

Laboration



Kryptering 1

MA1489

16/12/2022

Oliver Bölin

olbo20@student.bth.se

Förord

I filen laboration.sagews så finns det massvis med fler kommentarer som förklarar hur dessa uppgifter löstes.

Uppgift 1

a

Kryptering:

ADFGVX krypterades till: GXDVXAFVGDDFGXGFGGXXAV

Affint krypterades till: zjedtsymhok

Enigma krypterades till: ZLUKSWBNURH

Hill krypterades till: vqyklånldföu

Playfair krypterades till: ZQIRRZVGTNAL

b

Dekryptering

I. dekrypterades med enigma blir: ENGANSKANORMALMENKORTKLARTEXT

II. dekrypterades med hill blir: elakaspionerknäckerhemligameddelandenx

III. dekrypterades med affint blir: ofrjygtsiqåxfxypåxpfxrjyzmjqlfljs

IV. dekrypterades med adfgvx blir: THESEGOTO11

V. dekrypterades medplayfair blir: DONTTELXLNOBODYTHATX

Uppgift 2

Jag valde vigenere krypto och jag är född den 22a

Perioden fick jag till 6 med Babbage & Kasiski metoden.

Nyckeln fick jag fram till FINGER genom att göra monogramanalys på texten splittrat i 6 deltexter med hjälp av inbyggda funktionerna från kryptering1.

Klartexten fick jag till "pojken som åt ikapp med trollet. Det var en gång en bonde som hade tre söner." (Du kan se vad den printar för hela texten i källfilen.)

Uppgift 3

a

Svaret ser du i funktionen med förklaringar.

Jag använde kompendiet för att bygga funktionen med lite hjälp av pythonkunskaper. Listor är mycket bra att använda när man ska bygga detta kryptosystem. Att skapa följden är definitivt inte en svår uppgift utan man behöver enbart ta reda på hur lång texten som ska krypteras eller dekrypteras först och sedan skapa en följd som är lika lång!

b

Jag fick krypteringen till "i inebgb ha vpastiorale adiokesylic n stcle a rteBlbeenhwcg!"

c

Jag fick dekrypteringen till "Bättre vara ute på hal is och ha det glatt än att gå i lera och sörja."