Question 1.

I: Confidentiality, one of three concepts that forms the CIA triad. Confidentiality is preserving restrictions on access to information and handing out information. It also means for protecting personal privacy and/or proprietary information. We want to render data unintelligible to unauthorized users through encryption.

For example, with student grade information. That information is valuable to the students and keeping that information confident is highly important to the students. You only want the students, and the employers that need the information to do their job to have access to that information. That information could be modified by an unauthorized entity and the grade could be changed.

II: Integrity is about defending against modification or destruction of information. We want to detect unauthorized modifications.

If you were to text a friend that you will be hosting a movie night at Saturday 8:00PM, you don't want that information to be modified in an unauthorized manner, and have it for example say: next Sunday at the middle of the night.

III: Authenticity, means to verify the identity of an entity, through the digital signature.

When you login to your bank account, you are verifying that it is the correct place to be logging into, the same way the bank verifies that the correct person is attempting to gain access to the account. Let's say you're you want to login to Facebook, but when you type in the URL, a fake version of Facebook comes up. Maybe because you mistyped the URL wrong. That fake version of Facebook might want you to login, and when you do, your Facebook login details have been recorded, and assuming you use the same password/email elsewhere, they now have your login details there as well.

To counter this, when you go to the URL, you can verify that it is the correct receiver of your information through the padlock in the URL area. That shows the certificates that have been issued to the website. That will tell you if your information is private and secure, and whether it is the correct website.

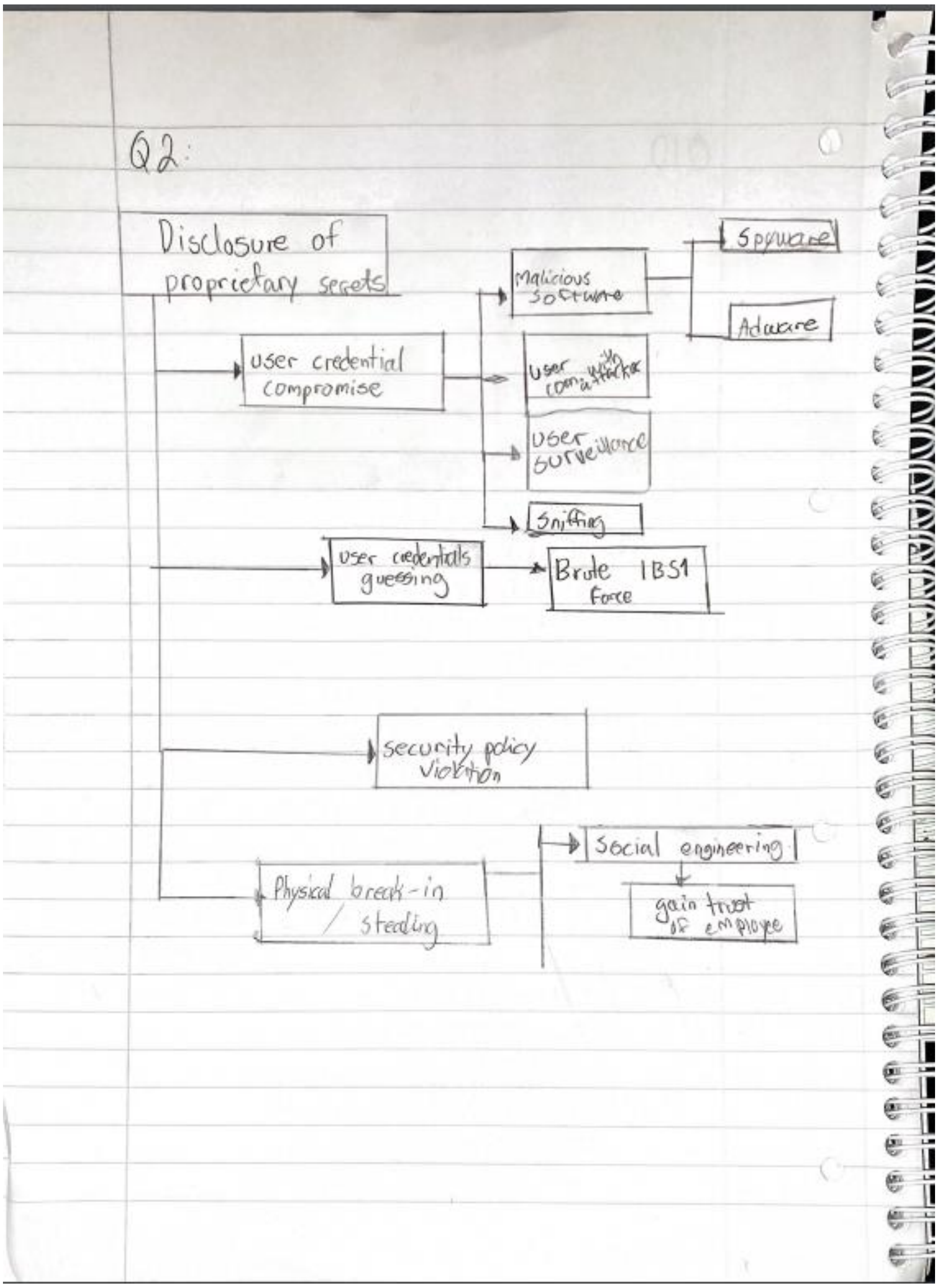
IV: Accountability is the security goal. It supports nonrepudiation (Sender cannot deny sending a message, with the digital signature), deterrence, fault isolation, intrusion detection and prevention. After-action, recovery and legal action.

All the processes in the system should be logged and if any bad actions are taken in the system, it can be traced back to the entity that performed such actions. If you were to buy something online, and the seller does not deliver the product. You want a way to prove that the seller did not deliver as promised so that legal action can be taken.

V: Availability, to ensure reliable and timely access to information. That the property of a system being made accessible, usable or operational when needed, and by an authorized entity.

