. Distribute the worksheet *Caesar code activities*  and conduct Activity 2.
First work through an example for students and answer any questions.

Students next encrypt, transmit and decrypt a three-letter word without the use of a table using a method which generates valid modular numbers. The steps are outlined on the worksheet.
2. **Choosing the keys**
	1. Choose a number between 25 and 50.
	2. Choose a second number between 25 and 50.
	3. Find product of the two numbers in A and B.
	4. Subtract 1
	5. **Public key** is A + B + C
	6. **Encryption key** is A + D
	7. **Decryption or private key** is B + D
	8. Students tell all others their public and encryption keys.
	9. Decryption key is kept private!
3. **Encryption**: students choose a message for transmission from a sheet of three letter words.
	1. Multiply the integer corresponding to that word by the encryption key.
	2. Divide the result by the public key integer and write down the integer appearing in front of the decimal point.
	3. Multiply this by the public key.
	4. Subtract this from the result in A.

The result is the encoded secret word.

1. **Decryption**:
	1. Multiply the encoded message by the decryption key.
	2. Divide this by the public key.
	3. Write down the integer in front of the decimal point.
	4. Multiply this by the public key.
	5. Subtract this from the result in A.

The result is a number corresponding to the secret three letter word, known only to those who have the private decrypting key.

1. Lead a class discussion:
	1. Demonstrate that the M product of the encryption key and decryption key when using the public key as the modulus is 1.
	2. Explain this is the basis behind the RSA algorithm invented in 1977 (letters R, S, A are the inventors’ initials).
	RSA relies on modular arithmetic, has a public key, encryption key and decryption key.
	It uses very, very large numbers which are the product of two very, very large primes.
	3. Elicit basic understanding of encoding using modular inverses.

## Learning demo

Students discuss what they have learnt about the limitations of public/private key encryption. It may be useful to capture this in the form of an infographic, table or resume notes. There is an opportunity here to develop some peer teaching strategies where learners are asked to teach each other some core elements form the learning sequence to clarify any misconceptions and deepen understanding.

## Curriculum links

| Links with Digital Technologies Curriculum Area |
| --- |
| **Strand** | **Content Description** |
| **Knowledge and Understanding** | Investigate how hardware and software manage, control and secure access to data in networked digital systems*(AC9TDI10K01)*. |

## Assessment

Note: Criteria are cumulative.

|  | **Quantity of Knowledge** | **Quality of Understanding** |
| --- | --- | --- |
| **Encryption and decryption** | No evidence of understanding | Student is able to describe the purpose of encryption | Student is able to describe one method of encryption used historically | Student is able to describe the particular need(s) met by an encryption method | Student is able to suggest shortcomings of an encryption method |
| **Public and private-key crytography** | No evidence of understanding | Student can describe a situation in which public/private-key encryption is used | Student can describe the function of a public and a private key | Student demonstrates an appreciation of the needs met by public/private-key encryption | Student demonstrates the detailed operation of public/private-key encryption |
| **Optional score** | 0 | 1 | 2 | 3 | 4 |