Faculty of Sciences | May 2026

Department of Computer Science | Last Name: ……

Course: Cybersecurity | First Name: ……

3rd year License ISIL | Group: …….

Written test 02 – Correction

Q01: What is the difference between symmetric and asymmetric encryption? (0.50pts)

Symmetric encryption uses a single secret key shared between parties for both encryption and decryption. In contrast, asymmetric encryption utilizes a pair of mathematically related keys: a public key for encryption and a private key for decryption. …….. **0.50**

Q02: What is a mono-alphabetic substitution cipher? Provide an example of such a cipher. (0.75pts)

A mono-alphabetic substitution cipher is a method of encryption where each letter of the plaintext is replaced by a single, fixed letter of the ciphertext throughout the entire message. A classic example of this is the Caesar cipher, which uses a fixed numerical shift for every letter in the alphabet. …… **0.75**

Q03: What is a poly-alphabetic substitution cipher? Provide an example of such a cipher. (0.75pts)

A poly-alphabetic substitution cipher is a method of encryption that uses multiple substitution alphabets to encrypt a single message. Unlike mono-alphabetic ciphers, the relationship between a plaintext letter and its ciphertext counterpart is not fixed; the same letter in the plaintext can be represented by different letters in the ciphertext depending on its position in the text. The most classic example of a poly-alphabetic substitution is the Vigenère Cipher**.** ……..…. **0.75**

Q04: Encrypt the message 'ENCR**Y**PTION ALGOR**I**THM' using the Vigenère cipher with the key 'secret'. Provide the calculation details only for the letters '**Y**' and '**I**'. (02pts)

To encrypt using the Vigenère cipher, the following formula is used: $C_i=(L_i+k_{\ i \bmod m}) \bmod 26$

where k represents the key and m its length (m=6 for "secret"). **…….. 0.25**

The letter '**Y**' is the 5th letter of the message (i=4).

Plaintext letter: L_4 = 'Y' = 24

Key letter: The 5th letter (i=4) of "secret" is '**e**'. Thus, $k_{\ 4 \bmod 6} = k_4$ = 'e' = 4

$C_4 = (L_4 + k_4) \bmod 26$ …. $C_4 = (24+4) \bmod 26$ …. $C_4 = (28) \bmod 26 = 2$ … $C_4 = 2$ → "C"

So, the letter 'Y' in the ciphertext is 'C' **……. 0.75**

The letter '**I**' is the 16th letter of the message (i=15).

Plaintext letter: L_{15} = 'I' = 8

Key letter: The 4th letter (i=3) of "secret" is '**r**'. Thus, $k_{\ 15 \bmod 6} = k_3$ = 'r' = 17

$C_{15} = (L_{15} + k_3) \bmod 26$ …. $C_{15} = (8+17) \bmod 26$ …. $C_{15} = (25) \bmod 26 = 25$ … $C_{15} = 25$ → "Z"

So, the letter 'I' in the ciphertext is 'Z'. **…….. 0.75**

In the end, the following ciphertext is "WREICILMQE EEYSTZXAE" **…… 0.25**

Q05: Decrypt the message 'FUBSWRJUDP' using the Caesar cipher with a key=3. Provide the calculation details only for the letters '**B**' and '**U**'. (02pts)

To decrypt using the Caesar cipher, the following formula is used: $L_i = (C_i - k) \bmod 26$.

where k represents the key (k=3). **…….. 0.25**

The letter '**B**' is the 3rd letter of the message (i=2).

Ciphertext letter: C_2 = 'B' = 1.

$L_2 = (C_2 - 3) \bmod 26$ … $L_2 = (1 - 3) \bmod 26$ …. $L_2 = -2 \bmod 26$ …. $L_2 = (-2+26) \bmod 26$

$L_2 = 24 \bmod 26 = 24$

$L_2 = 24$ → 'Y'. So, the letter 'B' in the plaintext is 'Y'. **…….. 0.75**

The letter '**U**' is the 8rd letter of the message (i=7).

Ciphertext letter: C_7 = 'U' = 20.

$L_7 = (C_7 - 3) \bmod 26$ … $L_7 = (20 - 3) \bmod 26$ …. $L_2 = 17 \bmod 26 = 17$

$L_7 = 17$ → 'R'. So, the letter 'U' in the plaintext is 'R'. **…….. 0.75**

In the end, the plaintext is **"Cryptogram".** **…….. 0.25**