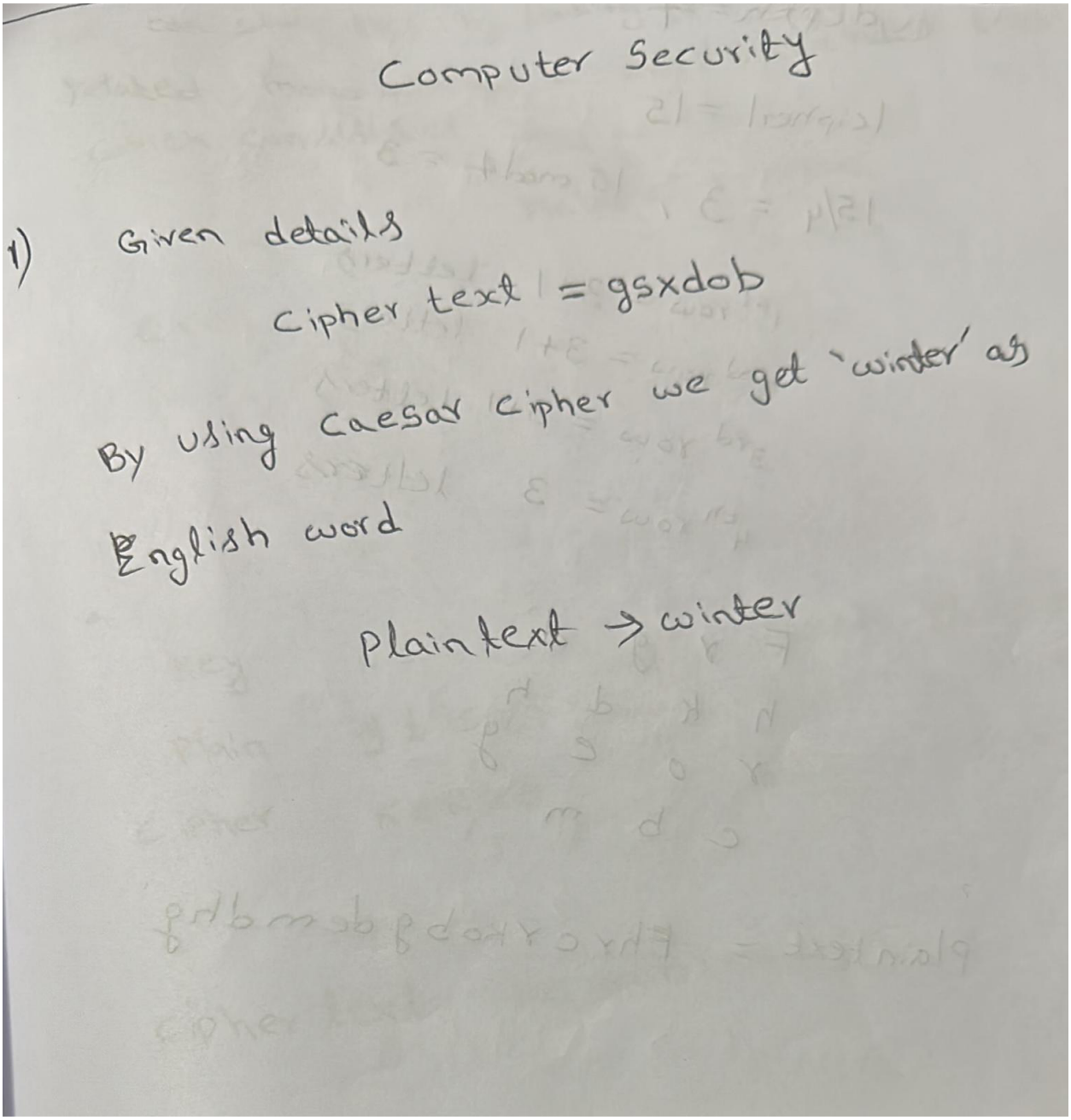
Computer Security
Assignment-2

Team members:

Sri Harsha Tanamala (stanama1@binghamton.edu)
Akhil Madiri (amadiri1@binghamton.edu)



```
s='gsxdob'
a='abcdefghijklmnopqrstuvwxyz'
for i in range(0,26):
    temp=''
    for j in range(len(s)):
        res=a.find(s[j])
        c=res-i-1
        if c>=26:
            c=c-26
        temp+=a[c]
    print('value for key ',i+1,'=',temp)
```

```
value for key  1 = frwcna
value for key  2 = eqvbmz
value for key  3 = dpualy
value for key  4 = cotzkx
value for key  5 = bnsyjw
value for key  6 = amrxiv
value for key  7 = zlqwhu
value for key  8 = ykpvgt
value for key  9 = xjoufs
value for key  10 = winter
value for key  11 = vhmsdq
value for key  12 = uglrcp
value for key  13 = tfkqbo
value for key  14 = sejpan
value for key  15 = rdiozm
value for key  16 = qchnyl
value for key  17 = pbgmxk
value for key  18 = oaflwj
value for key  19 = nzekvi
value for key  20 = mydjuh
value for key  21 = lxcitg
value for key  22 = kwbhsf
value for key  23 = jvagre
value for key  24 = iuzfqd
value for key  25 = htyepc
value for key  26 = gsxdob
```

2) Given details

ciphertext → frgdhkdhroegcbm

depth = 4

|cipher| = 15

15/4 = 3, 15 mod 4 = 3

1st row = 3+1 letters

2nd row = 3+1 letters

3rd row = 3+1 Letters

4th row = 3 letters

F r g d

h k d h

r o e g

c b m

plaintext = Fhrcrkobgdemdhg

3) Given details

plain text - 'it is raining

key word → clock

we can solve this by looking the set of related mono alphabetic substitution rules table which consists of key as row

plaint as column

ex:-

	a	b	c	...
a	a	b	c	
b	b	c	d	
c	c	d	e	
⋮				

key clock

plain gtisr

cipher KewuB

next →

clock gtisra

gtisraining

KewuBgBvaeg

cipher text KewubibvaEg

4) Given

Plain text → heecggs

Key word → class

matrix

c	l	a	s	b
d	e	f	g	h
i/j	k	m	n	o
p	q	r	t	u
v	w	x	y	z

heecggs → he ec gx gs

he → df
ec → dl
gx → fy
gs → ng

Cipher text → df dl fy ng

5) Given

plaintext → dhdplakshgis

Key → 315264

	1	2	3	4	5	6
Key :	3	1	5	2	6	4
plaintext :	d	h	d	p	l	a
	k	s	h	g	i	s

cipher text → dhdkLihsaspg

6)

1) 001000 → Row 0 Column 4

001011 → Row 1 column 5

101100 → Row 2 Column 6

100111 → Row 3 column 3

2) Given

001101

01 → Row 1

0110 → Colum 6

Value 13 output 1101

7)

1) The 20^{th} bit of input is 1 and
15^{th} bit of input is 1 all others are 0

2) 23^{rd} bit of output is 1 and
16^{th} bit of output is 1 all others are 0

8) $3^{502} \bmod 11$

$3^{10} \equiv 1 \pmod{11}$

$502 = 50 \cdot 10 + 2$

$= (3^{10})^{50} \cdot 3^2 = 1^{50} \cdot 3^2$

$= 9 \pmod{11}$

$= 9$

9) output bits of 58 is 29 30 31 32

29 → 5
30 → 27
31 → 15
32 → 21

5 → 6 : 51
5 → 8 : 52
27 → 40 : 57
15 → 22 : 54
21 → 30 : 55
21 → 32 : 56

51, 52, 54, 55, 56, 57