SUNWAY

INT’L BUSINESS SCHOOL

Programme Name: **BCS HONS**

Course Code: **CSC 2730**

Course Name: **Network And Data Security**

Internal Examination

Date of Submission: **1/21/2021**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

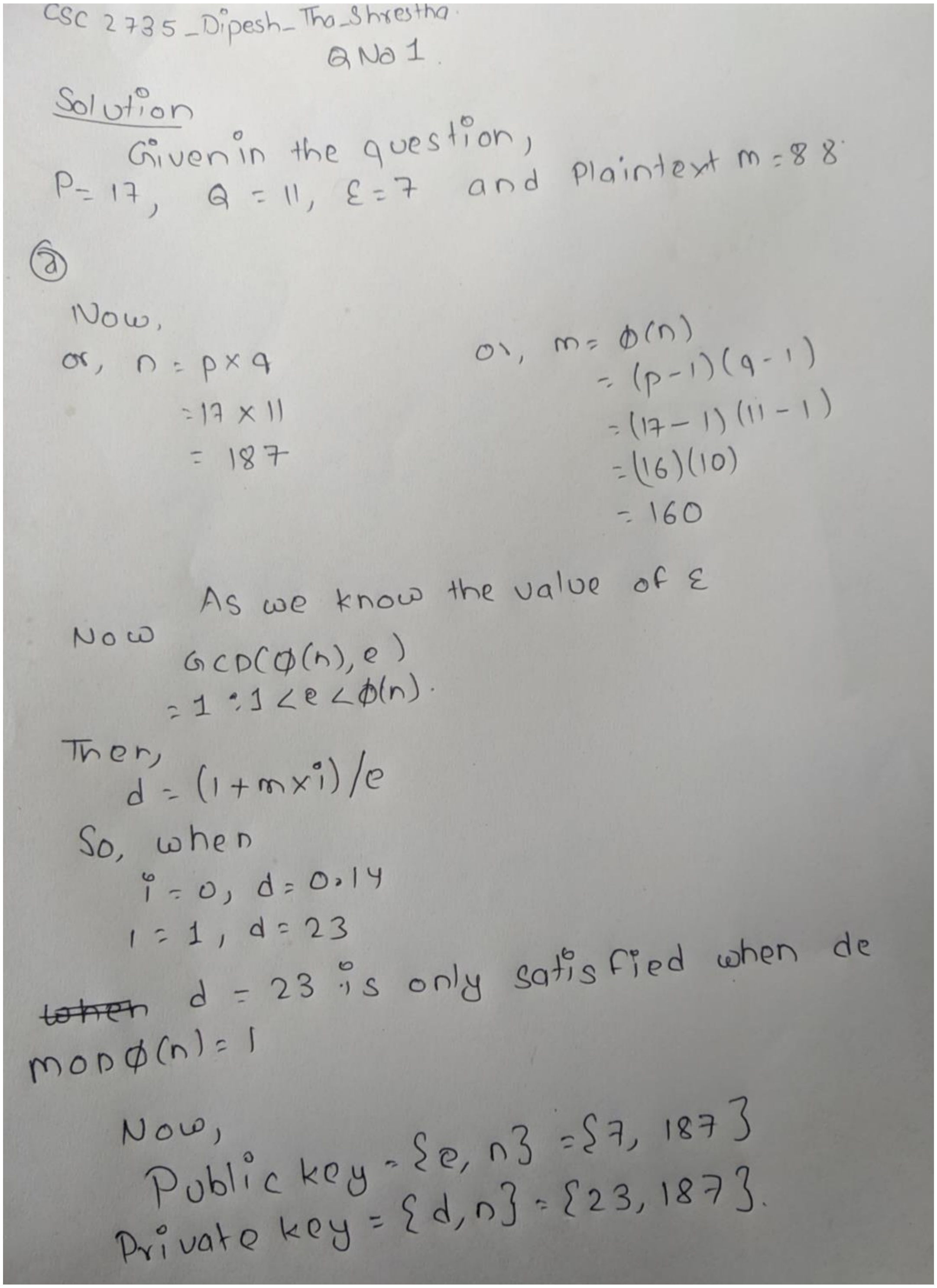
Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

1. **Perform encryption and decryption using RSA algorithm as shown below for the following.**
   P = 17, Q = 11, E= 7; Plain Text M = 88
   a. **In a public key system using RSA, Bob sent a plain text M=88 to Alice using her public key. What is the generated Cipher text C?**
   b. **Alice decrypts using her private key. Show the complete working process how to find the plaintext M?**



CSC 2735_Dipesh_Tha_Shrestha.

