ANSWERS

F11.6 Encryption

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

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

> **Answer:** A. Ciphertext is useless without the key.

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

> **Answer:** IFMMP. Each letter moves one along.

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

> **Answer:** A. A computer tries all 25 in an instant.

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

> **Answer:** A. The private key stays secret; the public key can be shared.

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

> **Answer:** A. Data sent is encrypted, so interception reveals only ciphertext.

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))
```

> **Answer:**
>
> ```
> CDE
> ```
>
> A->C, B->D, C->E.

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"
```

The hint students can ask for: Encrypt the message with the shared key, report what you are sending, and send that rather than the plain words. Decrypt each reply by shifting the other way.

A solution

```
from bugbot import *
connect()
message = "MEET AT BASE"

def caesar(text, key):
    out = ""
    for ch in text:
        if ch.isalpha():
            base = ord("A")
            out = out + chr((ord(ch.upper()) - base + key) % 26 + base)
        else:
            out = out + ch
    return out

secret = caesar(message, 7)
print("sending:", secret)
send(secret)
for tick in range(10):
    wait(0.1)
    for sender, text in messages():
        print("reply means:", caesar(text, -7))
```

Any program that meets the task's checks is marked correct in the simulator; this is one way, not the only way.