last name **first names** **id#**

CMPUT 210 **quiz 1** **60 min** **closedbook** **42 marks** **page 1**

1. [2] Vigenere cipher, keyword `stew`, encrypt `fleenow` _____

2. [2] Kama Sutra cipher, key `ab cd ef gh ij kl mn op qr st uv wx yz`, encrypt `fleenow` _____

3. [2] scytale cipher, circumference 4, encrypt `fleenow` _____

4. [2] book cipher, key `The vast sun was past its zenith, hot like an xray. Giant pandas raced back and forth. A mangy cat jumped on the kid, until then quietly eying the dozing newt. He yelped.` encrypt `fleenow`

   _____

5. [4] Playfair cipher, keyword `charlay`, show the encryption Polybius grid

   and then encrypt `crystalp`

   _____

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

6. [2] ADFGVX ciphertext after first stage of encryption: `DV DD DD DV FG FD DV DD AV XG AD GX`.

   The keyword is WETS. Give the ciphertext. _____

   Show your work.

7. [7] This is frequency data from a long ciphertext, rounded to the nearest percent:

.	..	...	....	...-	..-	..-.	.-	-.	-..	--	--.	---
13	7	6	6	1	3	2	8	6	4	2	2	0

-	-.	-..	-...	-..-	-.-	-.-.	-.--	--	--.	--..	--.-	---
9	7	4	1	0	1	3	2	2	2	0	0	8

This is the start of the ciphertext: crack it.

ROUGH WORK

.... -- . - .... --- -.. .-- --- .-. -.- ... .-- . .-.. .-..

.-- .. - .... .-.. --- -. --. -- . ...- --. . ...

FINAL ANSWER

.... -- . - .... --- -.. .-- --- .-. -.- ... .-- . .-.. .-..

.-- .. - .... .-.. --- -. --. -- . ...- --. . ...

8. [7] To find Vigenere ciphertext keylength, the Babbage/Kasiski method finds repeated _____ offsets, eg. 19 35 28 24 42 63.For this example the most likely keylength is _____ and the number of false positives is _____. By contrast, the Friedman method, for each guess of the keylength, computes the _____ of each of the resulting _____: if each has a value close to _____ the guess is probably correct, otherwise each value should be closer to _____.

9. [5] _____, the author of our text, starts his story in **(circle one)** 1486 1586 1686 1786 1826 with the trial of _____ (A), whose cryptosystem was an enhanced _____ substitution cipher. Unfortunately _____'s secretary _____ (B) had read widely on cryptography, and employed _____ (C) as a code cracker and Gifford to smuggle letters between (A) and the conspirator _____ (D). (A) was tricked into revealing the co-conspirators: (B) had (C) forge an encrypted _____ to a letter from (D) to (A) that asked for their names.

10. [5] Father and son _____ (AA) became cryptographers for the king of _____ (B). In **(circle one)** 1526 1626 1726 1826 1896 the father cracked a message revealing that an army trapped inside a city was _____. (AA) designed a special cipher for (B) that was not cracked until **(circle one)** 1526 1626 1726 1826 1896. This cipher had about **(circle one)** 50 150 300 450 600_____ characters: it was first thought to be a _____ cipher, but was a _____ cipher. After the cipher was cracked, secret correspondence of (B) suggested an identity of _____.

11. [4] The _____ (A) affair convinced America to enter WWI. In the year _____ a _____ German u-boat sank the passenger ship Lusitania, with about _____ people on board. A telegram from (A) to the country of _____ (B) suggested that (B) join the war against America. The country of _____ cracked the telegram: after giving the decryption to the Americans, they managed to keep secret the fact that _____.