QNo 1.

Solution

Given in the question,
$P = 17$, $Q = 11$, $E = 7$ and plaintext $m = 88$.

(a)

Now,
or, $n = p \times q$
$= 17 \times 11$
$= 187$

or, $m = \phi(n)$
$= (p-1)(q-1)$
$= (17-1)(11-1)$
$= (16)(10)$
$= 160$

As we know the value of E

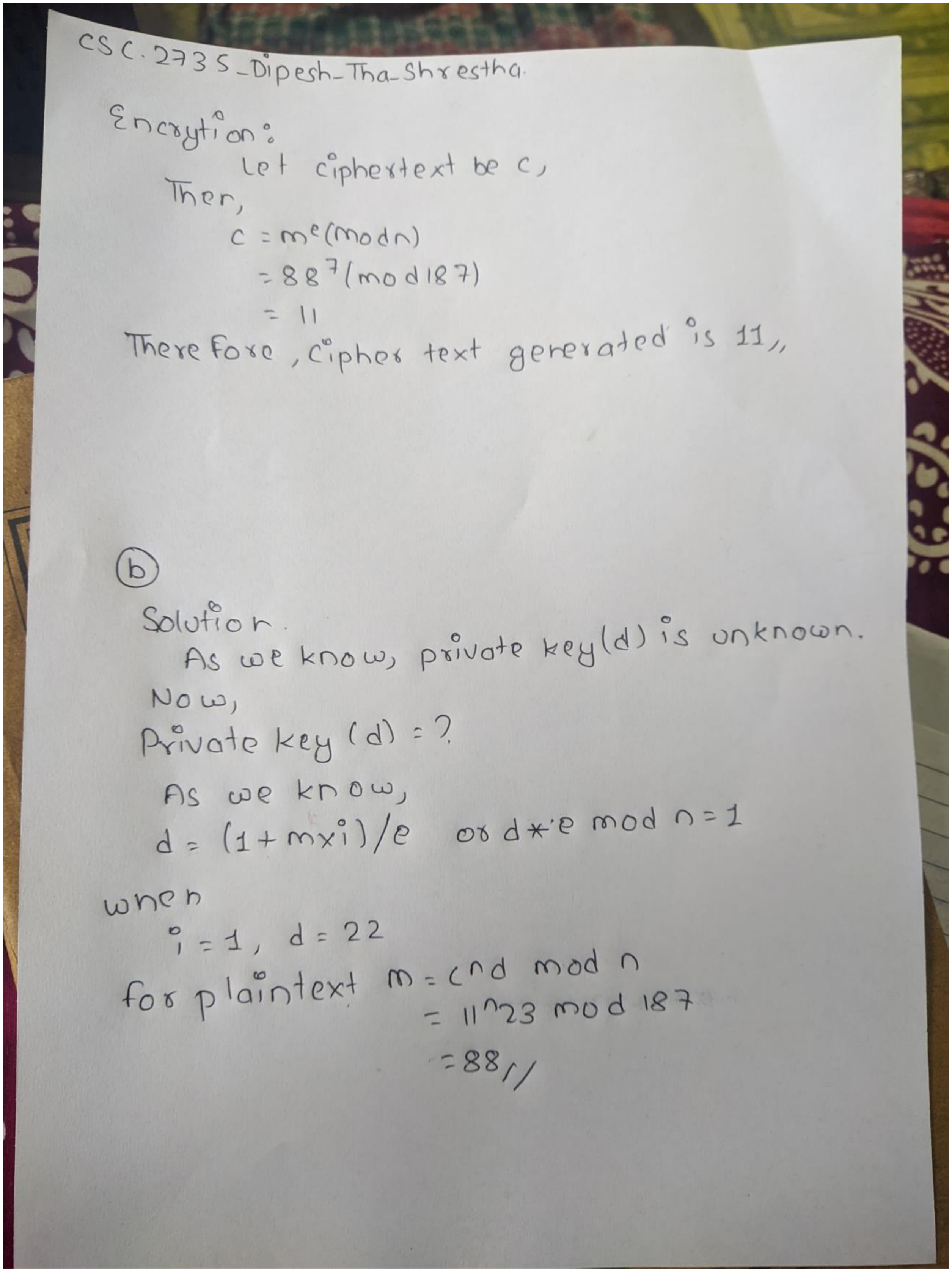
Now $GCD(\phi(n), e)$
$= 1 \therefore 1 < e < \phi(n)$.

