

Programme Name: \_\_\_\_\_\_\_\_**BCS HONS**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Course Code: \_\_**CSC 2730**\_\_\_\_\_\_\_

Course Name: \_\_\_\_\_\_\_\_**Network And Data Security**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Open Book Examination**

Date of Submission: \_\_\_\_\_\_**3/5/2020**\_\_\_\_\_\_\_\_\_\_\_\_\_

**Submitted By: Submitted To:**

Student Name**: Dipesh Tha Shrestha** Faculty Name**: Manoj Gautam**

IUKL ID: **041902900028** Department**: LMS**

Semester**: Third Semester**

Intake**: September 2019**

1. **Implement a Caesar cipher encryption and decryption algorithm for the given pseudo function**

**a. function encrypt(message=”SKYISBLUE”, key=13)**

**b. function decrypt(cipher=encrypt(message=”SKYISBLUE”, key=13), key=13)**

**Answer:**

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Algorithm for Caesar Cipher:

Input:

1. A String of upper-case letters, called Text.
2. An Integer between 0-25 denoting the required shift that is 13.

Procedure:

1. Traverse the given text one character at a time
2. For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
3. Return the new string generated.

Implementation in Python:

Encryption function

# A python program to illustrate Caesar Cipher Technique

def encrypt(text, s):

result = ""

# traverse text

for i in range(len(text)):

char = text[i]

# Encrypt uppercase characters

if (char.isupper()):

result += chr((ord(char) + s - 65) % 26 + 65)

# Encrypt lowercase characters

else:

result += chr((ord(char) + s - 97) % 26 + 97)

return result

# check the above function

text = "SKYISBLUE"

s = 13

print( "Text : " + text)

print( "Shift : " + str(s))

print("Cipher: " + encrypt(text, s))

In the above function:

Text: SKYISBLUE

Then using the give key: 13, we shift each characters in the Text by 13 letters.

The encryption algorithm results in the text “FXLVFOYHR”.

Decryption Function:

# A python program to illustrate Caesar Cipher Technique

def decrypt(text, s):

result = ""

# traverse text

for i in range(len(text)):

char = text[i]

# Encrypt uppercase characters

if (char.isupper()):

result += chr((ord(char) + s - 65) % 26 + 65)

# Encrypt lowercase characters

else:

result += chr((ord(char) + s - 97) % 26 + 97)

return result

# check the above function

text = "FXLVFOYHR"

s = 13

print( "Text : " + text)

print( "Shift : " + str(s))

print("Cipher: " + decrypt(text, s))

Similarly,

In the above function:

Text: FXLVFOYHR

Then using the give key: 13, we shift each characters in the Text by 13 letters.

The decryption algorithm results in the text “SKYISBLUE”

1. **With regards to network and data security, implementing password is an ideal solution for user authentication and to protect the data. Justify THREE (3) main concerns with the use of passwords for authentication.**

**Answer:**

Network and data security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment. Authentication is the process that ensures the individual requesting access to a system, website, or application is the intended user.

When it comes to protecting your information online, passwords are the most-used form of authentication for websites and applications alike. However, passwords are also one of the most insecure forms of user authentication out there.

Upon registration, users create a unique ID and key (typically a username and password) that are then stored securely on the website’s server. Ideally, the user is the only person with knowledge of their password, making it so that they’re the only one able to access the account. When the user re-enters their credentials, they are checked against those stored in the web server and, if they are a match, the user is verified.

The challenge is that since passwords are so widely used, the number of insecure accounts is substantial. Not to mention, passwords can provide a false sense of security when users are woefully unaware of the vulnerabilities they bring. **Passwords are not only difficult to manage on a personal level but can also cause large-scale data breaches when they are easily guessed or cracked by hackers.**

THREE (3) main concerns with the use of passwords for authentication are given below:

* **Shoulder Surfing Attack**

Shoulder surfing is looking over someone’s shoulder when they enter a password or a PIN code. It is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Considering all the above, there is a growing trend among many enterprises globally to move to a stronger authentication solution which provides high level of security with-out compromising the users convenience.

* **Problems with passwords** **that needs to be continuously changed.**

Computer systems require frequent password changes, to make the system robust from various attacks. Users must think of new passwords that conform to all of the organizations requirements but that are also easy to remember. System-enforced password policies, however, cannot guarantee password secrecy.