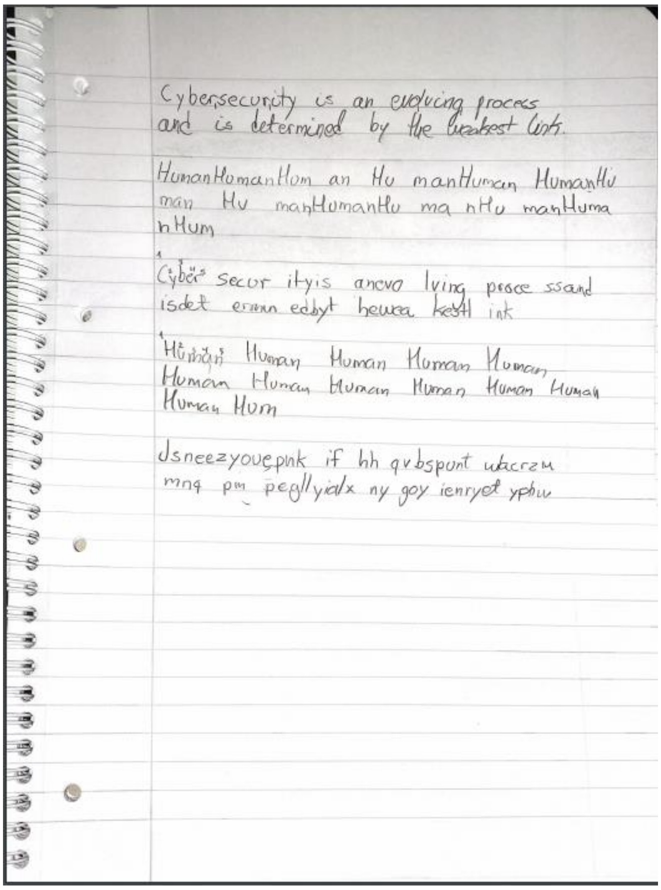
With availability, you can deny access to information with a Distributed Denial of Service attack (DDoS). DDoS overwhelms the server so that it can not be used. You can counter DDoS by mitigating it elsewhere, through perhaps a company the specializes on the topic.

Question 2.



Question 3.

I:



Cybersecurity is an evolving process
and is determined by the weakest link.

HumanHumanHum an Hu manHuman HumanHu
man Hu manHumanHu ma nHu manHuma
nHum

Cyber secur ityis anevo lving proce ssand
isdet ermin edbyt hewea kestl ink

Human Human Human Human Human
Human Human Human Human Human Human
Human Hum

Jsneezyouepnk if hh qvbspunt wlacrzm
mnq pm pegllyialx ny goy ienryet yphw

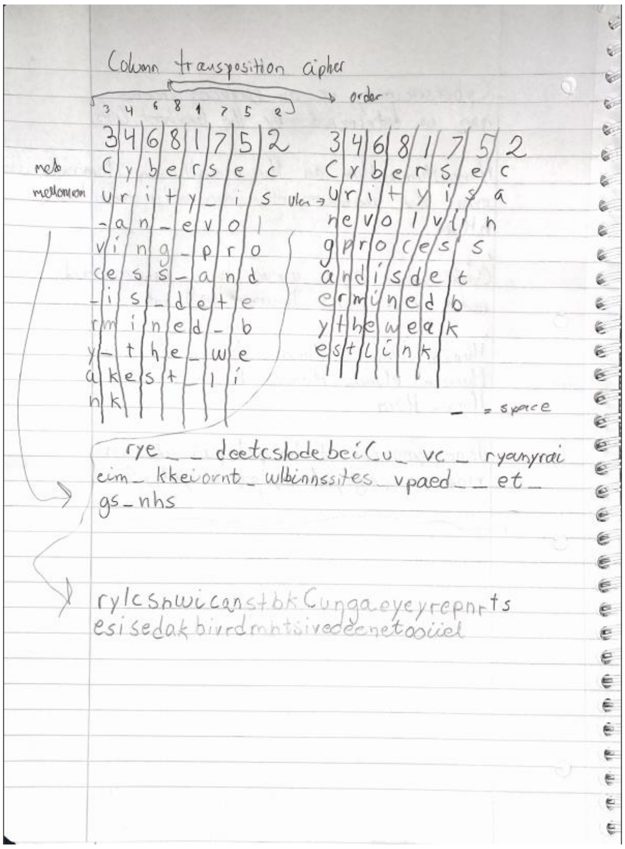
Using the Vigenère Table and replacing each letter corresponding to the one in the table we get.

“Jsneezyouepnkifhhqvbspuntwlacrzmmnqpmpegllyialxnygoyienryetyphw”

II:

The order of numbers being 34681752 and the sentence we want to encrypt. We get:

“rylcsnwicanstbkCungaeyeyrepnrtsesisedakbivrdmhtsivedeenetooiiel”



Column transposition cipher

3 4 6 8 1 7 5 2 → order

meb

mellomrom

3	4	6	8	1	7	5	2
C	y	b	e	r	s	e	c
u	r	i	t	y	_	i	s
_	a	n	_	e	v	o	l
v	i	n	g	_	p	r	o
c	e	s	s	_	a	n	d
_	i	s	_	d	e	t	e
r	m	i	n	e	d	_	b
y	_	t	h	e	_	w	e
a	k	e	s	t	_	l	i
n	k						

Uten →

3	4	6	8	1	7	5	2
C	y	b	e	r	s	e	c
u	r	i	t	y	i	s	a
n	e	v	o	l	v	i	n
g	p	r	o	c	e	s	s
a	n	d	i	s	d	e	t
e	r	m	i	n	e	d	b
y	t	h	e	w	e	a	k
e	s	t	l	i	n	k	

