Kryptering & Chiffer Del 2

Vigenere

Vigenere är en annan krypteringsmetod som är mer avancerad än de två föregående. Denna metod är säkrare men långt ifrån säker om man använder dåliga nycklar. Det finns dock en variant av vigenere som är omöjlig att knäcka vilket är unikt, mer om detta senare.

För att kryptera med vigenere behöver man ett meddelande och en nyckel. Nyckeln består av bokstäver. Meddelandet delas in i lika stora block som nyckeln är lång. Man plussar ihop positionen i alfabetet hos nyckelbokstaven och meddelandebokstaven och får då en ny position. Det krypterade meddelandet innehåller bokstaven på denna position i alfabetet.

Exempel

Kryptering

Nyckel: tjena
Meddelande: Vi testar att kryptera med vigenere

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
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

t	j	e	n	a	t	j	e	n	a	t	j	e	n	a	t	j	e	n	a	t	j	e	n	a	t	j	e	n	a
v	i	t	e	s	t	a	r	a	t	t	k	r	y	p	t	e	r	a	m	e	d	v	i	g	e	n	e	r	e

=

2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1
0	0		4		0	0		4		0	0		4		0	0		4		0	0		4		0	0		4	
2	9	2	5	1	2	1	1	1	2	2	1	1	2	1	2	5	1	1	1	5	4	2	9	7	5	1	5	1	5
2		0		9	0		8		0	0	1	8	5	6	0		8		3			2				4		8	

= (Om summan är större än 29 dras 29 bort.)

1	1	2	1	2	1	1	2	1	2	1	2	2	1	1	1	1	2	1	1	2	1	2	2	8	2	2	1	3	6
3	9	5	9	0	1	1	3	5	1	1	1	3	0	7	1	5	3	5	4	5	4	7	3		5	4	0		
m	s	y	s	t	k	k	w	o	u	k	u	w	j	q	k	o	w	o	n	y	n	å	w	h	y	x	j	c	f

Krypterat meddelande: msystkkwoukuwjqkowonynåwhyxjcf

Dekryptering

Nyckel: tjena
Krypterat meddelande: msystkkwoukuwjqkowonynåwhyxjcf

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
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

1	1	2	1	2	1	1	2	1	2	1	2	2	1	1	1	1	2	1	1	2	1	2	2	8	2	2	1	3	6
3	9	5	9	0	1	1	3	5	1	1	1	3	0	7	1	5	3	5	4	5	4	7	3		5	4	0		
m	s	y	s	t	k	k	w	o	u	k	u	w	j	q	k	o	w	o	n	y	n	å	w	h	y	x	j	c	f

nyckeln = tjena = 20 10 5 14 1 (denna ska dras bort från det krypterade meddelandet.)

1	1	2	1	2	1	1	2	1	2	1	2	2	1	1	1	1	2	1	1	2	1	2	2	8	2	2	1	3	6
3	9	5	9	0	1	1	3	5	1	1	1	3	0	7	1	5	3	5	4	5	4	7	3		5	4	0		
2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1	2	1	5	1	1
0	0		4		0	0		4		0	0		4		0	0		4		0	0		4		0	0		4	

= (Om resultatet av subtraktionen blir mindre än 1 läggs 29 på)

2	9	2	5	1	2	1	1	1	2	2	1	1	2	1	2	5	1	1	1	5	4	2	9	7	5	1	5	1	5
2		0		9	0		8		0	0	1	8	5	6	0		8		3			2				4		8	
v	i	t	e	s	t	a	r	a	t	t	k	r	y	p	t	e	r	a	m	e	d	v	i	g	e	n	e	r	e

=
Vi testar att kryptera med vigenere.

One time pad

Om man använder en nyckel som är lika lång som meddelandet så blir det krypterade meddelandet oknäckbart om man bara använder nyckeln till ett meddelande. Problemet är att man måste lämna över en nyckel för varje meddelande. Detta kan göras på ett sådant sätt att man träffas gemensamt och skapar en hel bunt med nycklar som är tillräckligt långa för vilka meddelanden som helst och sedan när man skickar meddelanden till varandra så använder man nycklarna i tur och ordning. Detta görs bland annat inom militären till väldigt viktig information. Det bästa är att oavsett hur snabba datorer som någonsin kommer att finnas så kommer de aldrig att kunna knäcka sådana här meddelanden eftersom det är teoretiskt omöjligt.

Övningar

Övning 1

Kryptera meddelandet: Hejsan allihopa
Nyckel: tja

Övning 2

Dekryptera: anqmsozj
Nyckel: hej

Övning 3

Knäck: umksa
Nyckel: ? (nyckellängd = 2)

Statistik

För att knäcka krypterade meddelanden som är krypterade med någon utav ”våra” tre metoder så gäller det först att ta reda på vilket som används och om det är ceasar eller metod 2 så går det att knäcka med hjälp av statistik eftersom vissa bokstäver används mer än andra. Har man nyckellängden för vigenere så går det även att knäcka detta med statistik. För att man ska kunna använda statistik så måste meddelandet var långt och nyckel helst vara kort.

