cmput 210 final exam

2016 april 21 1400 – 1700

cipher disc and/or vigenere square allowed

no other materials or devices allowed

your last name: ______________________________

your first names: ______________________________

your student id: ______________________________

do *not* detach any page from the staple

put your name and id on each page

if we cannot read your writing, you will not get full marks

on this page, do not write below this line

---

total marks	page	your marks
10	1	
10	2	
10	3	
10	4	
40		

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

1. Around the year ______________, in the city of __________________, __________________ wrote about how to crack monoalphabetic subsitution ciphers (MSCs). Cracking a Kama Sutra cipher is ______________ than cracking a general MSC, because ______________________________________

   ____

   ____

   Crack this Kama Sutra ciphertext. The letters `t y e x p g k o w c f l d i a b s u h j m`

   have respective frequencies `13 10 9 9 6 5 5 5 5 4 4 4 3 3 2 2 2 2 1 1 1`.

```
k w g s t  a y m t f  y x s t  e y w u  b t  e p k e

e p t  y x w o  l k o  e y  a x y l  l p t x  o y d

p k j t  u y x t  c y b t e p g x i  e f d w o

i f t k e  g c  l p t x  o y d f  c h g x t  e g x i w t c
```

2. Give two ways in which the cipher of Mary Queen of Scots was stronger than MSC.

   ____

   ____

   ____________________ was the principal secretary of Queen Elizabeth. He hired Phelippes as his

   __________________, and used Gifford to ____________________________________.

   Mary, Queen of Scots, was executed in the year ______________ because ______________________

   ____

   ____

   ____

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

3. (i) Define evolution. ____

____

(ii) List these ciphers in the order they evolved: Enigma, Lucifer, MS (monoalph. sub.).

For each cipher, briefly (20 words each) describe the cryptoanalytic method that evolved to crack it.

(1)______________ ______________________________________

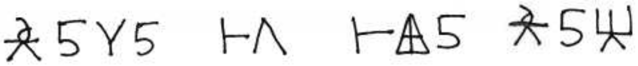
____

(2)______________ ______________________________________

____

(3)______________ ______________________________________

____

4. (i)__________________ guessed that the language (ii)______________ had noun declensions. For example, (i) organized the 4 words  in a table like this:

The number of (ii) language symbols is around _________, so each symbol probably represented __________________, namely a __________________ followed by a __________________.

(i) guessed that words in the first row are the same ______________ and so share the same _____-letter ______________, so symbols ______________ (also symbols ______________) share __________________.

(i) guessed that words in the first column are the same ____________ and so share the same _____-letter ______________, so symbols ______________ (also symbols ______________) share __________________.

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

5. Alice and Bob use a quantum crypto scheme: for filters, 0 means +, 1 means x; for +-spins, 0 means `-`, 1 means `|`; for x-spins, 0 means `\`, 1 means `/`. Alice picks string 1101 1110 for filter selection, so her filter sequence is ____________________. Alice picks string 0010 1110 for message selection, so the spin sequence she sends Bob is ____________________. Bob picks string 1000 0100 for filter selection, so to read Alice's spin sequence he uses filter sequence ____________________. So he sees spin sequence ____________________, where `?` means we do not know what Bob sees. Lastly,

   ____

   ____

   Assuming Eve did not interfere, Alice and Bob have created the secret key ______________________.

6. The NSA argued that the Data Encryption Standard should be limited to a size of _______________. Presumably, they wanted this limit because ____

   ____

   The 1-time pad is secure in this sense: if you assume that ____________________________________

   ____, then

   ____

7. Explain the role of Amnisos in cracking Linear B.

   ____

   ____

   ____

8. In Britain, a group led by _______________ helped the Brits crack _______________. His method starts with a crib, then uses a special purpose machine that finds the ____________________________________ but not the ____. This was useful, because the number

   ____

   ____

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

9. Alice wants to use public-key cryptography. She finds large primes p, q, and sets n to be ______________. Next, she picks a number e and finds a number d that satisfies this property: ____________________. Then she publishes n and e. To send Alice a message, Bob converts the message to a number m, computes $x =$______________, and sends x to Alice. To recover m, Alices computes $z =$____________________. It turns out that $z = m$, because ____

____

____

10. Encrypt plaintext `retreatnow` using the ADFGV cipher with keyword `spat` and grid below. Omit the last encryption step, which converts from letters to ______________ symbols.

```
p o l y b         your work:
i u s g r
d a n c e
t m f k q         your answer:
w z h v x
```

11. Encrypt `attackatdawn` using the Vigenere cipher with keyword `python`.

```
plaintext       a t t a c k a t d a w n
ciphertext
```

The Vigenere cipher can be cracked by first finding (i)________________________. E.g., the method of Babbage and Kasiski is to ____

____

while the method of Friedman is to ____

____

Next, the ciphertext can be broken into (i) substrings. Each substring is enciphered with ______________

________________________, so each substring can be independently deciphered easily in this way:

____

____