21. Sannolikt ord

Som ni har sett kan det ta ganska lång tid att forcera en text som är krypterad med Vigenèrekrypto om man inte vet något om klartexten mer än att den är skriven på ett särskilt språk. Men om man känner till att det finns ett speciellt ord i texten och helst vet att det förekommer på en särskild plats där, då blir det mycket lättare.

Övning 21A

Här är en kryptotext och ni vet att alla klartexter brukar börja med ordet hemlig och att man brukar använda Vigenèrekrypto. Hur många nyckeltal har använts och vad står det?

OEAÖD NTAQO LIÄJW SLYCN RAÖÖÖ

Börja med att översätta det ”sannolika ordets” bokstäver till tal. Sedan kan ni arbeta i den här uppställningen eller göra hela forceringsarbetet på ett särskilt rutat papper. En kryptobokstav kommer så många steg efter klartextbokstaven som nyckeltalet anger. Alltså är nyckeltalet kryptobokstaven minus klartextbokstaven.

Kryptotext i bokstavsform	O	E	A	Ö	D	N	T	A							
Kryptotext i talform	14	4	0	28											
Klartext i talform	7	4	12												
Nyckeltal = krypto – klar	7	0	-12												
+29			+29												
Nyckeltal, icke negativa	7	0	17												
Nyckelbokstäver	*H*														

Om ni bara vill använda bokstäver så går det också bra. Då tar ni fram Vigenèrerutan och får fram nyckelbokstaven ur klartextbokstaven i övre raden och kryptobokstaven i rutan.

Svar: Nyckelord:_____ Klartext:_____

Övning 21B

Här är en annan kryptotext och du vet att kryptören brukar fylla i klartexten med 'x' på slutet så att även sista kryptogruppen består av fem bokstäver. I denna övning slutar klartexten med tre 'x' det vill säga 'xxx'. Man har använt Vigenère-krypto med fyra kryptotal. Vilken är klartexten? Bildar nyckeltalen ett uttalbart nyckelord?

ZUÅPW WTZGW IYXVÖ RSGCF

Svar: Nyckelord:_____Klartext: _____

Övning 21C

Utmana din kryptokompis att forcera Vigenèrekrypto med sannolikt ord. Kom först överens om att klartexterna skall börja med något visst ord, t.ex. 'kompis'. Gör sedan var sin klartext, högst 50 tecken lång, och bestäm var sitt nyckelord, tre eller fyra bokstäver långt. Håll klartexten och nyckeln hemlig. Översätt eventuellt nyckelordet till nyckeltal och kryptera med Vigenèrekrypto. Byt sedan kryptotext med din kompis och forcera den du får.