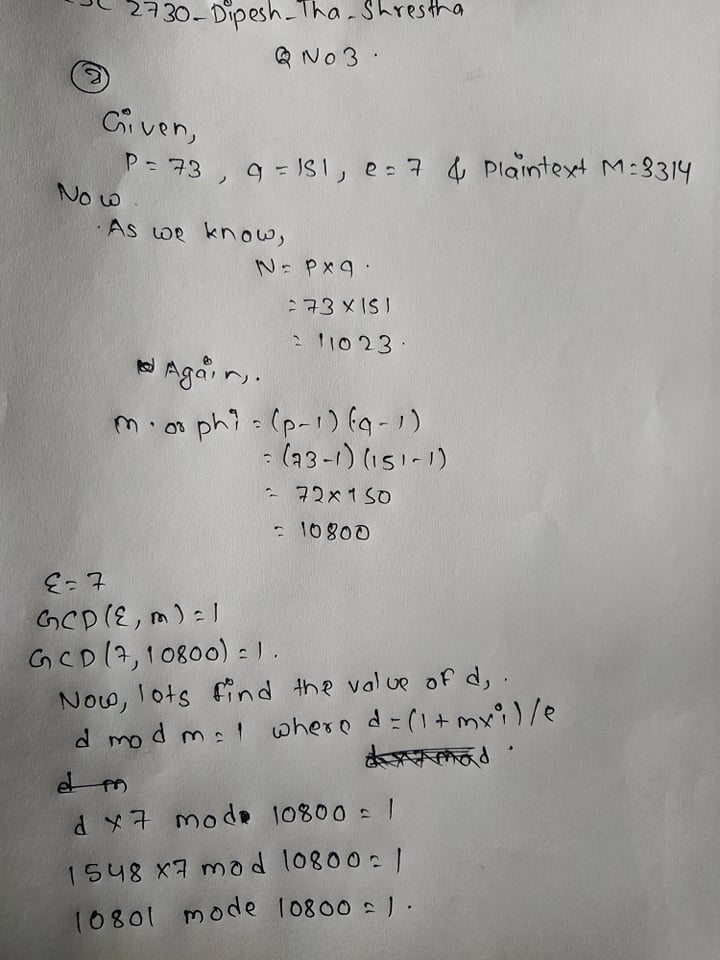
* **Easy passwords can be cracked**

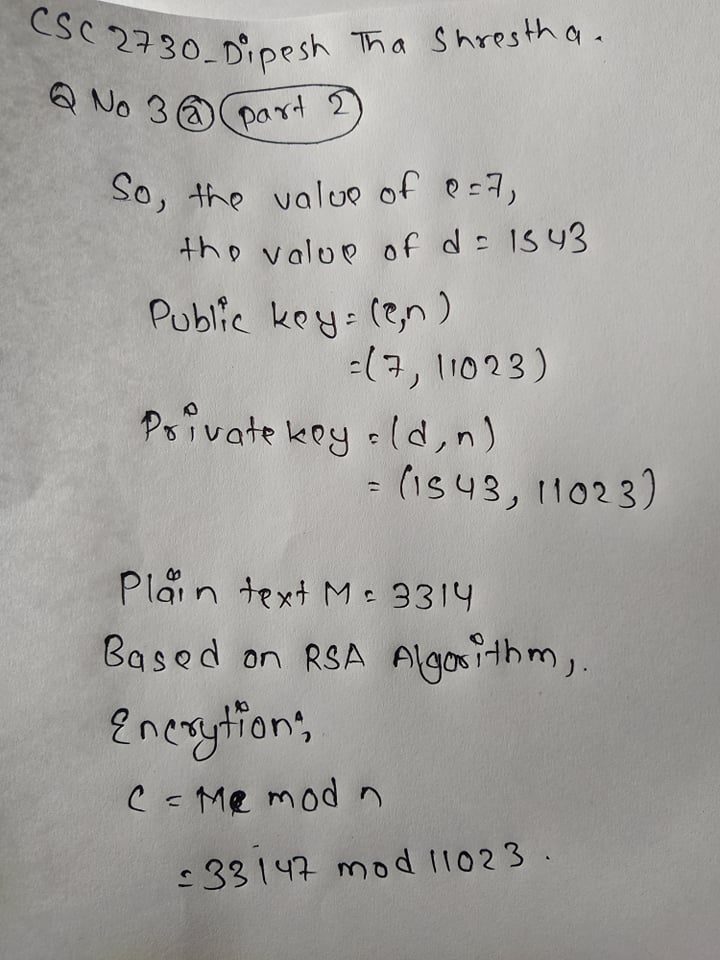
The end users behavior such as choosing passwords that are easy to remember introduces the majority of the password weaknesses. For a hacker, these passwords can easily be cracked or guessed. Surveys show that frequent passwords are the word password, personal names of family members, names of pets, and dictionary words.