Then,
$d = (1 + m \times i)/e$

So, when
$i = 0$, $d = 0.14$
$1 = 1$, $d = 23$

~~when~~ $d = 23$ is only satisfied when de $\bmod \phi(n) = 1$

Now,
Public key $= \{e, n\} = \{7, 187\}$
Private key $= \{d, n\} = \{23, 187\}$.



CSC.2735_Dipesh_Tha_Shrestha.

Encrytion:

Let ciphertext be c,

Then,

$c = m^e (\bmod n)$

$= 88^7 (\bmod 187)$

$= 11$

There Fore, cipher text generated is 11,,

(b)

Solution.

As we know, private key(d) is unknown.

Now,

Private key (d) = ?

As we know,

$d = (1 + m \times i)/e$ or $d * e \bmod n = 1$

when

$i = 1, \ d = 22$

for plaintext $m = c^\wedge d \bmod n$

$= 11^\wedge 23 \bmod 187$

$= 88$ //

2. **Robert runs a large website that allows users to log in and share images. When a new user sets up their account, the website hashes their password with SHA256 and stores the hash in a database. When a user logs in, the website hashes the supplied password with SHA265 and compares it to the stored hash. Robert figures that with this scheme, if anyone hacks into his database, they will only see hashes and won't learn the user's passwords. Out of curiosity, Robert does a Google search on several hashes in the database and is alarmed to find that, for a few of them, the google search results reveal the corresponding password.**

a) **What is the risk that it introduces and how many of Robert's users could be affected?**

Answer; The risk that it introduces is in this case passwords are stored with outdated irreversible cryptographic functions (SHA256,SHA265). As all password are frequently used and are among the most used password, also these both passwords are of same hash so they do not have a notion of randomness. Therefore, the risk it shows, is it is possible to retrieve all hashes directly by queries in a search engine except for the users who has a complex password. If the hashes are not found directly in google, the attacker has other methods such as, Brute force, Dictionary, Rainbow table, Benchmark to retrieve Md5 password, Improving SHA512, Inappropriate hash function, etc.