_ = space

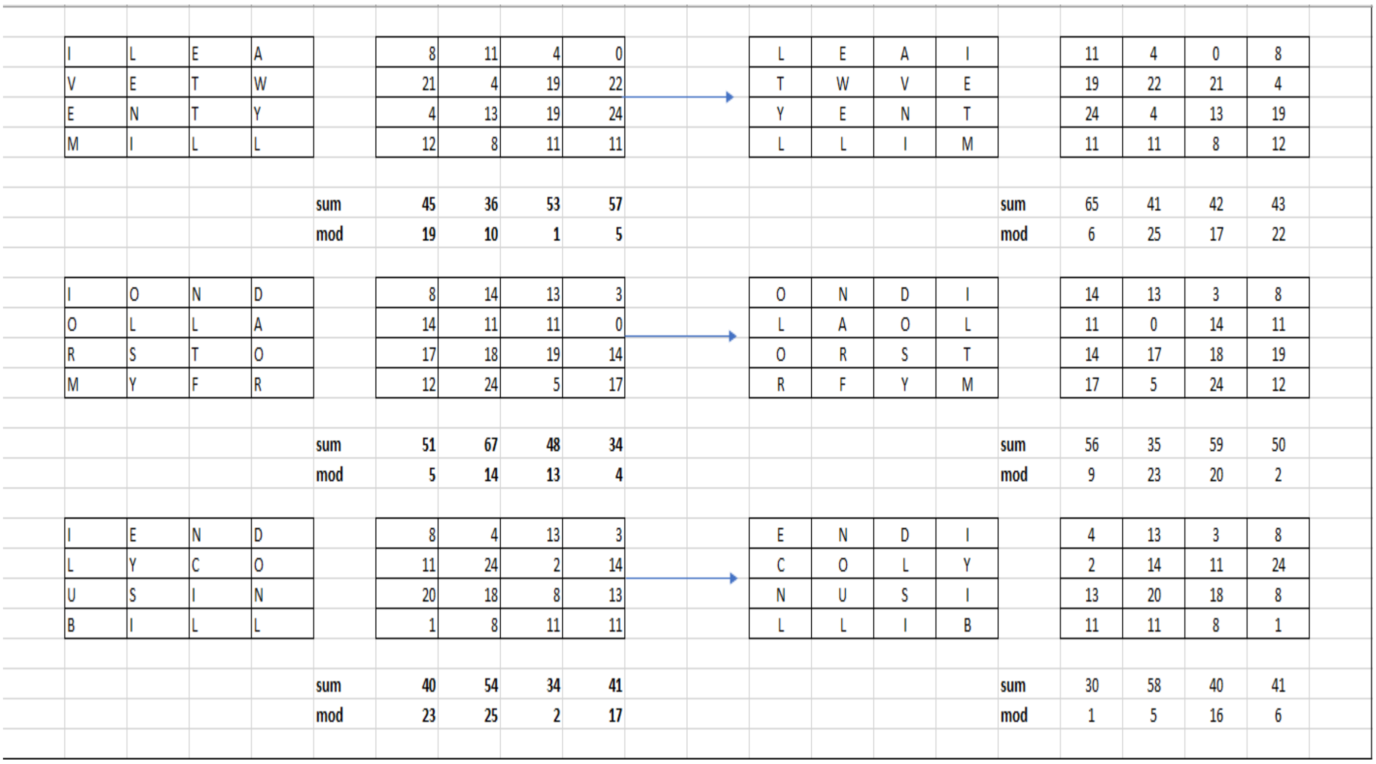
rye _ _ deetcslodebeiCu_ vc _ ryanyrai
eim_ kkeiornt_ wlbinnssites_ vpaed_ _ et_
gs_nhs

rylcsnwicanstbkCungaeyeyrepnrts
esisedakbivrdmhtsivedeenetooiiel

Question 4:

4.1 ?

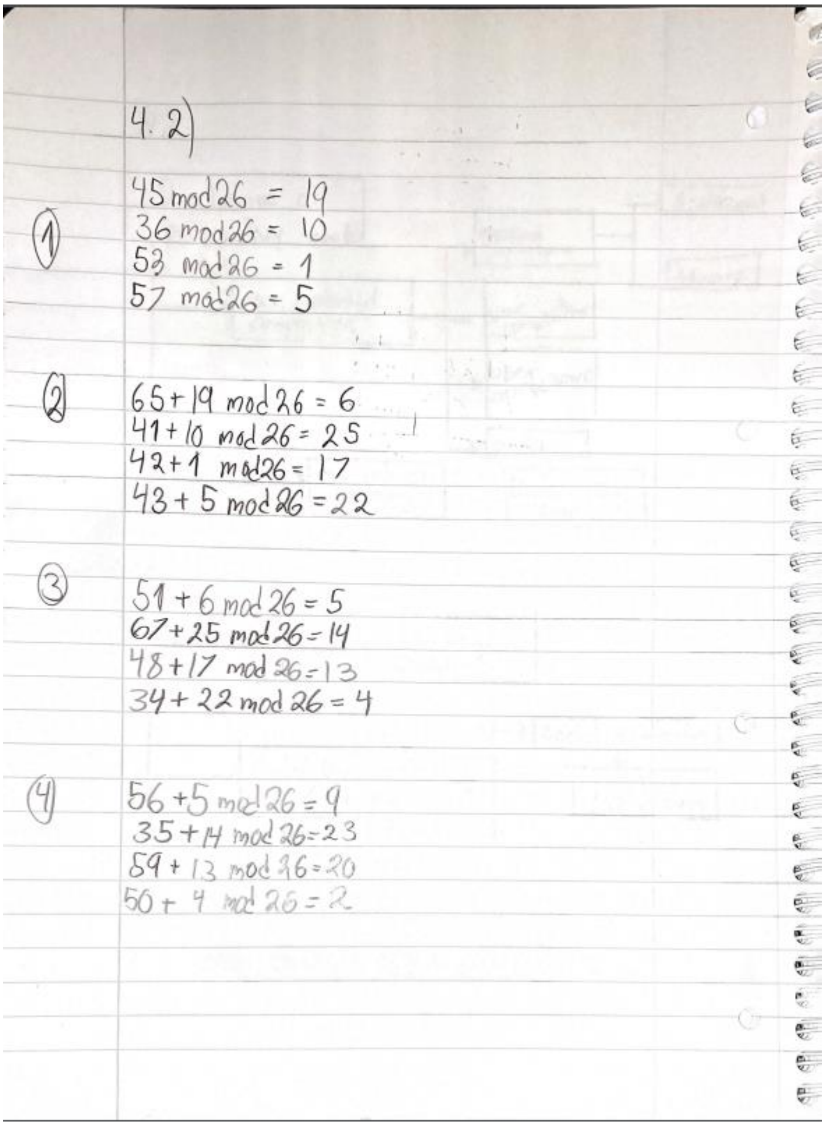
4.2



I	L	E	A		8	11	4	0		L	E	A	I		11	4	0	8
V	E	T	W		21	4	19	22	→	T	W	V	E		19	22	21	4
E	N	T	Y		4	13	19	24		Y	E	N	T		24	4	13	19
M	I	L	L		12	8	11	11		L	L	I	M		11	11	8	12
				sum	45	36	53	57						sum	65	41	42	43
				mod	19	10	1	5						mod	6	25	17	22

I	O	N	D		8	14	13	3		O	N	D	I		14	13	3	8
O	L	L	A		14	11	11	0	→	L	A	O	L		11	0	14	11
R	S	T	O		17	18	19	14		O	R	S	T		14	17	18	19
M	Y	F	R		12	24	5	17		R	F	Y	M		17	5	24	12
				sum	51	67	48	34						sum	56	35	59	50
				mod	5	14	13	4						mod	9	23	20	2

I	E	N	D		8	4	13	3		E	N	D	I		4	13	3	8
L	Y	C	O		11	24	2	14		C	O	L	Y		2	14	11	24
U	S	I	N		20	18	8	13	→	N	U	S	I		13	20	18	8
B	I	L	L		1	8	11	11		L	L	I	B		11	11	8	1
				sum	40	54	34	41						sum	30	58	40	41
				mod	23	25	2	17						mod	1	5	16	6



4.2)