Tabell över engelska språket

a	-- -- -- -- -- -- -- --	(8.07%)
b	-- -	(1.40%)
c	-- -- -	(2.27%)
d	-- -- -- -- --	(4.71%)
e	-- -- -- -- -- -- -- -- -- -- -- -- -	(12.49%)
f	-- -- -	(2.26%)
g	-- --	(2.08%)
h	-- -- -- -- -- -- -	(6.57%)
I	-- -- -- -- -- -- --	(6.81%)
j	.	(0.11%)
k	--	(0.79%)
l	-- -- -- -	(3.68%)
m	-- -- -	(2.56%)
n	-- -- -- -- -- -- --	(7.08%)
o	-- -- -- -- -- -- -- -	(7.74%)
p	-- -	(1.62%)
q	.	(0.11%)
r	-- -- -- -- -- --	(6.16%)
s	-- -- -- -- -- -- -	(6.30%)
t	-- -- -- -- -- -- -- -- --	(8.99%)
u	-- -- --	(2.78%)
v	--	(0.86%)
w	-- -- -	(2.37%)
x	.	(0.11%)
y	-- --	(2.03%)
z	.	(0.04%)

Knäcka ceasar med statistik

För att knäcka en engelsk text som är krypterad med ceasar så kan man se vilken bokstav som förekommer oftast och anta att denna bokstav är ett ’e’ i det riktiga meddelandet. Om det inte går ihop testar man om den bokstav som förekommer näst oftast kan vara ett ’e’ osv. Det krävs antagligen inte mer ett par tre tester innan man har hittat rätt beroende på hur långt meddelandet är.

Knäcka metod 2 med statistik

Det enda man kan komma fram till är om meddelandet är krypterat med en metod som använder omflyttning av bokstäver eftersom man då kan se att det är bokstaven ’e’ som förekommer oftast och sedan ’a’ osv. det går dock inte att få fram originalmeddelandet med statistik men metod 2 går oftast lätt att knäcka ändå.

Knäcka Vigenere med statistik

Om man känner till nyckellängden (den går att beräkna fram) så kan man knäcka vigenere på samma sätt som man knäcker ceasar:

Exempel:

Krypterat meddelande: ikofvvugvuxlhgqfth (Hi, let's test vigenere)
Nyckelängd: 3 (abc)

i	k	o
f	v	v
u	g	v
u	x	l
h	g	q
f	t	h

Nu kan vi lösa kolumn ett, två och tre som tre olika ceasarchiffer.

kolumn1
ifuuhf = 2 f , 2 u, 1 i, 1 h
antag f = e => nyckelbokstav = a.
=> hettge (t är en vanlig bokstav i engelskan så detta verkar vara en trolig lösning)

kolumn2
kvgxgt = 2 g, 1 k, 1 v, 1 x, 1 t
antag g = e => nyckelbokstav = b
=> itever (vanliga bokstäver i engelskan så detta verkar vara en trolig lösning)

Vi har nu hi_et_te_tv_ge_er_

kolumn3
ovvlqh = 2 v, 1 o, 1 l, 1 q, 1 h
antag v = e => nyckelbokstav = q
=> xeeuzq (ovanliga bokstäver så vi testar något annat)
testar o = e (inte bra)
testar l = e (inte bra)
testar q = e (inte bra)
antag h = e => nyckelbokstav = c
=> lssine => hiletstestvigenere = hi lets test vigenere = hi, let's test vigenere. LÖST!

Naturligtvis är det inte alltid så här enkelt, i alla fall inte med så korta meddelanden men det fungerar bra som exempel.

Övningar

Övning 4

Bestäm vilken metod som har använts för att kryptera följande meddelanden (ceasar eller metod 2) (engelska):

- qrzbrxnqrzwkdwlxvhgfhdvduwrhqfubsw
- rheesieuedtmdhtozwzo

Övning 5

Knäck följande vigenere-meddelande på engelska som är krypterad med en nyckel på 3 bokstäver:

- vmdsqggmpotahwrsbaaiwsqfzqfhtqawdsmmgg

FACIT

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
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

1

h	e	j	s	a	n	a	l	l	i	h	o	p	a
t	j	a	t	j	a	t	j	a	t	j	a	t	j

=

8	5	10	19	1	14	1	12	12	9	8	15	16	1
20	10	1	20	10	1	20	10	1	20	10	1	20	10

= (summa % 29)

15	5	11	10	11	15	21	22	13	29	18	16	7	11
o	e	k	j	k	o	u	v	m	ö	r	p	g	k

=

oekjkouvmörpgk

2

v	i	g	e	n	e	r	e
h	e	j	h	e	j	h	e

=

22	9	7	5	14	5	18	5
8	5	10	8	5	10	8	5

= (Summa)

1	14	17	13	19	15	26	10
a	n	q	m	s	o	z	j

=
anqmsozj

3

k	l	a	r	t
j	a	j	a	j

=

11	12	1	18	20
10	1	10	1	10

= (summa)

21	13	11	19	1
u	m	k	s	a

=
umksa

4

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
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Now you know that I used ceasar to encrypt = qrzbrxnqrzwkdwlxvhgfhdvduwrhqfubsw

---

0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
h	e	r	e	i	u	s	e	d	m	e	t	h	o	d	t	w	o	z	z

2	0	3	1	2	0	3	1	2	0	3	1	2	0	3	1	2	0	3	1
r	h	e	e	s	i	e	u	e	d	t	m	d	h	t	o	z	w	z	o

here I used method two = rheesieuedtmdhtozwzo

5

n h l

h	e	r
e	i	u
s	e	d
a	l	o
t	o	f
e	t	o
m	a	k
e	i	t
l	i	t
t	l	e
m	o	r
e	e	a
s	y	

14 8 12

8	5	18
5	9	21
19	5	4
1	12	15
20	15	6
5	20	15
13	1	11
5	9	20
12	9	20
20	12	5
13	15	18
5	5	1
19	25	

22	13	4
19	17	7
7	13	16
15	20	1
8	23	18
19	2	1
1	9	23
19	17	6
26	17	6
8	20	17
1	23	4
19	13	13
7	7	

v	m	d
s	q	g
g	m	p
o	t	a
h	w	r
s	b	a
a	i	w
s	q	f
z	q	f
h	t	q
a	w	d
s	m	m
g	g	

here I used a lot of e to make it little more easy =
vmdsqggmpotahwrsbaaiwsqfzqfhtqawdsmmgg