1. (16%) Given an Affine cipher defined as follows:

C = (P × K1 + K2 )mod 26

P = ((C − K2 ) × K1−1)mod 26

1. Please encrypt the plaintext “NCHU” using key (6,3).

明文 加密 密文

N->13 (13x06+3) mod 26 03->D

C->02 (02x06+3) mod 26 15->P

H->07 (07x06+3) mod 26 19->T

U->20 (20x06+3) mod 26 19->T

1. Please decrypt the ciphertext “HSWZ” using key (3,2).

密文 解密 明文

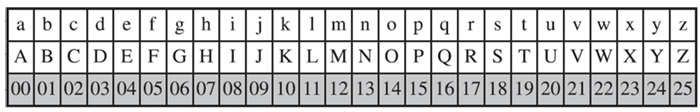
H->07 ((07-2)x3-1) mod 26 19->T

S->18 ((18-2)x3-1) mod 26 14->O

W->22 ((22-2)x3-1) mod 26 24->Y

Z->25 ((25-2)x3-1) mod 26 25->Z

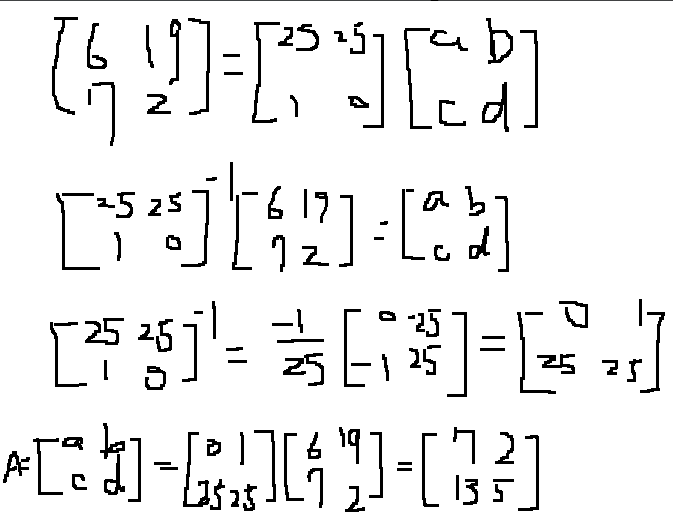
1. (12%) Consider a Hill cipher that uses a 2 × 2 square matrix 𝐴 as key. The elements of 𝐴 are integers in 𝑍26 that encodes the 26 English alphabets as follows:



Suppose the application of this Hill cipher yields the following results:

o The plaintext “ba” is encrypted into ciphertext “HC”.

o The plaintext “zz” is encrypted into ciphertext “GT”. Based on the above known plaintext results, please derive the key 𝐴 of the given Hill cipher.



1. (10%) Please give an example to illustrate the One-Time Pad (OTP) mechanism and further describe its advantages and disadvantages.

Example: A send to B

(i): A send HELLO with key “XYKLP”

(ii):XOR : XYKLP-> LVVND

(iii):Send to B

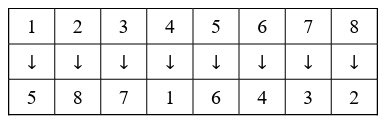
(iv):LVVND ->use key “XYKLP” -> HELLO

For sender and receiver, they both have a pre-shared pad of random keys. The pad consists of a series of random characters, with each character being used only once. Key is used to encrypt and decrypt a single message and then is discarded.

advantages : Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code

disadvantages: Problem of making large quantities of random keys, heavily used system might require millions of random characters on a regular basis, Mammoth key distribution problem.

1. (12%) Given a columnar transposition cipher that uses the following permutation table:



1. Please encrypt the plaintext “COMPUTER”.

1 2 3 4 5 6 7 8

C O M P U T E R

encrypt

P R E T C U M O

1. Please decrypt the ciphertext “VRPYYHRPITCAUGLO”.

1 2 3 4 5 6 7 8

V P Y R I C U L

R Y H P T A G O

Decrypt

I L U V C R Y P

T O G R A P H Y

1. (20%) 請用任何程式語言實作一個反轉換位的程式，將使用者所輸入的字串反向顯示。舉例來說，若使用者輸入“5793”，則程式輸出“3975”；若使用者輸入“this is a test”，則程式輸出“tset a si siht”。本程式不得依賴任何字串反轉的 API 來完成，並且須自行設計合適的防呆機制。

def reverse\_string(input\_str):

    if not isinstance(input\_str, str):

        raise TypeError("String!!!!")

    reversed\_str = ""

    for i in range(len(input\_str) - 1, -1, -1):

        reversed\_str += input\_str[i]

    return reversed\_str

user\_input = input("input: ")

try:

    reversed\_input = reverse\_string(user\_input)

    print("result:", reversed\_input)

except TypeError as e:

    print("錯誤:", e)

執行的方式: 使用python,

直接執行,終端機會出現”input:”字樣,

在後面輸入想轉換的字串,

會印出:”result: 反轉後的字串”



1. (30%) 凱撒密碼（Caesar cipher）是一種最簡單且最廣為人知的加密技術，它是一種代換法，將明文中的所有字母都在字母表上向後（或向前）按照一個固定數目進行偏移後取代替換成密文，如下圖所示。使用者可以輸入一個字串𝑡𝑒𝑥𝑡作為明文，及一個整數𝑘𝑒𝑦作為金鑰。請用任何程式語言實作一個加密函式𝑒𝑛𝑐𝑟𝑦𝑝𝑡𝑖𝑜𝑛(𝑡𝑒𝑥𝑡,𝑘𝑒𝑦)進行加密，並輸出密文；再實作一個解密函式𝑑𝑒𝑐𝑟𝑦𝑝𝑡𝑖𝑜𝑛(𝑡𝑒𝑥𝑡,𝑘𝑒𝑦)進行解密，並輸出明文。請自行設計程式的防呆機制。（提示：本程式需使用到字元與ASCII碼之間的轉換，鍵盤上各字元的ASCII碼如下頁附表所示）

def encryption(text, key):

    input\_text = ""

    for char in text:

        if char.isalpha():

            shift = key % 26

            if char.islower():

                input\_text += chr((ord(char) - ord('a') + shift) % 26 + ord('a'))

            elif char.isupper():

                input\_text += chr((ord(char) - ord('A') + shift) % 26 + ord('A'))

        else:

            input\_text += char

    return input\_text.upper()

def decryption(text, key):

    ciphertext = ""

    for char in text:

        if char.isalpha():

            shift = key % 26

            if char.islower():

                ciphertext += chr((ord(char) - ord('a') - shift) % 26 + ord('a'))

            elif char.isupper():

                ciphertext += chr((ord(char) - ord('A') - shift) % 26 + ord('A'))

        else:

            ciphertext += char

    return ciphertext.lower()

text = input("input: ")

while True:

    try:

        key = int(input("input your key(int): "))

        break

    except ValueError:

        print("The key must be an integer!!!")

encrypted\_text = encryption(text, key)

print("encrypt:", encrypted\_text)

decrypted\_text = decryption(encrypted\_text, key)

print("decrypt:", decrypted\_text)

執行的方式: 使用python,

直接執行,會在terminal出現”input:”,然後輸入想傳遞的訊息,enter,再輸入鑰匙(需是整數),enter,會出現加密後的結果以及解密後的結果:

