Advanced Security 1 | Lab 2

# Question 1

## Caesar

import string

plain\_text = input("Enter Message to be Encrypted: ")

print("Key Must be Integer")

shift = int(input("Enter Key: "))

shift %=26

alphabet = string.ascii\_letters

#Shiftinhg the Alphabet by the Key

shifted\_alphabet= alphabet[shift:] + alphabet[:shift]

#Mapping the Alphabet to the new Shifted Alphabet

eTable = str.maketrans(alphabet, shifted\_alphabet)

#Mapping the Shifted Alphabet to the Alphabet

dTable = str.maketrans(shifted\_alphabet, alphabet)

#Translating the Plain Text String into the new Encrypted String

encrypted = plain\_text.translate(eTable)

#Translating the Encrypted String back into the Plain Text String

decrypted = encrypted.translate(dTable)

print(encrypted)

print(decrypted)

## Vignere

import string

alphabet = "abcdefghijklmnopqrstuvwxyz "

letter\_to\_index = dict(zip(alphabet, range(len(alphabet))))

index\_to\_letter = dict(zip(range(len(alphabet)), alphabet))

def encrypt(message, key):

    encrypted = ""

    split\_message = [

        message[i : i + len(key)] for i in range(0, len(message), len(key))

    ]

    for each\_split in split\_message:

        i = 0

        for letter in each\_split:

            number = (letter\_to\_index[letter] + letter\_to\_index[key[i]]) % len(alphabet)

            encrypted += index\_to\_letter[number]

            i += 1

    return encrypted

def decrypt(cipher, key):

    decrypted = ""

    split\_encrypted = [

        cipher[i : i + len(key)] for i in range(0, len(cipher), len(key))

    ]

    for each\_split in split\_encrypted:

        i = 0

        for letter in each\_split:

            number = (letter\_to\_index[letter] - letter\_to\_index[key[i]]) % len(alphabet)

            decrypted += index\_to\_letter[number]

            i += 1

    return decrypted

def main():

    message = "he we will bring wano into the dawn"

    key = "strawhat"

    encrypted\_message = encrypt(message, key)

    decrypted\_message = decrypt(encrypted\_message, key)

    print("Original message: " + message)

    print("Encrypted message: " + encrypted\_message)

    print("Decrypted message: " + decrypted\_message)

main()

# Question 2

# Question 3

ONE VARIATION TO THE STANDARD CAESAR CIPHER IS WHEN THE ALPHABET IS "KEYED" BY USING A WORD. IN THE TRADITIONAL VARIETY, ONE COULD WRITE THE ALPHABET ON TWO STRIPS AND JUST MATCH UP THE STRIPS AFTER SLIDING THE BOTTOM STRIP TO THE LEFT OR RIGHT. TO ENCODE, YOU WOULD FIND A LETTER IN THE TOP ROW AND SUBSTITUTE IT FOR THE LETTER IN THE BOTTOM ROW. FOR A KEYED VERSION, ONE WOULD NOT USE A STANDARD ALPHABET, BUT WOULD FIRST WRITE A WORD (OMITTING DUPLICATED LETTERS) AND THEN WRITE THE REMAINING LETTERS OF THE ALPHABET. FOR THE EXAMPLE BELOW, I USED A KEY OF "RUMKIN.COM" AND YOU WILL SEE THAT THE PERIOD IS REMOVED BECAUSE IT IS NOT A LETTER. YOU WILL ALSO NOTICE THE SECOND "M" IS NOT INCLUDED BECAUSE THERE WAS AN M ALREADY AND YOU CAN'T HAVE DUPLICATES.

