20. Vigenères krypto

Ni såg i föregående avsnitt att det blir svårare att forcera kryptot med två nyckeltal än med ett. Då kan vi förstås fortsätta och använda fler nyckeltal och använda dem om och om igen. Ett sådant krypto kallas Vigenère-krypto efter den franske diplomaten *Blaise de Vigenère*, född år 1523.

I flera hundra år ansåg man att Vigenère-kryptot var oforcerbart, men som ni säkert anar var det inte så. Ni skall få lära er hur man knäcker Vigenères krypto. Men först skall vi gå igenom hur man krypterar och dekrypterar med Vigenère-krypto på två olika sätt. Det första sättet använder Vigenère-rutan:

NYCKELBOKSTAV \ klartextbokstav	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
A	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
B	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	A
C	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	A	B
D	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	A	B	C
E	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	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	Å	Ä	Ö	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	Å	Ä	Ö	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
Å	Å	Ä	Ö	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
Ä	Ä	Ö	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
Ö	Ö	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

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall

Övning 20A

Man behöver ett nyckelord. Låt oss ta POTTER. Klartexten *Kryptera är som att trolla* krypterar man så här:

k	r	y	p	t	e	r	a	ä	r	s	o	m	a	t	t	t	r	o	l	l	a
P	*O*	*T*	*T*	*E*	*R*	*P*	*O*	*T*	*T*	*E*	*R*	*P*	*O*								
Z	C	O	F	X																	

Klartextbokstaven bestämmer kolumnen och nyckelbokstaven bestämmer raden där man skall ta kryptobokstaven i Vigenèrerutan. Kryptera färdigt i tabellen ovan och skriv kryptotexten i grupper om fem stora bokstäver här:

Z C O F X

Övning 20B

Dekryptera kryptotexten ZWWJS SOLÖB ZLIIV LENYÖ YJZKW YOA
Nyckeln är HOKUS. Arbeta i den här tabellen:

Z	W	W	J	S	S	O	L	Ö	B	Z	L	I	I													
H	*O*	*K*	*U*	*S*	*H*	*O*	*K*	*U*	*S*	*H*	*O*															
s	i	m	s	a																						

Nyckelbokstaven bestämmer en rad i Vigenèrerutan. Där söker ni upp kryptobokstaven och avläser klartextbokstaven i klartextraden upptill.

Skriv den redigerade klartexten här:

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall

Men det finns ett annat sätt att ordna arbetet när man krypterar och dekrypterar med Vigenèrekrypto. Först tänker vi oss att vi använder fyra nyckeltal, 1, 4, 3 och 20. Att kryptera med ett visst nyckeltal innebär ju att man går just det antal steg fram i alfabetet. Om vi först översätter bokstäverna i alfabetet till tal blir kryptering det samma som att addera nyckeltalet till klartexttalet. Så här kan man göra:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Och så här blir krypteringen av klartexten *Tjuven stal båten*. Tänk på att ni måste subtrahera 29 om kryptobokstaven motsvarar ett tal som är större än 28

Övning 20C

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21	4	13	18	19	0	11					
Addera nyckel	1	4	3	20	1	4	3	20	1	4					
Mellantext m. tal	20	13	23	41	5	17	21	39	1	15					
Subtrahera 29				-29				-29							
Kryptotext m. tal	20	13	23	12	5	17	21	10	1	15					
Kryptotext	U	N	X	M	F	R	V	K	B	P					

Och när man dekrypterar skall man subtrahera nyckeltalen från kryptotexttalen. Blir det negativt skall man addera 29. Gör färdigt krypteringen i rutorna ovan.

Övning 20D

Här är kryptotexten WMOBF RERUX RÅISQ som skall dekrypteras med samma nyckeltal som i övning 20C.

Kryptotext	W	M	O	B	F	R	E	R	U	X	R	Å	I	S	Q
Kryptotext m. tal	22	12	14	1	5	17									
Subbtrah. nyckel	1	4	3	20	1										
Mellantext m. tal	21	8	11	-19											
Addera 29				+29											
Klartext m tal	21	8	11	10											
Klartext	v	i	l	k											

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall

Det kan bli lättare att hantera negativa tal och tal större än 28 om ni använder en omvandlingstabell som visar hur samma bokstav kan motsvara olika tal:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57
0	-28	-27	-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1

Kryptera och dekryptera färdigt exemplet ovan. Vilken blir klartexten efter dekrypteringen?

Svar: _____

Det kan vara svårt att komma ihåg flera nyckeltal till Vigenèrekryptot. Och man vill inte gärna ha nyckeltalen nedskrivna någon längre tid. Ett papper försvinner ju så lätt. Men man kan använda ett nyckelord och sedan översätta ordets bokstäver till tal efter tabellen som finns på förra sidan. I övningarna 20C och 20D motsvarar talen 1, 4, 3 och 20 ”ordet” BEDU som är uttalbart men inte så lätt att gissa.

Övning 20E

Vilket nyckelord motsvarar 6, 8, 17, 14? Svar:_____

Övning 20F

Nu skall ni forcera en text som är krypterad med Vigenèrekrypto. Fyra nyckeltal har använts:

CQÄTU RÖLBS CUOCR RTÄXN JMTEO UNRJE ELMFK NHÖYL UHÅGG
NDOHQ NFFQN DFRFA SDÅDB LRTFQ ZASJE NEDBS AJDET ÖYLBH
NKUSN GFKCE SOBOU NXOMK SÖSCR SYENN ORQEU MKGSÖ CPÄQR
FUDBM AQQAS DÅFPS NVUQI CLDYL FQCÅY MRJJM TEOSV NHHÅT
FRKMZ BXEGR ÄMFMO OSSXA TSNDD HTASQ RTURD UNO

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall

Arbeta tillsammans med denna uppgift. När ni gör de fyra pinnstatistikerna, en för varje nyckeltal, kan det vara svårt att hålla reda på vilket nyckeltal som hör till vilken bokstav. Arbetet blir säkrare om ni först skriver om texten på ett rutat papper med fyra bokstäver i varje rad; här är början. De bokstäver som står i första kolumnen hör till det första nyckeltalet osv.

	C	Q	Ä	T							
	U	R	Ö	L							
	B	S	C	U							

Vad blir klartexten? Motsvarar de fyra nyckeltalen ett uttalbart nyckelord?

Övning 20G

Nu kan du utmana din kryptokompis på forcering av Vigenèrekrypto. Arbeta först var för sig. Välj var sitt nyckelord och håll det hemligt. Ta inte ett för långt ord, tre bokstäver kan vara lagom. Översätt nyckelordets bokstäver till nyckeltal. Välj sedan var sin text, cirka 150 tecken lång, och kryptera den med nyckeltalen eller använd Vigenère-rutan. Håll klartexten hemlig. Byt sedan kryptotext med din kompis och forcera texten som du fått.

Det blir omväxling i arbetet om ni tar klartexter på något annat språk, till exempel engelska.

© Nämnaren, Bengt Beckman & Stig-Arne Ekhall