1. **Perform the encryption and decryption using RSA algorithm for the following:**

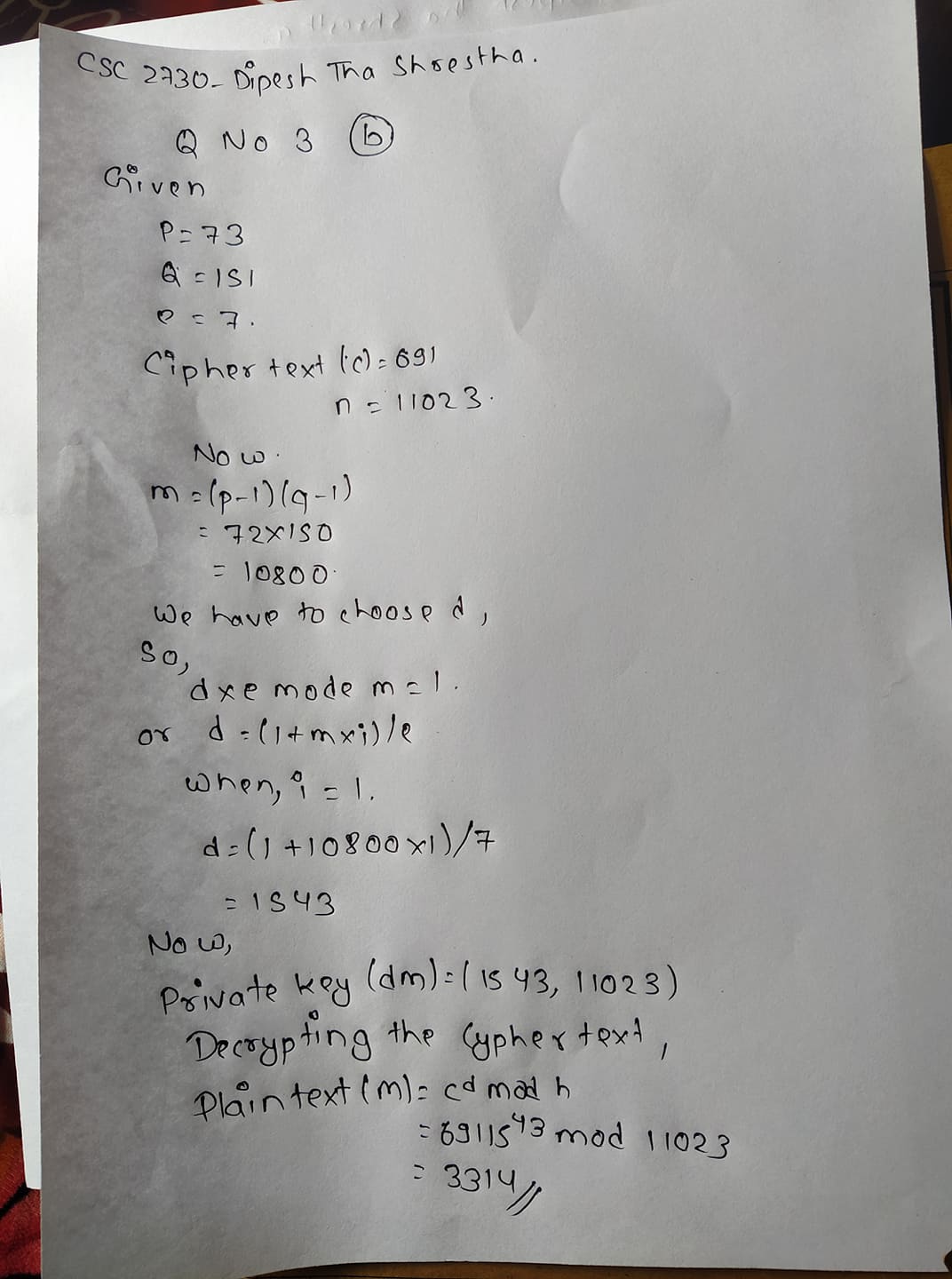
**P = 73, q = 151, e = 7; plaintext M=3314;**

1. **In Public key system using RSA, Bob sent a plaintext M = 3314 to Alice using her public key. What is the generated cipher text C?**





