Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

Université Internationale de Rabat
THE INNOVATIVE UNIVERSITY

Prepared by: EL M'RABET ZINEB , EL BEKKALI WISSAL

Lab 1: Introduction to Cryptography (Symmetric)

Review Questions:

1. The three main security goals are **confidentiality** that means information is not disclosed to unauthorized people, **integrity** ensures that data is not altered or tampered with without authorization and **availability** guarantee data and services are accessible when needed.

2. Passive attacks: attacker only observes (for example eavesdropping, traffic analysis).
Active attacks: attacker modifies or disrupts data (for example DoS, masquerading, replay)

3. Cryptography transforms the message into an unreadable format (ciphertext) so even if intercepted, it cannot be understood without the key. Steganography hides the existence of the message itself.

Exercises:

4.

- **Regular mail** : availability.
- **Regular mail with delivery confirmation** : availability.
- **Regular mail with delivery + recipient signature** : authentication and non-repudiation.
- **Certified mail** : confidentiality and authentication.
- **Insured mail** : availability and integrity.
- **Registered mail**: confidentiality, authentication, integrity, and non-repudiation.

5. a. Student breaks into office : Active attack (unauthorized access).
b. Check cashed for $100 instead of $10 : Modification attack (data integrity

violation).
c. Hundreds of fake emails sent : Denial of Service (DoS) attack.

6. a. School login with ID + password : Authentication.
b. Server disconnects after 2h : Access control.
c. The professor requires a preassigned ID : Authentication.
d. Bank requires signature : Authentication + Non-repudiation.

7. a. Steganography.
b. Cryptography.
c. Steganography.
d. Steganography.

8. Authentication, integrity and Non-repudiation.

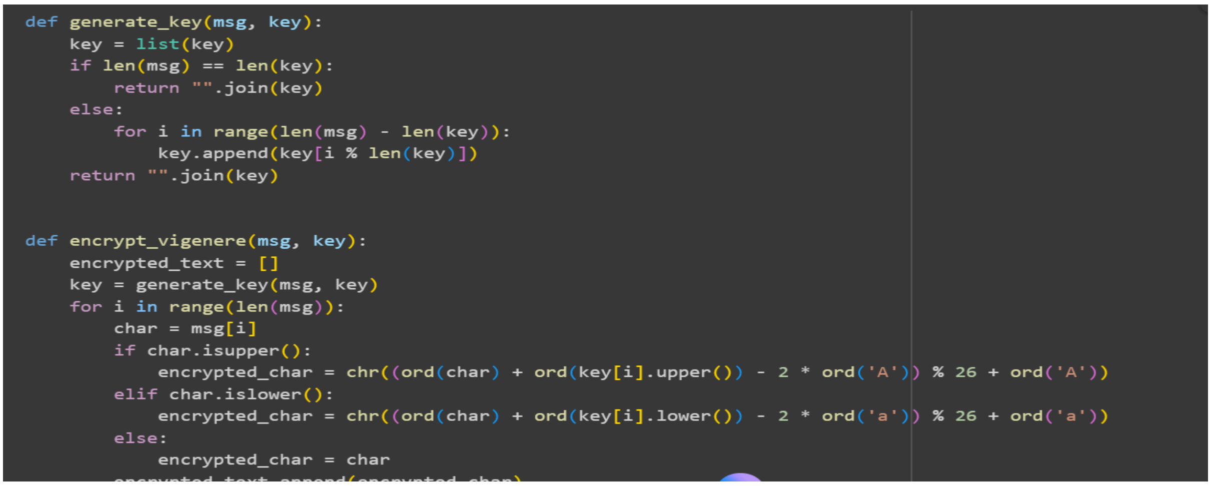
Exercise Additive and Multiplicative Ciphers:

a. C=(P+15) mod 26
   The result is Vdds Bdgcxcv Hipghwxct
b. P=(C−14) mod 26
   The result is THE MAN WHO SOLD THE WORLD
c. I (8) − E (4) = 4 so the key = 4.
   Plaintext = THE HOUSE IS NOW FOR SALE FOR FOUR MILLION DOLLARS IT IS WORTH MORE HURRY BEFORE THE SELLER RECEIVES MORE OFFERS
   So the key = 4 is correct.
d. C=(7 x P) mod 26
   hello -> XCZZU
e. C= (7 x P+2) mod 26
   hello -> zebbw
f. P=key^−1 x (C−b) mod 26 and key =7 , 7^−1=15
   so the formula is P=15 x (C−2)
   rwquprwbb ymgqgxe -> rocknroll suicide

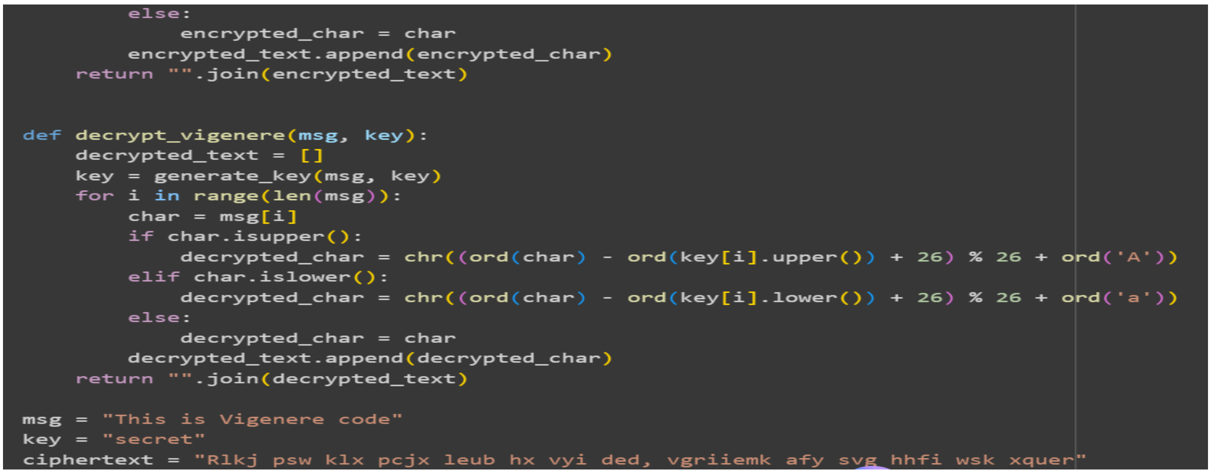
Exercise Vigenere:

Encryption formula: Ci=(Pi+Ki)mod 26

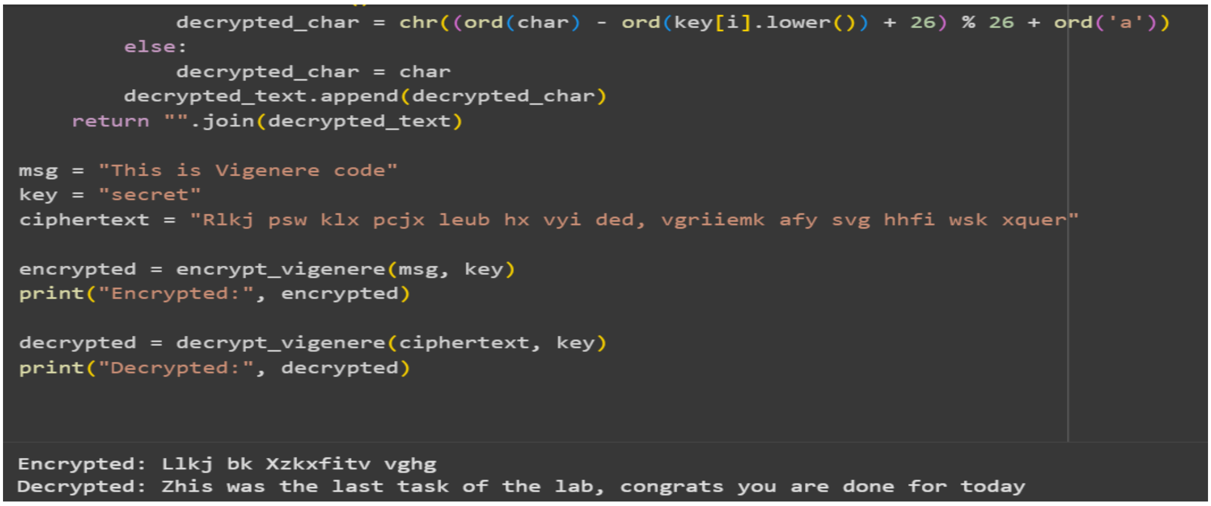
Decryption formula: Pi=(Ci−Ki+26)mod 26



```
def generate_key(msg, key):
    key = list(key)
    if len(msg) == len(key):
        return "".join(key)
    else:
        for i in range(len(msg) - len(key)):
            key.append(key[i % len(key)])
    return "".join(key)


def encrypt_vigenere(msg, key):
    encrypted_text = []
    key = generate_key(msg, key)
    for i in range(len(msg)):
        char = msg[i]
        if char.isupper():
            encrypted_char = chr((ord(char) + ord(key[i].upper()) - 2 * ord('A')) % 26 + ord('A'))
        elif char.islower():
            encrypted_char = chr((ord(char) + ord(key[i].lower()) - 2 * ord('a')) % 26 + ord('a'))
        else:
            encrypted_char = char
        encrypted_text.append(encrypted_char)
```



```
        else:
            encrypted_char = char
        encrypted_text.append(encrypted_char)
    return "".join(encrypted_text)


def decrypt_vigenere(msg, key):
    decrypted_text = []
    key = generate_key(msg, key)
    for i in range(len(msg)):
        char = msg[i]
        if char.isupper():
            decrypted_char = chr((ord(char) - ord(key[i].upper()) + 26) % 26 + ord('A'))
        elif char.islower():
            decrypted_char = chr((ord(char) - ord(key[i].lower()) + 26) % 26 + ord('a'))
        else:
            decrypted_char = char
        decrypted_text.append(decrypted_char)
    return "".join(decrypted_text)

msg = "This is Vigenere code"
key = "secret"
ciphertext = "Rlkj psw klx pcjx leub hx vyi ded, vgriiemk afy svg hhfi wsk xquer"
```



```
            decrypted_char = chr((ord(char) - ord(key[i].lower()) + 26) % 26 + ord('a'))
        else:
            decrypted_char = char
        decrypted_text.append(decrypted_char)
    return "".join(decrypted_text)

msg = "This is Vigenere code"
key = "secret"
ciphertext = "Rlkj psw klx pcjx leub hx vyi ded, vgriiemk afy svg hhfi wsk xquer"

encrypted = encrypt_vigenere(msg, key)
print("Encrypted:", encrypted)

decrypted = decrypt_vigenere(ciphertext, key)
print("Decrypted:", decrypted)
```

```
Encrypted: Llkj bk Xzkxfitv vghg
Decrypted: Zhis was the last task of the lab, congrats you are done for today
```