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

CMPUT 210 **quiz 2** **60 min** **closedbook** **42 marks** **page 1**

1. [5] The Enigma used by the German army at the start of World War II has ______________ rotor slots, ______________ rotors, and ______________ plugboard cables. It uses a keyboard for input and a ______________ for output. After rotors have been put in their slots, there are about **(circle one)** 18000 1800000 18000000 180000000 different initial rotor settings.

2. [4] Compute the Rejewski 2-5 fingerprint for this set of data. Show your work.

```
ABOLBG BTLKFZ CYJXNU DHWRAQ EKZUQF FPYOLD GZNFZJ HSGZUV IDUAWR
JWEWSH KNACPY LCSNVM MIDSTB NUKVRK OFMIKN PRBHDE QLHJMT ROPGEP
SVXTOC TMCMYX UETBGO VAQDIW WGFQJS XQIPHL YJVEXA ZXRYCI
```

3. [2] Is the Enigma crib/ciphertext alignment **below left** acceptable? Explain in at most 20 words.

____

____

```
     WETTERVORHERSAGEBONN              WETTERVORHERSAGEBONN
KTWLAXIOOHNXPQHCBESXYEWOLP          KTWLAXIOOHNXPQHCBESXYEWOLP
```

[3] For the alignment **above right**, on the letters below, draw the Turing diagram.

```
I  B  A  E  G  L  S  Q

T  X  R  O  N  W  C

   P  H  V  Y
```

4. [5] The first version of the __________ code-talker system had two flaws. One flaw was that words not in this language or the lexicon had to be spelled out. A second flaw was (20 words)

____

____

The second flaw was fixed by (at most 20 words)

____

____

5. [5] __________, the language that descended from Old Egyptian, was the main language of Egypt until around the year __________, when it was replaced by the language __________.

How did Athanasius Kircher delay the cracking of the hieroglyphs? Explain (20 words).

____

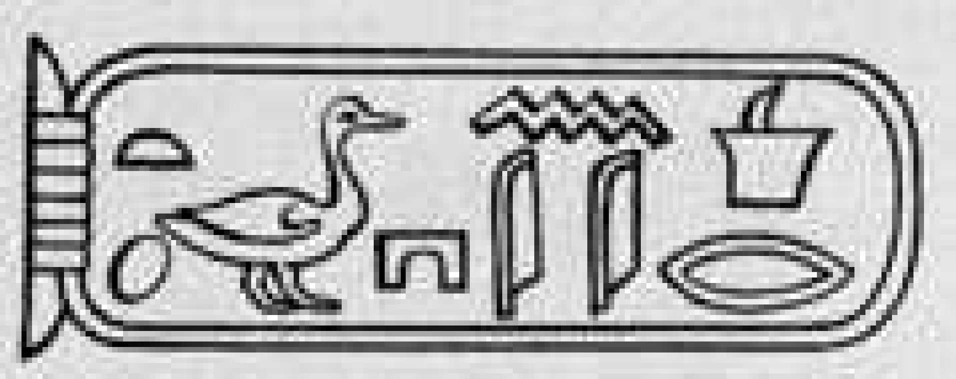
____

6. [4] For this cartouche, for these symbols, give the meaning or sound. (duck symbol is *a* sound.)

loaf and oval together __________ stool __________ ripples __________

two reeds __________ pot with plant __________ mouth __________

This is the cartouche for ____________________.



7. [7]

word x	word y
35-63-04-72	61-37-72
35-63-04-19	61-37-19
35-63-25	61-41

__________________ helped crack __________________. For the words above, she guessed symbol __________ and symbol __________ share the same __________,
and symbol __________ and symbol __________ share the same __________,
and symbol __________ and symbol __________ share the same __________,
and symbol __________ and symbol __________ share the same __________.

__________ extended her work. He guessed that a certain symbol, say 49, that occurred frequently as the start of a word was a __________. He guessed that certain words that occurred frequently must be __________________. In the end, he guessed that a certain four-symbol word starting with 49 must be the word for __________________.

8. [7] The DHM protocol was invented in American around the year __________ and in Britain around the year __________ to solve the problem of __________________.

i) Alice and Bob use DHM. They communicate by internet email. What steps do they take to make sure that Eve cannot intercept their communication? (20 words)

____

____

ii) Alice and Bob use prime number p and base g. Alice picks a random number a and computes the number given by this mathematical expression: __________. She calls this number α and sends it to Bob. Bob picks a random number b and computes the number given by this mathematical expression: __________. He calls this number β and sends it to Alice.

iii) Finally, Alice computes the number given by this mathematical expression __________. (Bob does something similar).