WORKSHEET

F11.6 Encryption

Cyber security · GCSE · OCR J277 1.4.2, AQA 8525 3.6.3, Edexcel 1CP2 5.3.2 · about 20 min

BugBotLab

Name _____ Class _____ Date _____

What this lesson is about

Plaintext, keys and ciphertext, the Caesar cipher, symmetric and asymmetric, and a secret over the radio.

- The idea
- The Caesar cipher
- Symmetric and asymmetric
- A secret over the radio

Questions

6 marks in all

1. What is encryption? [1 mark]

- ☐ **A** Scrambling data so only someone with the key can read it
- ☐ **B** Making data smaller
- ☐ **C** Deleting data safely
- ☐ **D** Copying data to another place

2. Encrypt HELLO with a Caesar cipher, key 1. [1 mark]

3. Why is the Caesar cipher easy to break? [1 mark]

- ☐ **A** There are only 25 possible keys to try
- ☐ **B** It uses no key
- ☐ **C** It cannot be decrypted
- ☐ **D** It only works on numbers

4. In asymmetric encryption, what can be shared openly? [1 mark]

- ☐ **A** The public key
- ☐ **B** The private key
- ☐ **C** The plaintext
- ☐ **D** Both keys

5. What does the padlock and https in a browser mean? [1 mark]

- ☐ **A** The connection is encrypted
- ☐ **B** The site is free
- ☐ **C** The site is fast
- ☐ **D** The site has no adverts

6. What does this program print? [1 mark]

```
def caesar(t, k):
    return ''.join(chr((ord(c) - 65 + k) % 26 + 65) for c in t)
print(caesar('ABC', 2))
```

The task: send a secret

Write `caesar(text, key)` that shifts letters by the key and leaves anything else unchanged. Using a key of 7, encrypt `message`, print `sending: <ciphertext>`, and send the ciphertext by radio. The Ally replies with its own encrypted message; decrypt each reply and print `reply means: <plaintext>`. You should read the Ally saying `ALL CLEAR`.

```
# the two lines every program starts with: the commands, then the robot
from bugbot import *
connect()

message = "MEET AT BASE"
```

Plan your program here, then type it in and press Run.

Do it on the robot

www.bugbotlab.com/learn/f11-6-encryption/

The simulator checks it and tells you when it passes. Nothing to install, no account.

Challenges

1. Break a Caesar cipher: given only the ciphertext, print all 25 possible decryptions and pick the one that reads as English.
2. Why is a shift of 13 special? Encrypt a message twice with key 13.
3. Explain why the public key can be shared openly without helping an attacker.