Encryption

1. What is the main purpose of encryption? (1)

a) To compress data

b) To make data smaller

c) To scramble data to hide its meaning

d) To improve data transfer speed

2. Define the term "encryption" and give one real-world example of where it is used. (2)

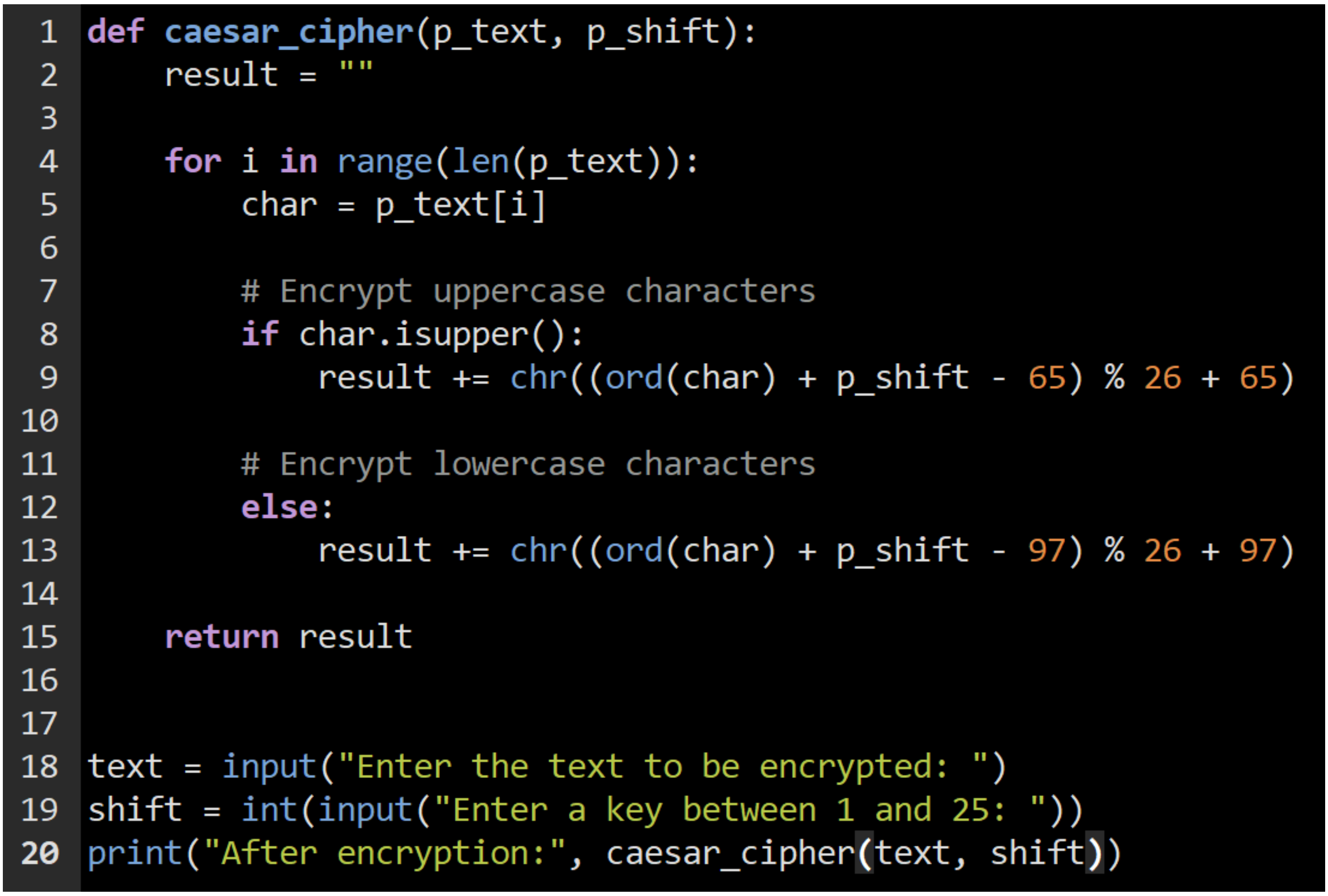
3. The Caesar Cipher is a simple encryption technique. Explain how the Caesar Cipher works by describing the steps involved in encrypting a message. (2)