① 45 mod 26 = 19

36 mod 26 = 10

53 mod 26 = 1

57 mod 26 = 5

② 65 + 19 mod 26 = 6

41 + 10 mod 26 = 25

42 + 1 mod 26 = 17

43 + 5 mod 26 = 22

③ 51 + 6 mod 26 = 5

67 + 25 mod 26 = 14

48 + 17 mod 26 = 13

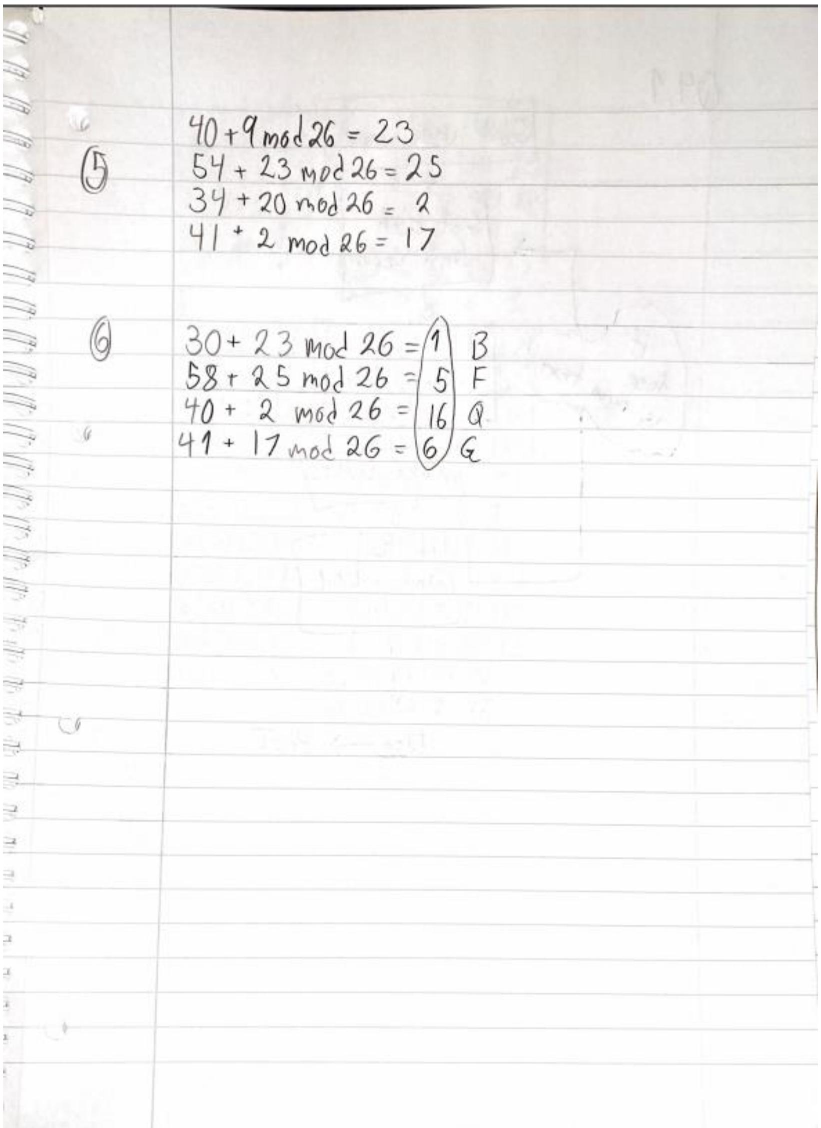
34 + 22 mod 26 = 4

④ 56 + 5 mod 26 = 9

35 + 14 mod 26 = 23

59 + 13 mod 26 = 20

50 + 4 mod 26 = 2



40+9 mod 26 = 23

5 54 + 23 mod 26 = 25

34 + 20 mod 26 = 2

41 + 2 mod 26 = 17

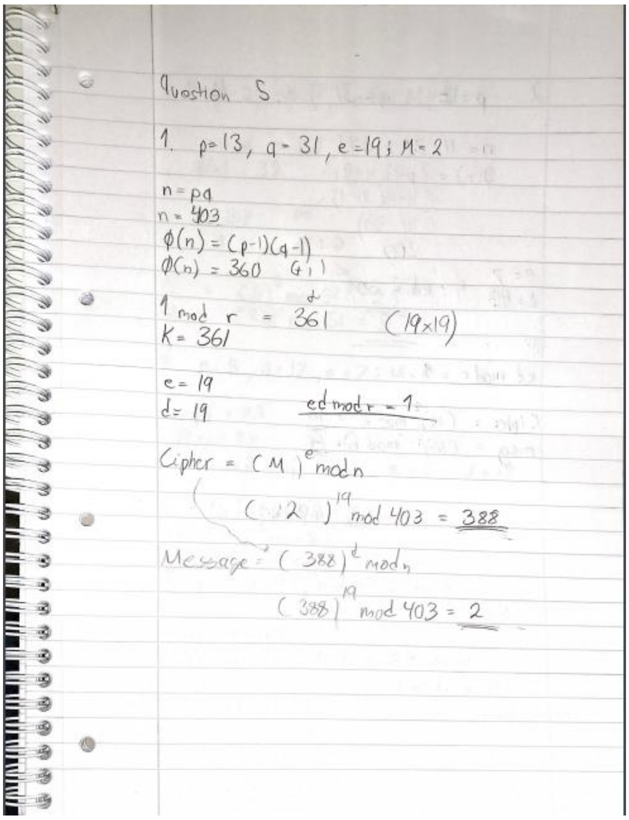
6 30 + 23 mod 26 = 1 B

58 + 25 mod 26 = 5 F

40 + 2 mod 26 = 16 Q

41 + 17 mod 26 = 6 G

Question 5: (1)



