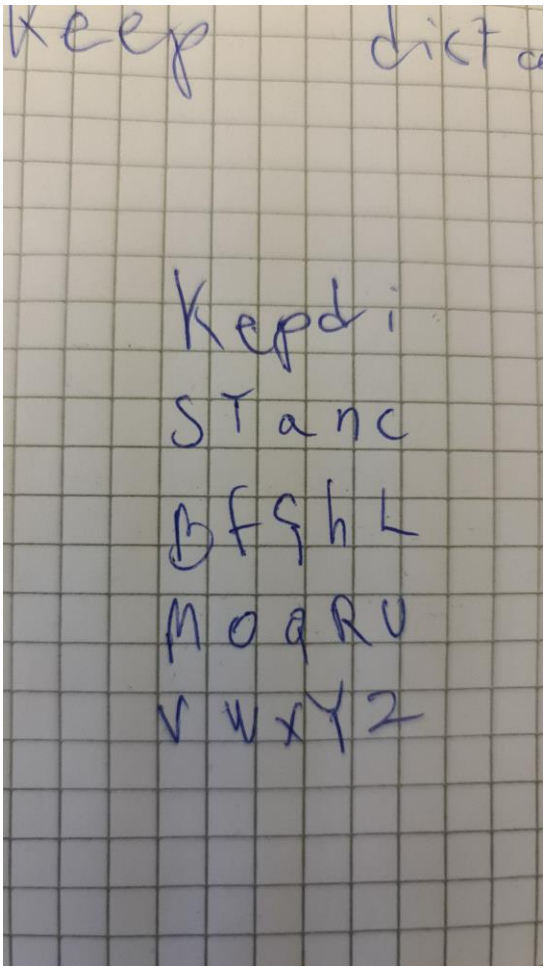
INF143A Assignment 1

Sigmund Volden

Problem 1:

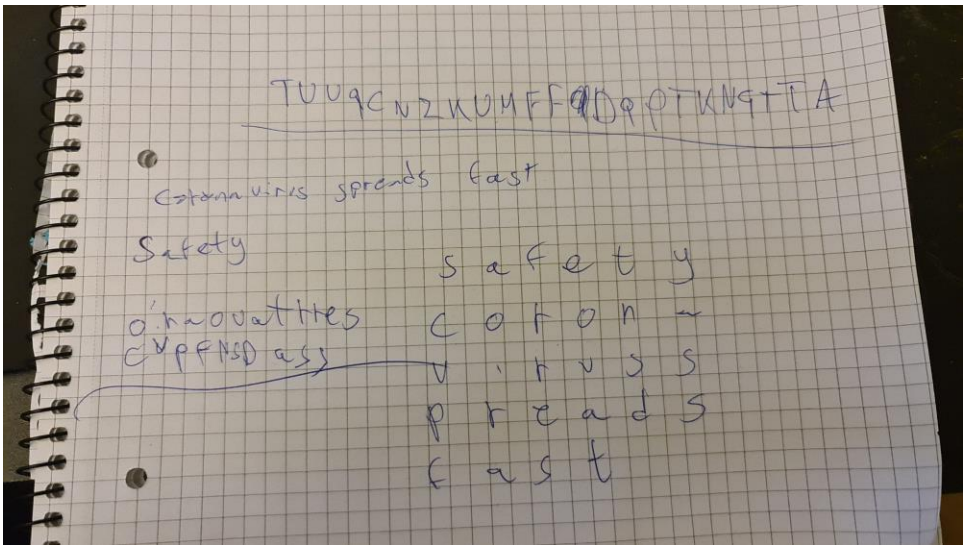
(I):

TUUQCNZKUMFFDQPTKNGTTA



(ii):

OINAOUATTRESCVPFNSDASS



Problem 2:

I)

Initial state 0011: [0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1]

Initial state 0111: [0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1]

Ii)

I included the script for this as I did the last part in the last minute (the groups).

The sequences are:

Initial sequence: 0000, sequence: [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Initial sequence: 0001, sequence: [0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0]

Initial sequence: 0010, sequence: [0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1]

Initial sequence: 0011, sequence: [0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0]

Initial sequence: 0100, sequence: [0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0]

Initial sequence: 0101, sequence: [0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]

Initial sequence: 0110, sequence: [0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0]

Initial sequence: 0111, sequence: [0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0]

Initial sequence: 1000, sequence: [1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0]

Initial sequence: 1001, sequence: [1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1]

Initial sequence: 1010, sequence: [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1]

Initial sequence: 1011, sequence: [1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1]

Initial sequence: 1100, sequence: [1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1]

Initial sequence: 1101, sequence: [1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1]

Initial sequence: 1110, sequence: [1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1]

Initial sequence: 1111, sequence: [1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1]

Problem 3:

Script

Problem 4:

(I):

x	y	X'	Y'	dx	dy
0000	1110	1011	1100	1011	0010
0001	0100	1010	0110	1011	0010
0110	1011	1101	1001	1011	0010
1010	0110	0001	0100	1011	0010
1111	0111	0111	1000	1000	1111

The key for the cipher is 0011, found by using the differential cryptanalysis in the script for the final task, so is the DDS table. I didn't include a visual of the DDS table as I didn't really use it other than for finding the combinations used to find the keys. I did however use a more primitive version of the script to find the key, so instead of permutating it and splitting it into two parts I ran the script straight forward.