Grundläggande kryptering & chiffer

Allmänt om kryptering

För att inte hackers ska kunna snappa upp den information som skickas över nätet så bör man använda sig av någon form av kryptering, d.v.s. förvrängning av informationen. Det finns väldigt många olika sätt att kryptera information och en välkänd tidig metod är Ceasars chiffer. En metod som många kanske känner till är rövarspråket. Dessa metoder är inte längre godtagbara eftersom både människor och datorer knäcker dessa snabbt. För att hindra att dagens datorer ska kunna knäcka ens krypteringar krävs avancerade metoder såsom t.ex. RSA-kryptering.

Nycklar

Gemensamt för alla krypteringsmetoder är användandet av nycklar. Ibland används samma nyckel för att kryptera som för att dekryptera. Dessa metoder kallas symmetriska och motsatsen kallas asymmetriska och då används olika nycklar för kryptering och dekryptering.

Nycklar gör att även om hackern känner till vilken krypteringsmetod som används så kan hackern ändå inte få fram originalmeddelandet om nyckeln är väl vald.

Det som behövs för att kryptera ett meddelande ordentligt är alltså:

- En krypteringsmetod
- En eller två nycklar

Nedan gås metoden Ceasars chiffer igenom.

Ceasars chiffer

Ceasars chiffer går ut på att man byter ut bokstäverna i originalmeddelandet mot andra. Vilka bokstäver man ersätter med beror på nyckeln.

Exempel

Originalmeddelande: Hej jag heter Niklas
Nyckel: 5

Kryptering
Eftersom nyckeln är 5 byts alla bokstäver i originalmeddelandet ut mot den bokstav som finns 5 placeringar längre fram i alfabetet.

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
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

H	e	j		j	a	g		h	e	t	e	r		N	i	k	l	a	s
M	j	o		o	f	l		m	j	y	j	w		S	n	p	q	f	x

Krypterat meddelande: Mjo ofl mjyjw Snpqfx

Dekryptering

För att dekryptera meddelandet krävs att mottagaren har nyckeln (5) och naturligtvis det krypterade meddelandet.

För att dekryptera meddelandet gör man tvärt om d.v.s. man byter ut alla bokstäver mot bokstaven som ligger 5 placeringar tidigare i alfabetet.

M	j	o		o	f	l		m	j	y	j	w		S	n	p	q	f	x
H	e	j		j	a	g		h	e	t	e	r		N	i	k	l	a	s

Meddelande: Hej jag heter Niklas

Övning 1

Kryptera följande meddelande med ceasars chiffer med nyckel 3:

- Hejsan kompis

Övning 2

Du har lyckats komma över ett krypterat meddelande som ser ut så här:

- hy opevehi hix

Du har även ringt till avsändaren och låtsas vara it-supporten och sagt att du behöver hans senaste nyckel vilket han naturligtvis ger dig nämligen nyckeln 4.

Knäck meddelandet.

Övning 3

Du har återigen lyckats komma över ett krypterat meddelande men den här gången gick det inte att lura avsändaren utan du måste försöka knäcka följande meddelande utan nyckel:

- pgm ex osvutkxgj

Annan enkel metod

Nu ska vi kolla på en metod där man byter plats på bokstäverna istället för att byta ut dem. Det går till på det sättet att man delar in originalmeddelandet i block som är lika stora t.ex. 10 tecken stort. I varje block växlar man sedan plats på bokstäverna enligt nyckeln som är lika lång som antalet tecken i varje block. Om vi har delat in meddelandet i block om 10 tecken ska alltså siffrorna 0 till 9 ingå i nyckeln.

Exempel

Meddelande: Hej jag skickar ett meddelande
Nyckel: 4921506738

Vi delar in meddelandet i block:

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
h	e	j	j	a	g	s	k	i	c	k	a	r	e	t	t	m	e	d	d	e	l	a	n	d	e	x	x	x	x

Eftersom vi har nyckeln 4921506738 så flyttar vi om bokstäverna i varje block så att 4 kommer först o.s.v.

4	9	2	1	5	0	6	7	3	8	4	9	2	1	5	0	6	7	3	8	4	9	2	1	5	0	6	7	3	8
a	c	j	e	g	h	s	k	j	i	t	d	r	a	t	k	m	e	e	d	d	x	a	l	e	e	x	x	n	x

Krypterat meddelande: acjeghskjitdratkmeeddxaleexxnx

För att dekryptera så flyttar man bara tillbaka bokstäverna i rätt ordning vilket är lätt med nyckel men betydligt svårare utan nyckel.

Övning 4

Kryptera följande:

Meddelande: Hej jag flyttar runt
Nyckel: 2310

Övning 5

Dekryptera följande:

Krypterat meddelande: aaveldtetödg
Nyckel: 352140

Övning 6

Försök dekryptera följande utan nyckel:

Krypterat meddelande: kirgitvstxrå
Nyckel: ?

X:trauppgift

Försök knäcka följande meddelande som först är krypterat med Ceasar och sedan med den andra metoden:

AWTPVGUFVWHNKTFBXIXC

FACIT

1

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
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

H	e	j	s	a	n		k	o	m	p	i	s
K	h	m	v	d	q		n	r	p	s	l	v

Hejsan kompis = Khmvdq nrpslv

2

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
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

D	u		k	l	a	r	a	d	e		d	e	t
h	y		o	p	e	v	e	h	i		h	i	x

hy opevehi hix = Du klarade det

3

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
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

j	a	g		ä	r		i	m	p	o	n	e	r	a	d
p	g	m		e	x		o	s	v	u	t	k	x	g	j

pgm ex osvutkxgj = jag är imponerad, nyckel = 6

4

0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
h	e	j	j	a	g	f	l	y	t	t	a	r	r	u	n	t	x	x	x

2	3	1	0	2	3	1	0	2	3	1	0	2	3	1	0	2	3	1	0
j	j	e	h	f	l	g	a	t	a	t	y	u	n	r	r	x	x	x	t

Hej jag flyttar runt = jjehflgatatyyunrrxxxt

5

0	1	2	3	4	5	0	1	2	3	4	5
d	e	v	a	l	a	g	ö	t	t	d	e

3	5	2	1	4	0	3	5	2	1	4	0
a	a	v	e	l	d	t	e	t	ö	d	g

aaveldtetödg = de va la gött de

6

0	1	2	0	1	2	0	1	2	0	1	2
r	i	k	t	i	g	t	s	v	å	r	x

2	1	0	2	1	0	2	1	0	2	1	0
k	i	r	g	i	t	v	s	t	x	r	å

kirgitvstxrå = riktigt svår, nyckel = 210

X

Nu är det slut för idag

N	U	Ä	R	D	E	T	S	L	U	T	F	Ö	R	I	D	A	G	
P	W	A	T	F	G	V	U	N	W	V	H	B	T	K	F	C	I	X	X
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3

Ceasar nyckel = 2
Metod 2 nyckel = 2130