Question 5

1. $p=13$, $q=31$, $e=19$; $M=2$

$n=pq$
$n=403$
$\phi(n)=(p-1)(q-1)$
$\phi(n)=360$ G, 1

$1 \bmod r = \overset{d}{361}$ (19×19)
$K=361$

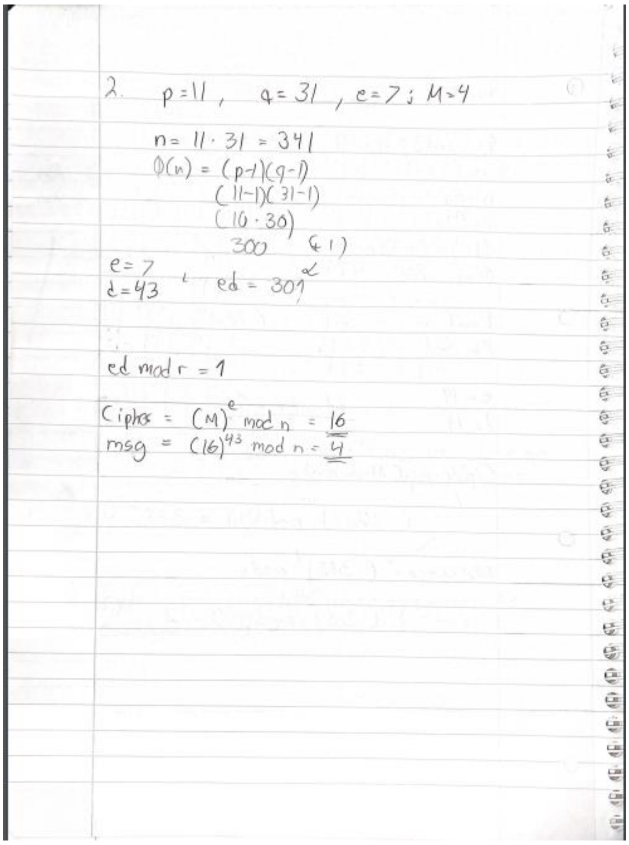
$e=19$
$d=19$ $\underline{ed \bmod r = 1}$

Cipher $= (M)^{e} \bmod n$

$(2)^{19} \bmod 403 = \underline{\underline{388}}$

Message $= (388)^{d} \bmod n$

$(388)^{19} \bmod 403 = \underline{\underline{2}}$



2. $p = 11, \quad q = 31, \quad e = 7; M = 4$

$n = 11 \cdot 31 = 341$

$\phi(n) = (p-1)(q-1)$

$(11-1)(31-1)$

$(10 \cdot 30)$

$300 \quad (+1)$

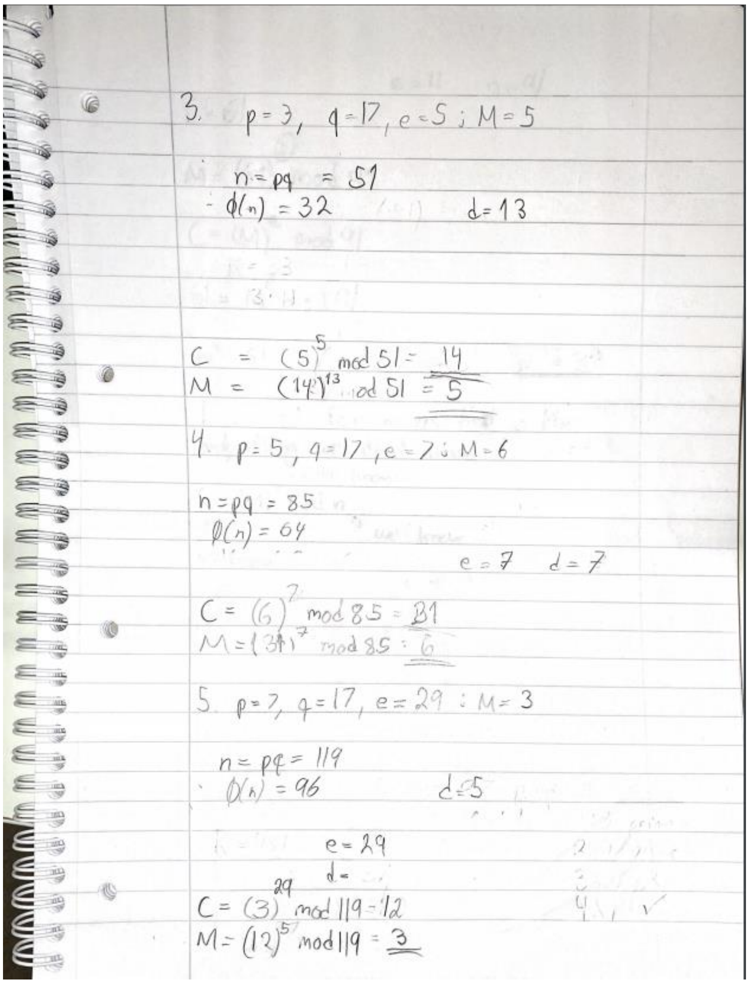
$e = 7$

$d = 43 \quad ed = 301$

$ed \bmod r = 1$

$\text{Cipher} = (M)^e \bmod n = \underline{\underline{16}}$

$\text{msg} = (16)^{43} \bmod n = \underline{\underline{4}}$



3. $p = 3, \; q = 17, e = 5; M = 5$

$n = pq = 51$

$\phi(n) = 32 \qquad d = 13$

$C = (5)^5 \bmod 51 = \underline{\underline{14}}$

$M = (14)^{13} \bmod 51 = \underline{\underline{5}}$

4. $p = 5, q = 17, e = 7; M = 6$

$n = pq = 85$

$\phi(n) = 64$

$e = 7 \quad d = 7$

$C = (6)^7 \bmod 85 = \underline{31}$

$M = (31)^7 \bmod 85 = \underline{\underline{6}}$

5. $p = 7, q = 17, e = 29; M = 3$

$n = pq = 119$

$\phi(n) = 96 \qquad d = 5$

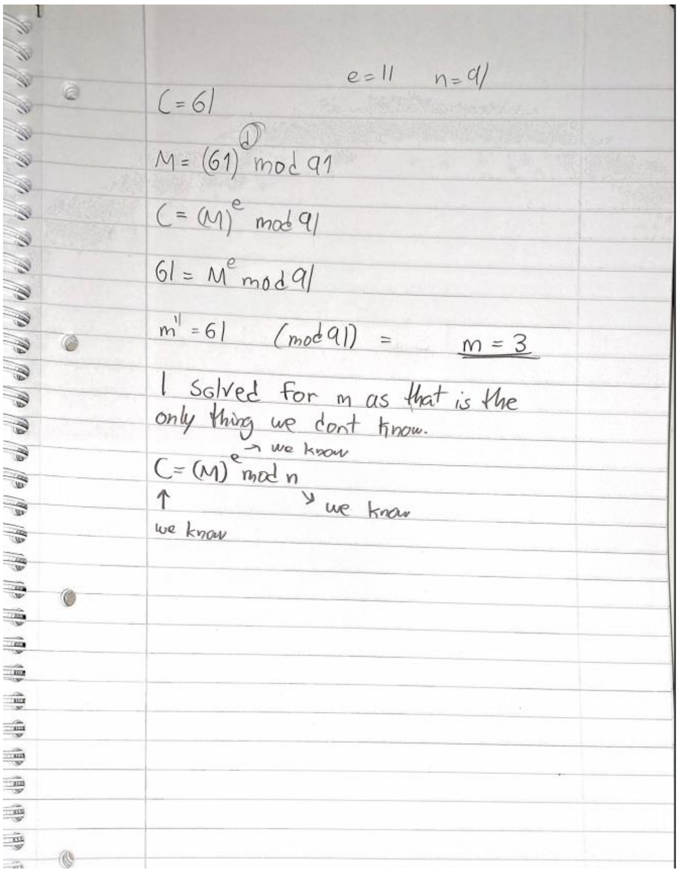
$e = 29$

$d =$

$C = (3)^{29} \bmod 119 = 12$

$M = (12)^5 \bmod 119 = \underline{\underline{3}}$

(2)



$e=11 \quad n=91$

$C=61$

$M=(61)^{\textcircled{d}} \bmod 91$

$C=(M)^{e} \bmod 91$

$61=M^{e} \bmod 91$

$m^{11}=61 \pmod{91} = \underline{\underline{m=3}}$

I solved for m as that is the only thing we dont know.

