17. Caesarkrypto och språkstatistik

I detta avsnitt får ni se hur en statistik över bokstäverna i en kryptotext ser ut som kommer av Caesar-krypto och hur den liknar statistiken för klartext. Ni får också se hur man kan utnyttja detta för att få fram kryptonyckeln som man har använt. På så sätt har ni fått ett nytt sätt att forcera Caesar-krypto.

Till höger är slutet av statistiken för en 80 teckens kryptotext som hör till ett Caesarkrypto. När man krypterar med Caesarkrypto ersätter man varje klartextbokstav med den bokstav som kommer ett visst antal steg längre fram i alfabetet. Det antal steg som man använder kallas kryptonyckeln för kryptot och det skall vara oförändrat för ett helt meddelande. Det borde betyda att språkstatistiken med dess toppar och nollor har förskjutits lika många steg neråt, d.v.s. framåt i alfabetet som kryptonyckeln anger. (Och den del som ramlar över kanten efter 'ö' finns överst i statistiken från och med 'a'.)

R	////
S	///
T	
U	~~////~~ //
V	~~////~~
W	~~////~~ ///
X	/
Y	//
Z	
Å	
Ä	
Ö	

I exemplet ovan kan man se att det finns en lucka med fyra nollor vid ZÅÄÖ. Kan det motsvara klartextens wxyz ? Det stämmer med de tre topparna UVW som kan motsvara rst i klartexten och i så fall med T som motsvarighet till nollan 'q'. Om ni vill se kryptonyckeln mycket tydligt kan ni använda en kryptonyckelmall.

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö
Krypto																	T	U	V	W			Z	Å	Ä	Ö			

T kommer tre steg efter klartextbokstaven 'q' och så vidare. Det verkar mycket troligt att nyckeln till denna kryptotext är 3. Fyll i resten av kryptonyckeln.

Övning 17A och 17B

Ni kan nu gå tillbaka till grundkursens övningar 11A och 11B. Kryptotexterna är kortare än 80 tecken, men ni kan göra pinnstatistik på kryptotexterna och se om ni kan få fram kryptonyckeln med dem. Ta var sin övning och jämför era erfarenheter.

Övning 17C

Arbeta först var för sig. Leta upp var sin text, 50 - 80 bokstäver lång. Bestäm var sin kryptonyckel (ett tal mellan 1 och 28) och håll text och nyckel hemliga för kompisen. Caesar-kryptera och byt kryptotext med varandra. Gör pinnstatistik på kompisens kryptotext och bestäm vilken kryptonyckel som använts. Dekryptera texten. Byt erfarenheter med varandra.

Övning 17D

Forcera den här kryptotexten. Den är skriven med fem bokstäver i taget för att det skall vara enklare att hantera den. Gör pinnstatistik. Det är en fördel att vara två personer även här. En läser bokstäverna och en sätter pinnarna i statistikrutorna. Studera statistiken. Hur är kryptot gjort? Dekryptera Vad står det?

ZYJVB LBLYJ JQYZZ YRÖPZ YKOQS LENJY LÖJKQ YZYJJ PEÅSY
RÖRXÖ ÄYJKO QKSLU HUJKÄ ÖSRBP WYKFF

