Kryptering med förskjutningskrypto - uppgifter med lösningar

1. Kryptogrammet ILVNDUQD har krypterats med förskjutningen 3. Bestäm klartexten.

Skriv in bokstäverna i kryptogrammet i tabellen.
Omvandla bokstäverna till tal med hjälp av tabellen.
Om meddelandet är krypterat med förskjutningen 3 behöver vi ”backa” 3 steg. Vi tar -3.
Räkna fram den kodade klartexten.
Översätt klartexten till bokstäver med hjälp av tabellen.

Kryptogram	I	L	V	N	D	U	Q	D
Kodat kryptogram	8	11	21	13	3	20	16	3
Beräkning	−3	−3	−3	−3	−3	−3	−3	−3
Kodad klartext	5	8	18	10	0	17	13	0
Klartext	f	i	s	k	a	r	n	a

Klartext: fiskarna

2. Kryptogrammet YPXNIYPT har krypterats med en förskjutning mellan 3 och 7. Bestäm klartexten.

Börja med att dekryptera de första bokstäverna med de olika nycklarna.

Kryptogram	Y	P		Y	P		Y	P		Y	P		Y	P
Kodat kryptogram	23	15		23	15		23	15		23	15		23	15
Beräkning	−3	−3		−4	−4		−5	−5		−6	−6		−7	−7
Kodad klartext	20	12		19	11		18	10		17	9		16	8
Klartext	u	m		t	l		s	k		r	j		q	i

Undersök nu de inledande bokstäverna i det som kan vara klartexten. Vi känner knappt till några ord som börjar med tl, rj och qi. Kvar är um och sk. Vi testar med sk först.

Kryptogram	y	p	x	n	i	y	p	t					
Kodat kryptogram	23	15	22	13	8	23	15	19					
Beräkning	−5	−5	−5	−5	−5	−5	−5	−5					
Kodad klartext	18	10	17	8	3	18	10	14					
Klartext	s	k	r	i	d	s	k	o					

Det visar sig att nyckeln 5 (som gav oss sk) var den rätta. Hade det inte blivit något läsbart här hade vi istället fått testa med nyckeln 3 som var den som gav oss um.

Klartext: skridsko

3. Kryptogrammet JUÄQLQJHQ har krypterats med en okänd förskjutning. När ordet fiskarna krypterades med samma förskjutning fick vi ILVNDUQD. Bestäm klartexten.

Börja med att undersöka vilken förskjutning av ordet fiskarna som ger ILVNDUQD. Det räcker med att använda första bokstaven. Då får vi veta hur vi ska dekryptera.

Kryptogram	I			J	U	Ä	Q	L	Q	J	H	Q	
Kodat kryptogram	8			9	20	26	16	11	16	9	7	16	
Beräkning	−3			−3	−3	−3	−3	−3	−3	−3	−3	−3	
Kodad klartext	5			6	17	23	13	8	13	6	4	13	
Klartext	f			g	r	y	n	i	n	g	e	n	

Klartext: gryningen

4. Kryptogrammet EDOORQJ har krypterats med en okänd förskjutning. När kryptogrammet krypterades med samma förskjutning en gång till blev kryptogrammet HGRRUTM. Bestäm klartexten.

Här måste vi hantera kryptogrammet som en klartext. Sedan kan vi göra som i uppgift 3 för att ta reda på hur vi ska dekryptera.

Kryptogram	H		E	D	O	O	R	Q	J				
Kodat kryptogram	7		4	3	14	14	17	16	9				
Beräkning	−3		−3	−3	−3	−3	−3	−3	−3				
Kodad klartext	4		1	0	11	11	14	13	6				
Klartext	e		b	a	l	l	o	n	g				

Klartext: ballong

5. Alice har krypterat ett meddelande och fått kryptogrammet HXÖFSDFXR. Hon säger till Bob att han ska *kryptera* hennes kryptogram med samma nyckel som hon använt för att få fram klartexten. Vilken nyckel har Alice valt? Använd nyckeln för att dekryptera Alice kryptogram.

Alice har förskjutit ett okänt antal steg. Om Bob förskjuter det kryptogram han fått av Alice med samma nyckel som hon använt så får han fram klartexten. Tillsammans ska de alltså ha förskjutit 28 steg (så att de är tillbaka på klartexten). 28/2=14, det är alltså 14 som är nyckeln.

