Tutorial 1: Classical Cryptography

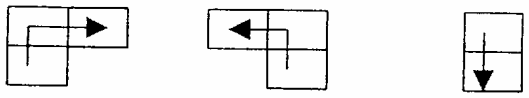
1. Do an internet search on the following terms, read up on them and provide a short paragraph describing each:
   - Monoalphabetic ciphers
   - Cryptographical Rotor Machine
   - Steganography

2. What is the difference between encoding and encryption?

3. Decrypt the following encrypted quotations:
   - `fqjcb rwjwj vnjax bnkhj whxcq nawjv nfxdu mbvnu ujbbf nnc`
   - `oczmz vmzor jocdi bnojv dhvod igdaz admno ojbzo`
     `rcvot jprvi oviyv aozmo cvooj ziejt dojig toczr`
     `dnzno jahvi fdiyv xcdzq zoczn zxjiy`

4. In the translation table shown below, each plaintext character is enciphered by moving a certain number of blocks in the vertical and then the horizontal direction to determine the ciphertext character. The number of positions moved changes from character to character in order to hide patterns. These moves can be represented graphically – an example of a repeating pattern of 3 move sequences (which can be thought of as a rudimentary key) is shown below the block. Notice that there is no plaintext for `Z', in order to make the plaintext alphabet fit into the square grid. Z's in the plaintext are either replaces by `S' or encoded as `YY'. Spaces are not coded – they are removed from the plaintext before encipherment.

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



An example encryption using this cipher is (spaces shown for clarity)

```
SHE SELLS SEA SHELLS
obj oxqhm xuy xdxqhm
```

i. Is this cipher equivalent to (possibly a combination) of ciphers you have learnt about? If so, determine and state the precise details of this equivalence.

ii. What kind of ciphertext-only attack would you use on this cipher?

5. Is the transposition cipher a block or a stream cipher? Explain. Repeat for substitution ciphers.

6. Do an internet search on the following terms and read up on them:
   - Confusion and Diffusion (in the cryptographic sense)
   - Digrams and Trigrams
   - Letter frequency distributions and the index of coincidence
   - Double transposition algorithms
   - Generalised Transposition Ciphers

7. Using the Vigenere table, encrypt the following message using the keyword INFO. You can ignore punctuation and spaces.

   `HE'S FALLEN IN THE WATER`

8. How many (monoalphabetic substitution) alphabets would every possible permutation of the English alphabet give?

9. Suppose a Kasiski analysis identifies the following pairs of repeated sequences. What can you conclude about the number of alphabets used to encrypt this message? Explain your answer.

Location of 1st occurrence	Location of 2nd occurrence
10	34
21	62
37	109
49	105
58	162
72	132

10. Demonstrate using the formula for the Index of Coincidence, that for a perfectly flat frequency distribution, IC = 0.0384

11. In a particular language, there are 12 letters. Two of these are used with relative frequency 3, four are used with relative frequency 2 and the remaining six are used with relative frequency of 1. Compute the index of coincidence for monoalphabetic substitutions in this language. *[ans = 0.10651]*

12. Verify (or disprove) each of the following conjectures:
    - For successive monoalphabetic encipherments E_2 and E_1,
      $C = E_2(E_1(P)) = E_1(E_2(P))$
      i. If the alphabets are rotations of each other. That is, the order of encipherments is not important. Further, $E_2(E_1(P)) = E_3(P)$
      ii. Two or more successive monoalphabetic encipherments are equivalent to a single monoalphabetic encipherment.

    - For the more general case where the alphabets are arbitrary permutations of the English language: (i) above is not true, but (b) is.

- Hint: There are two ways of doing this:
  i. The more mathematical among you can prove this analytically. To do this you will need to use modular arithmetic with the following properties:
     1. *(a+b) mod n = a mod n + b mod n*
     2. *(a mod n) mod n = a mod n*
  ii. Those who have given up on mathematics can prove this by example.

13. *Suppose a plaintext of length 84 characters is enciphered with a columnar transposition of table width 7. The same ciphertext is then applied to the resulting ciphertext again, and again, etc. Would the plaintext re-appear after a certain number of encipherments? If so how many? (You should be able to answer this using some simple MATLAB code)

14. Find out how one could hide, say a copyright notice inside a picture so that it cannot be detected (and removed)?

15. Read up more on the one-time pad. Find out what cryptanalytic technique is used to break ciphertext, which has been generated by using the one time pad twice.

16. The permutation function below is used by Rufus to generate tables for a monoalphabetic substitution cipher. The value of **a** (ranging from 0 to 25) represents one of the 26 letters of the alphabet and different values of the key **k** give different translation tables. Using your knowledge of the rules of modular arithmetic from *Question 12*, determine the keyspace of this cipher.
    $P_1(a) = (k*a + 7) \bmod 26$ *[Exam 2002; 5 marks]*

17. Explain why it is considered important for the security of a cipher to reside in the key and not in the algorithm. Explain also the difference between classic and modern ciphers. *[Exam 2001; 4 marks]*