4. Explain one advantage of using the Caesar Cipher. (2)

5. Describe one weakness of the Caesar Cipher and how it can be exploited to break the encryption. (2)

6. You have a message " `hqfubswlrqlpsuryhvgdwdvhfxulwb` " encrypted with a Caesar Cipher left shift of 3. Decrypt the message to reveal the original text. (1)

Here is a Python program to implement the Caesar cipher. Type it up if you want to see it in action. Then answer the questions underneath



```python
def caesar_cipher(p_text, p_shift):
    result = ""

    for i in range(len(p_text)):
        char = p_text[i]

        # Encrypt uppercase characters
        if char.isupper():
            result += chr((ord(char) + p_shift - 65) % 26 + 65)

        # Encrypt lowercase characters
        else:
            result += chr((ord(char) + p_shift - 97) % 26 + 97)

    return result


text = input("Enter the text to be encrypted: ")
shift = int(input("Enter a key between 1 and 25: "))
print("After encryption:", caesar_cipher(text, shift))
```

7. What type of programming structure begins on line 1? (1)
a) Selection
b) Iteration
c) Repetition
d) user-defined sub program

8. What is the special name for the variables inside the brackets on line 1? (1)

9. What is the correct term for a for loop, as shown starting on line 4? (1)
a) Selection
b) Iteration
c) Repetition
d) user-defined sub program

10. What does the built-in sub program ord( ) do? (1)

11. What does the built-in sub-program chr( ) do? (1)

12. What does the % sign mean on lines 9 and 13? (1)

13. Why is the number 65 there on line 9 and 97 there on line 13? (2)

14. Is the programming structure that starts on line 1 a function or a procedure? (1)

15. How can you tell? (1)

ANSWERS

1. C – the purpose of encryption is to scramble data to stop it being read by unauthorised people

2. Encryption means scrambling data with a key. The data becomes unreadable and can only be decrypted using the same key that is was encrypted with. Examples in the real-world include the HTTPS protocol where encrypted data is sent across the internet, and encrypting sensitive files when saving them on a network.

3. The Caesar cipher involves shifting the alphabet along by a set number – known as the key. This can be from 1 to 25. The shifted alphabet is lined up alongside a non-shifted alphabet and the plain text is then encrypted using the shifted alphabet.

4. An advantage of the Caesar cipher is its **simplicity**, which makes it easy to understand and implement for basic encryption needs.

5. The weakness of the Caesar cipher is there are only 25 possible keys. This means that it can quickly be cracked even without knowing the key. This makes it very insecure.

6. Encryption improves data security.

7. D – 'def' indicates that this is a user-defined sub-program

8. Parameters. They receive data passed from the main program. In this case, the text and the key

9. B – a for loop is iteration. It 'iterates' over every character in the string.

10. ord( )would contain a character inside the brackets…eg. ord("A") It will then return the ASCII value for that character.

11. chr ( ) would contain a number inside the brackets. Eg. chr(65)   It will then return the character that corresponds to the ASCII number.

12. The % sign indicates modulus division which is division where the result is just the remainder as a whole number.

13. Line 9 is dealing with upper case letters that were entered in the plain text. 65 is the ASCII code for capital A. Line 13 is dealing with lower case letters that are in the plain text. 97 is the ASCII code for lowercase a. (Remember: there are 32 values between a capital letter and its equivalent lower case because there are 6 codes for punctuation between Z and a)

14. The user-defined sub-program is a function.

15. You can tell because it has the return command at the end. A function returns a value back to the main program. A procedure doesn't; it just executes its code.