Krypteringsprogrammet Kryptogamen

Om programmet

Detta program är avsett som en pedagogisk leksak. Det hindrar inte att det kan användas för att försvåra insyn i exempelvis en mailkommunikation mellan privatpersoner.

Den krypteringsmetod som används här kallas ”Caesarkrypto”, efter den romerske kejsaren Julius Caesar. Han och hans armè lär ha använt den här metoden.
På den tiden ansågs detta vara avancerat. För dagens kryptoexperter - med tillgång till moderna kodknäckarverktyg – är den här sortens kryptering närmast att likna vid klartext. För verkligt viktiga saker ska man använda betydligt mer avancerade verktyg, exempelvis ”PGP”.

Programkonstruktör och ägare: Erik Kullberg.
Synpunkter rörande programmet emottages tacksamt per epost.

Bruksanvisning

Programmet manövreras med hjälp av ett antal knappar, vilkas funktion förklaras i det följande. Efter den genomgången följer ett par exempel.

Sök i rullisten tills du hittar den bokstav som du vill att ditt nya alfabet ska börja med. Markera den och tryck på knappen ”**Välj nyckel”** .

Fönstret nedanför rullisten visar alfabetet, dels i ordinarie ordning och dels i förskjutet skick. Det förskjutna alfabetet (som på bilden ovan börjar på den markerade och valda bokstaven ”E”) är det som används för krypteringen.

Det meddelande som ska krypteras, skrivs in i rutan ”**Klartextmeddelande**”. Det går bra med vilka tecken som helst, men det är bara alfabetets bokstäver som bytes vid kryptering. Alla andra tecken (mellanslag, komma, utropstecken osv) går igenom oförändrade.

Knappen ”**=> Kryptera =>**” verkställer kryptering med den givna nyckeln.
Det krypterade meddelandet visas i rutan ”**Krypterat meddelande**”.

Knappen ”**<= Dekryptera <=**” transformerar texten tillbaka till det skick den hade före krypteringen. Detta förutsätter förstås att inställd nyckel är densamma som den som användes vid krypteringen.

Det finns en knapp ”**Rensa**” för vardera textrutan. Den raderar all text i resp. textruta.

Knappen ”**Flytta till ”Krypterat” =>**” flyttar den text som står i rutan ”**Klartextmeddelande**” till rutan ”**Krypterat meddelande**”.

Knappen ” **<= Flytta till ”Klartext”** ” flyttar den text som står i rutan ”**Krypterat meddelande**” till rutan ”**Klartextmeddelande**” .

Exempel 1. <u>Ett</u> nyckeltecken

Agent Knatte ska skicka följande meddelande till agent Fnatte:
”Nyckeln till det blå skåpet ligger i skålen!”
Knatte och Fnatte har kommit överens om att alltid använda kodnyckel ”X”, så Knatte markerar och väljer ”X”.
Han skriver in meddelandet i klartextrutan och trycker på ”**=> Kryptera =>**”.
Det krypterade meddelandet ser ut så här:
”HSZEÄFH NCFF ÅÄN YFU MEUJÄN FCAAÄL C MEUFÄH!”

Knatte klipper ut det och klistrar in det i ett mail, som han skickar till Fnatte.

När Fnatte får mailet, klipper han ut det krypterade meddelandet, startar programmet ”Kryptogamen” och klistrar in meddelandet i rutan för ”**Krypterat meddelande**”.
Han väljer nyckel ”X” som överenskommits.
När han trycker på knappen ”**<= Dekryptera <=**”, får han upp klartextmeddelandet i rutan ”**Klartextmeddelande**” och läser ”Nyckeln till det blå skåpet ligger i skålen!”

Kommentar:
Antag nu att Björnligan får tag i mejlet. Dom gissar att det handlar om ett krypto av Kryptogamen-typ, men vet inte vilken nyckel som ska användas. Dom startar Kryptogamen och klistrar in meddelandet i ”**Krypterat meddelande**”.
Dom väljer nyckel och trycker ”**<= Dekryptera <=**”. *Den proceduren upprepas med ny nyckel tills meddelandet i* ”**Klartextmeddelande**” är begripligt*, vilket sker när dom kommit fram till nyckel=”X”.*
Detta har då krävt <u>högst 28 försök</u> – ganska låg säkerhet, får man nog säga!
Men antagligen tillräckligt besvärligt att knäcka om man inte har tillgång till Kryptogamen.

Exempel 2 <u>Två</u> nyckeltecken

Agent Knatte ska skicka följande meddelande till agent Fnatte:
”Detta är ett prov med två tecken i nyckeln (eller egentligen två nycklar)!”
Han börjar med att skriva in meddelandet i rutan för ”**Klartextmeddelande**”.

Knatte och Fnatte har nu kommit överens om att alltid använda nyckel ”BX”.
Knatte markerar och väljer först ”B” och trycker på ”**=> Kryptera =>**”.
Därefter trycker han på ”**<= Flytta till ”Klartext”**”.
Knatte markerar och väljer nu ”X” och trycker på ”**=> Kryptera =>**”.

Knatte klipper ut meddelandet från ”**Krypterat meddelande**” och klistrar in det i ett mail, som han skickar till Fnatte.

Fnatte klipper ut meddelandet från mailet, startar Kryptogamen och klistrar in meddelandet i ”**Krypterat meddelande**”.
<u>Nycklarna ska tas i omvänd ordning när man dekrypterar</u>, så
Fnatte ställer in och väljer ”X” ,
trycker ”**<= Dekryptera <=**”,
trycker ”**Flytta till ”Krypterat” =>**”
ställer in och väljer ”B” ,
trycker ”**<= Dekryptera <=**”.

Nu framträder meddelandet i läsbart skick.

Kommentar:
Den som vill läsa mailet utan att känna till nyckeltecknen, sätter igång med att gå igenom alla 28 nyckeltecknen. När det visar sig att det inte hjälper, inser man att meddelandet är krypterat med mer än ett nyckeltecken.
Då börjar man med att välja ett visst första nyckeltecken, exempelvis ”A”,
trycker ”**<= Dekryptera <=**”,
trycker ”**Flytta till ”Krypterat” =>**”,
och dekrypterar sedan med alla tecknen i tur och ordning.

*Om detta inte ger träff, så byter man första-tecken och provar sig igenom alla 28 andra-tecknen igen. Antalet kombinationer är 28*28=784, så det kan ta en stund.*

Metoden är helt ofelbar – förr eller senare träffar man rätt! Detta gäller oavsett hur många nyckeltecken som använts – det är bara en fråga om tålamod och tid:
*3 nyckeltecken ger 28*28*28=21952 kombinationer,*
*4 nyckeltecken ger 28*28*28*28=614656 kombinationer,*
osv.
Om man tänker sig att man kan prova tio kombinationer (nycklar) per minut, så tar det ungefär

- *1 timma och 20 minuter att prova sig igenom en kod med 2 nyckeltecken,*
- *37 timmar att prova sig igenom en kod med 3 nyckeltecken,*
- *1024 timmar att prova sig igenom en kod med 4 nyckeltecken!*

Man behöver nog aldrig använda mer än 2 nyckeltecken – Björnligan ger nog upp efter ett par hundra misslyckade försök.

Exempel 3 Kan det bli fel?

Om man krypterar ett meddelande – kan det se ut som en vanlig, begriplig mening ändå? Kanske med en helt annan betydelse än den ursprungliga?

Om meddelandet består av ett enda ord, blir chansen större – vi provar:

Klartext	***Nyckel***	***Krypterat***
I	S	Å
BY	Ö	AX
BY	C	DÅ
HEJ	K	ROT
HUT	E	LYX

Kan du hitta fler ord som blir riktiga ord även i krypterat skick?
Försök med längre ord.
Försök med två ord.

Vi ser att om meddelandet består av två eller flera ord, så är det i praktiken omöjligt att det skulle bli begripligt efter kryptering.

Exempel 4 Försvåra gissningar – undvik andra tecken än bokstäver!

Antag att vi ska skicka ett meddelande som innehåller följande:
”JAS 39 Gripen”.
I krypterat skick (med exempelvis nyckel X) ser det ut så här:
”DXM 39 ALCJÄH”

Om nu Björnligans kryptoexpert får se detta meddelande, kan man gissa att han resonerar såhär:
”Hmm … tre bokstäver, följt av siffrorna 39 … där kanske står JAS 39 … i så fall är ju X = A, vi provar med nyckel = X”.
Därmed har han knäckt koden. Metoden fungerar även med flera nycklar.

Han fick hjälp av siffrorna, som ju går igenom oförvanskade.
Tänk på att det är endast bokstäver som ändras vid krypteringen – alla andra tecken går igenom helt oförvanskade! Man kan alltså försvåra för Björnligan genom att undvika siffror – så här:
”JAS trettionio Gripen”,
vilket, krypterat med nyckel X blir
”DXM NLÄNNCIHCI ALCJÄH”.

Om man dessutom undviker alla andra tecken som inte är bokstäver (exempelvis punkt, komma, utropstecken, frågetecken, bindestreck, parentes, mellanslag …) så har man försvårat tjuvläsandet maximalt:
”DXMNLÄNNCIHCIALCJÄH”
Klartextmeddelandet blir lite mer svårläst för mottagaren om det saknas skiljetecken,
”JASTRETTIONIOGRIPEN”
men det kan det ju vara värt.