# Question 4

This Caesar Cipher had a Shift Key of 17

# Question 5

NIST IS ABOUT TO ANNOUNCE THE NEW HASH ALGORITHM THAT WILL BECOME SHA-3. THIS IS THE RESULT OF A SIX-YEAR COMPETITION, AND MY OWN SKEIN IS ONE OF THE FIVE REMAINING FINALISTS (OUT OF AN INITIAL 64). IT'S PROBABLY TOO LATE FOR ME TO AFFECT THE FINAL DECISION, BUT I AM HOPING FOR "NO AWARD." IT'S NOT THAT THE NEW HASH FUNCTIONS AREN'T ANY GOOD, IT'S THAT WE DON'T REALLY NEED ONE. WHEN WE STARTED THIS PROCESS BACK IN 2006, IT LOOKED AS IF WE WOULD BE NEEDING A NEW HASH FUNCTION SOON. THE SHA FAMILY (WHICH IS REALLY PART OF THE MD4 AND MD5 FAMILY), WAS UNDER INCREASING PRESSURE FROM NEW TYPES OF CRYPTANALYSIS. WE DIDN'T KNOW HOW LONG THE VARIOUS SHA-2 VARIANTS WOULD REMAIN SECURE. BUT IT'S 2012, AND SHA-512 IS STILL LOOKING GOOD.

EVEN WORSE, NONE OF THE SHA-3 CANDIDATES IS SIGNIFICANTLY BETTER. SOME ARE FASTER, BUT NOT ORDERS OF MAGNITUDE FASTER. SOME ARE SMALLER IN HARDWARE, BUT NOT ORDERS OF MAGNITUDE SMALLER. WHEN SHA-3 IS ANNOUNCED, I'M GOING TO RECOMMEND THAT, UNLESS THE IMPROVEMENTS ARE CRITICAL TO THEIR APPLICATION, PEOPLE STICK WITH THE TRIED AND TRUE SHA-512.

AT LEAST FOR A WHILE. I DON'T THINK NIST IS GOING TO ANNOUNCE "NO AWARD"; I THINK IT'S GOING TO PICK ONE. AND OF THE FIVE REMAINING, I DON'T REALLY HAVE A FAVORITE. OF COURSE I WANT SKEIN TO WIN, BUT THAT'S OUT OF PERSONAL PRIDE, NOT FOR SOME OBJECTIVE REASON. AND WHILE I LIKE SOME MORE THAN OTHERS, I THINK ANY WOULD BE OKAY. WELL, MAYBE THERE'S ONE REASON NIST SHOULD CHOOSE SKEIN. SKEIN ISN'T JUST A HASH FUNCTION, IT'S THE LARGE-BLOCK CIPHER THREEFISH AND A MECHANISM TO TURN IT INTO A HASH FUNCTION. I THINK THE WORLD ACTUALLY NEEDS A LARGE-BLOCK CIPHER, AND IF NIST CHOOSES SKEIN, WE'LL GET ONE.

# Question 6

Swahili

CHAMA Cha Mapinduzi along with its youth through its UVCCM coalition, has slammed the former Chairman of the Commission for Constitutional Change, Justice Joseph Warioba, urging him to stop deceiving himself, as the issue of a new Constitution cannot be on the agenda for next year's general election. In the case of UVCCM, it has asked Judge Warioba to immediately stop using the mandate he was given to be the Chairman of the Commission for Constitutional Change, as his term has expired legally. The remarks were made at various times by party leaders, just days after Judge Warioba made his views on the Draft proposed by the Constituent Assembly, in which he criticized the omission of some public comments.

In addition, he has maintained that he will be the President of Tanzania, regardless of religion, ethnicity or party affiliation, so the development of his government will not discriminate. Speaking yesterday in the city here at a campaign rally attended by thousands of people who he admitted was the greatest he had ever seen, he assured them that he would run the country civilized and not dictatorial as some people have been claiming.

Even after being elected, I will not change, I will remain your same child John Magufuli, said and added; I will run the country in a civilized way, I will not run the country in a dictatorship there have been people talking, because I speak the truth and the truth will remain the truth. People remain threatening each other. You Chato people tell them the truth that when I was a minister I used to herd cattle, I used to milk milk