1. **A man in the middle intercept the cipher text C from Bob sent to Alice. Discuss the complete working process how to find the plaintext M.**

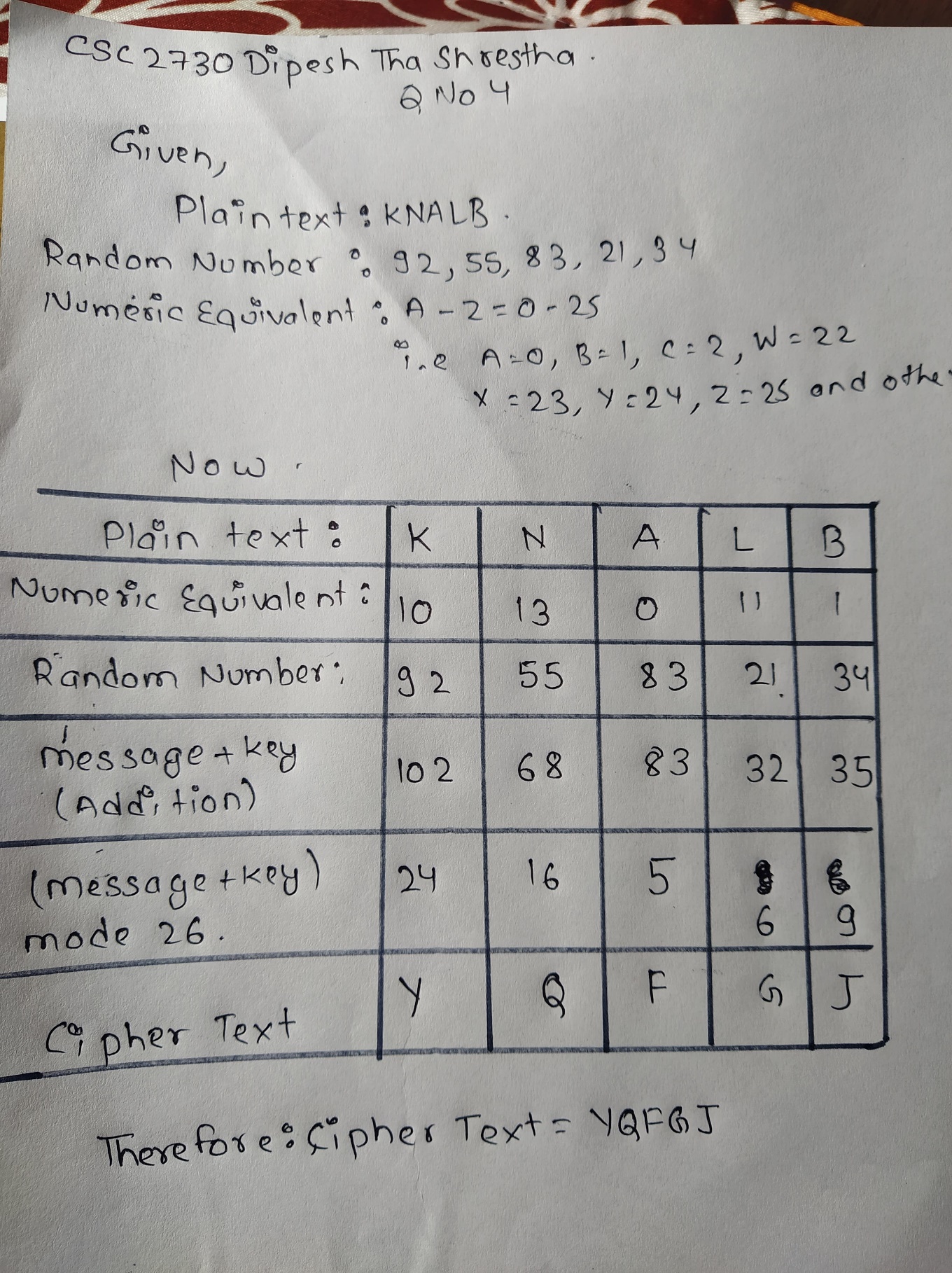


1. **One time pad algorithms are devised by Gilbert Vernam for AT&T. Encrypt the plain text shown below by using Vernam ciphers technique and given random number. Write your calculation.**

**Plaintext: KNALB**

**Random Number: 92, 55, 83, 21, 34**

**Numeric Equivalent: A – Z = 0 – 25**



1. **For the Sentence “STUDYISFUN”, generate an equivalent cipher text using play fair cipher the given key is “MONARCHY”**