→ we know

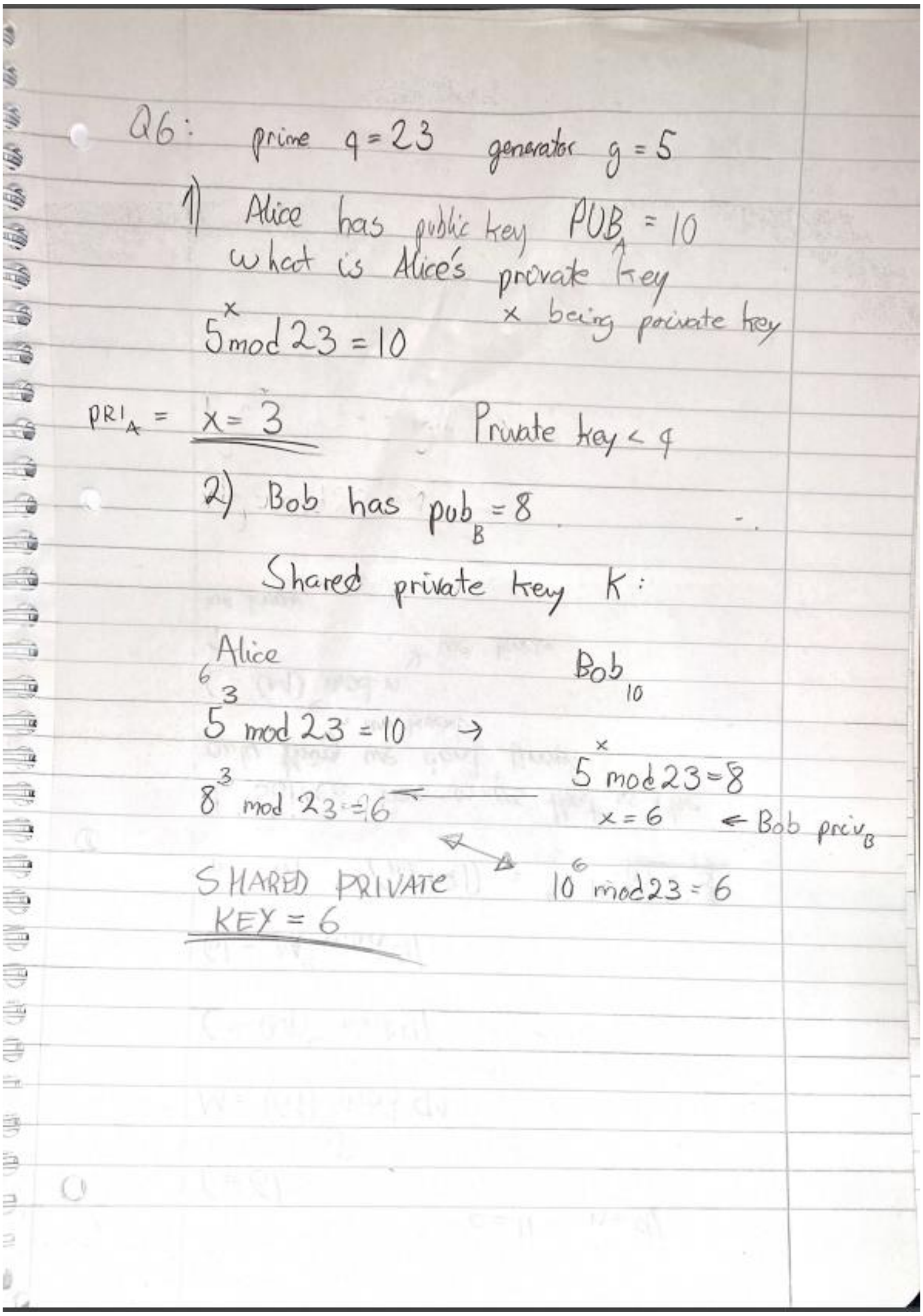
$C=(M)^{e} \bmod n$

↑ ↘ we know

we know

M = 3

Question 6:



Q6: prime $q = 23$ generator $g = 5$

1) Alice has public key $PUB_A = 10$
what is Alice's private key

$5^x \bmod 23 = 10$ x being private key

$PRI_A =$ $\underline{x = 3}$ Private key < q

2) Bob has $pub_B = 8$

Shared private key K:

Alice $_6$ Bob $_{10}$

$5^3 \bmod 23 = 10$ →

$5^x \bmod 23 = 8$

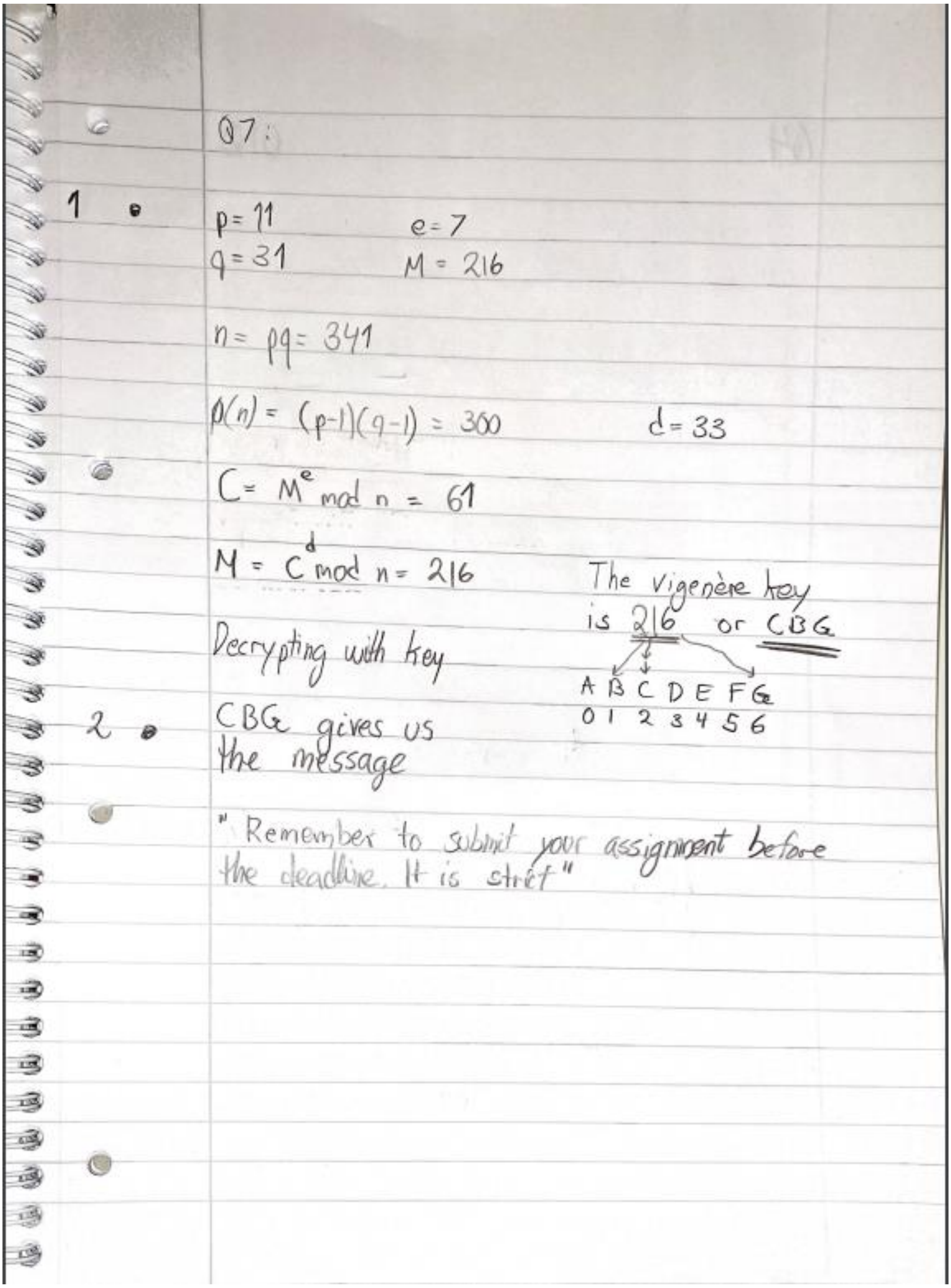
$8^3 \bmod 23 = 6$ ←

$x = 6$ ← Bob $priv_B$

$10^6 \bmod 23 = 6$

SHARED PRIVATE KEY = 6

Question 7:



Q7:

1 • $p = 11$ $e = 7$

$q = 31$ $M = 216$

$n = pq = 341$

$\phi(n) = (p-1)(q-1) = 300$ $d = 33$

$C = M^e \bmod n = 61$

$M = C^d \bmod n = 216$

The vigenère key is 216 or CBG

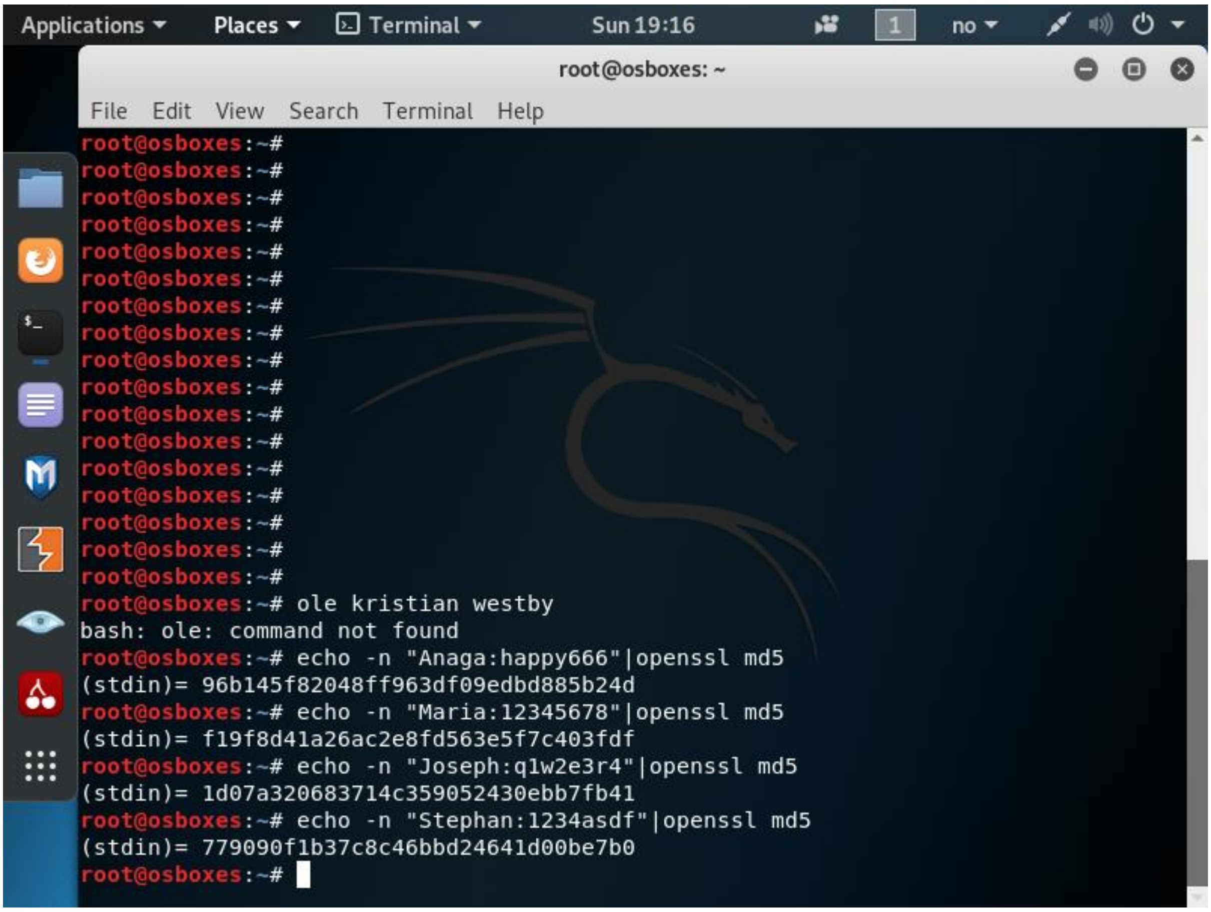
A	B	C	D	E	F	G
0	1	2	3	4	5	6

Decrypting with key CBG gives us the message

2 • "Remember to submit your assignment before the deadline. It is strict"