I tabellerna ser vi att förskjutning med 14 eller -14 båda ger samma klartext.

Kryptogram	H	X	Ö	F	S	D	F	X	R				
Kodat kryptogram	7	22	27	5	18	3	5	22	17				
Beräkning	−14	−14	−14	−14	−14	−14	−14	−14	−14				
Kodad klartext	−7	8	13	−9	4	−11	−9	8	3				
Kodad klartext	21	8	13	19	4	17	19	8	3				
Klartext	v	i	n	t	e	r	t	i	d				

Kryptogram	H	X	Ö	F	S	D	F	X	R				
Kodat kryptogram	7	22	27	5	18	3	5	22	17				
Beräkning	14	14	14	14	14	14	14	14	14				
Kodad klartext	21	36	41	19	32	17	19	36	31				
Kodad klartext	21	8	13	19	4	17	19	8	3				
Klartext	v	i	n	t	e	r	t	i	d				

6. Kryptogrammet RSFMDROUETNDSÖBJEESÅHSDZEFOR har krypterats med en okänd förskjutning. I klartexten finns 3 st d. Bestäm klartexten.

Börja med att räkna hur många bokstäver det är av varje i kryptogrammet. Det vi vill hitta är de bokstäver som förekommer 3 gånger eftersom bokstaven d kommer att krypteras tre gånger.

RSFMD**R**OUETNDSÖBJEESÅHSDZEFO**R** **här finns 3 st R**

R**S**FMDROUETND**S**ÖBJEE**S**ÅH**S**DZEFOR här finns 3 st S

Det är R och S som finns tre gånger i kryptogrammet. Då vet vi att bokstaven d krypteras till antingen R eller S.

Nu tar vi först reda på vilken nyckel som motsvarar dessa olika möjligheter. (De grå kolumnerna.)

Sedan fyller vi på med de första bokstäverna i kryptogrammet och ser hur inledningen till klartexten kan se ut.

Kryptogram	R	S	F	M		R	S	F	M				
Kodat kryptogram	17	18	5	12		17	18	5	12				
Beräkning	−14	−14	−14	−14		−15	−15	−15	−15				
Kodad klartext	3	4	19	26		2	3	18	25				
Klartext	d	e	t	ä		c	d	s	å				

Vi väljer den inledning som fungerar att läsa och dektypterar med den nyckeln.

Kryptogram	R	S	F	M	D	R	O	U	E	T	N	D	S	Ö
Kodat kryptogram	17	18	5	12	3	17	14	20	4	19	13	3	18	27
Beräkning	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14
Kodad klartext	3	4	19	26	17	3	0	6	18	5	27	17	4	13
Klartext	d	e	t	ä	r	d	a	g	s	f	ö	r	e	n

Kryptogram	B	J	E	E	S	Å	H	S	D	Z	E	F	O	R
Kodat kryptogram	1	9	4	4	18	25	7	18	3	24	4	5	14	17
Beräkning	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14	−14
Kodad klartext	15	23	18	18	4	9	21	4	17	10	18	19	0	3
Klartext	p	y	s	s	e	l	v	e	r	k	s	t	a	d

Klartext: det är dags för en pysselverkstad

7. Alice har krypterat med nyckeln 7. Om Alice upprepar krypteringen flera gånger så upptäcker hon att hon får tillbaka klartexten. Hur många gånger måste Alice kryptera om hon vill få tillbaka klartexten?

Alice måste kryptera så många gånger att hon sammanlagt har förskjutit 28 steg. 28/7=4, alltså 4 gånger.

OBS!
Om vi istället hade låtit Alice kryptera med nyckeln 8 så hade den beräkning vi gjort inte fungerat. När vi delar 28 med 8 får vi inte ett heltal. Det betyder att Alice inte kan komma till förskjutningen 28. Men hon kan förskjuta två ”varv”. Då blir förskjutningen 56 steg. 56/8=7. Alltså 7 gånger.

Det finns ett antal förskjutningar som ger det största möjliga antalet förskjutningar. Det enklaste exemplet på det är förskjutningen 1 som måste genomföras 28 gånger. Det finns ett antal sådana nycklar. Hur många? 12 stycken. (1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27).