b) **How should Robert store passwords?**

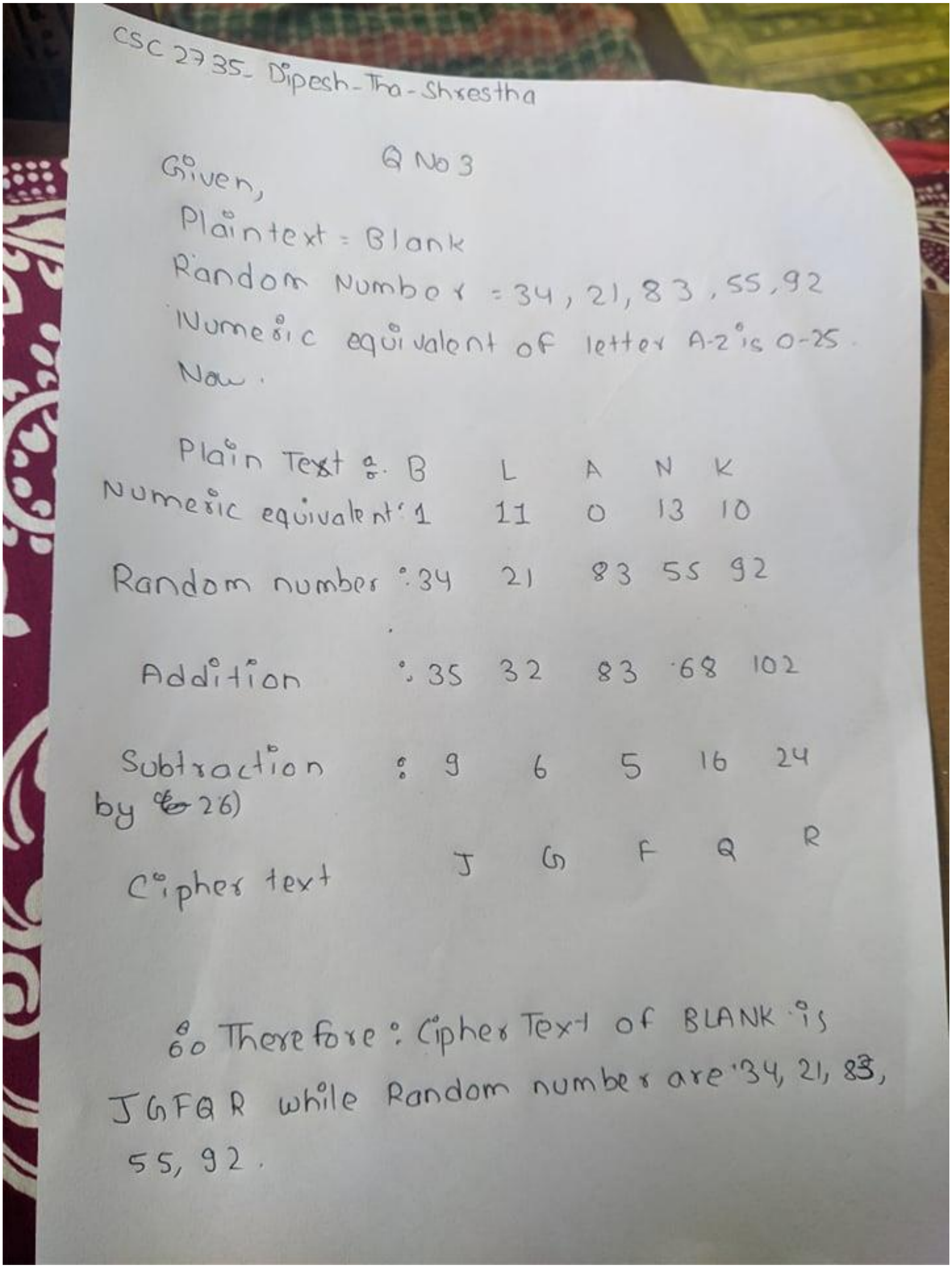
Answer: Robert should store the password by adding some salt to them. A salt is a random data that concatenated with your password before sending it as the input of the hashing function. For example, if your password is abc and the salt is Sunway@12020, the result of hash Function('abc!Sunway@12020') will be stored in the database instead of hash Function('abc'). Hence the rainbow table attacks won't be effective now as the probability that rainbow table contains hash of 'abc!Sunwway@12020' is meager (because generally rainbow tables are constructed from common wordwords, dictionary words etc)

3. **One time pad ciphers are devised by Gilbert Vernam for AT&T. Encrypt the plaintext below using the Vernam cipher technique and given random number. Write your calculation**

Plaintext: BLANK

Random Number: 34, 21 83, 55, 92

Numeric equivalent of letters A-z is 0 to 25.



CSC 2735_ Dipesh_Tha-Shrestha

Q No 3

Given,

Plaintext = Blank

Random Number = 34, 21, 83, 55, 92

Numeric equivalent of letter A-Z is 0-25.

Now.

Plain Text :	B	L	A	N	K
Numeric equivalent :	1	11	0	13	10
Random number :	34	21	83	55	92
Addition :	35	32	83	68	102
Subtraction by 26) :	9	6	5	16	24
Cipher text	J	G	F	Q	R

∴ Therefore : Cipher Text of BLANK is JGFQR while Random number are 34, 21, 83, 55, 92.