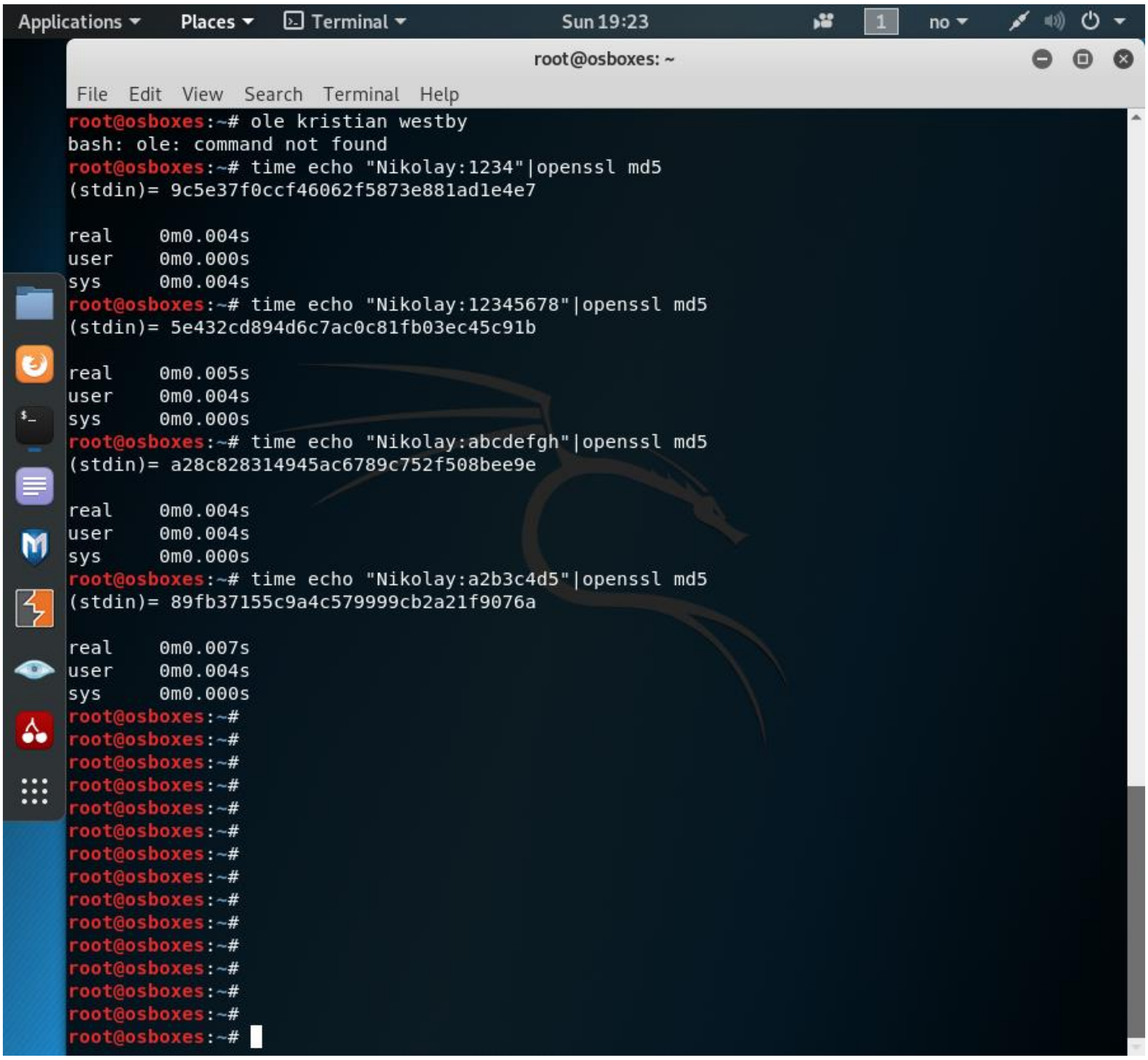
Question 8:

(1)



```
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~# ole kristian westby
bash: ole: command not found
root@osboxes:~# echo -n "Anaga:happy666"|openssl md5
(stdin)= 96b145f82048ff963df09edbd885b24d
root@osboxes:~# echo -n "Maria:12345678"|openssl md5
(stdin)= f19f8d41a26ac2e8fd563e5f7c403fdf
root@osboxes:~# echo -n "Joseph:q1w2e3r4"|openssl md5
(stdin)= 1d07a320683714c359052430ebb7fb41
root@osboxes:~# echo -n "Stephan:1234asdf"|openssl md5
(stdin)= 779090f1b37c8c46bbd24641d00be7b0
root@osboxes:~#
```

(2)



```
root@osboxes:~# ole kristian westby
bash: ole: command not found
root@osboxes:~# time echo "Nikolay:1234"|openssl md5
(stdin)= 9c5e37f0ccf46062f5873e881ad1e4e7

real	0m0.004s
user	0m0.000s
sys	0m0.004s
root@osboxes:~# time echo "Nikolay:12345678"|openssl md5
(stdin)= 5e432cd894d6c7ac0c81fb03ec45c91b

real	0m0.005s
user	0m0.004s
sys	0m0.000s
root@osboxes:~# time echo "Nikolay:abcdefgh"|openssl md5
(stdin)= a28c828314945ac6789c752f508bee9e

real	0m0.004s
user	0m0.004s
sys	0m0.000s
root@osboxes:~# time echo "Nikolay:a2b3c4d5"|openssl md5
(stdin)= 89fb37155c9a4c579999cb2a21f9076a

real	0m0.007s
user	0m0.004s
sys	0m0.000s
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~#
root@osboxes:~# 
```

a) Four digits would take 10^4*0,004 = 40s.

b) Eight digits would take 10^8*0,005 = 5,787 days.

c) Eight letters would take 26^8*0,004 = 26,487 years.

d) Eight digits and letters would take 36^8*0,007 = 626,19 years.

Question 9:

The salt protects against a systematic attack agains long lists of passwords. If the two users pick a password, then the encryptet password entries for both of them won't be the same.

Question 10:

```
root:$6$Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT
/1OJT4rtBACAm4NlEFV4n4x6ndTN3wD9A5uHOjEQQ/JJqN./:18142:0:99999:7:::
```

root is your login name.

$6$ is SHA-512.

Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT
/1OJT4rtBACAm4NlEFV4n4x6ndTN3wD9A5uHOjEQQ/JJqN is the encrypted password.

:18142: days since Jan 01, 1970 that password was last changed.

:0: is the minimum amount of days before user can change password.

:99999: is the maximum amount of days the password is valid.

The last number, 7 is the number of days before password is to expire that user is warned that his/her password must be changed.