Nämnarens kryptoskola

2. Krypto – språk och matematik

Denna andra del av Kryptoskolan belyser kopplingar mellan språk och matematik. De andra delarna finner du på ncm.gu.se/arkivN. Kryptoskolan är ett studiematerial som är skyddat av upphovsrättslagen. Studiematerialet får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Med kryptering menar vi hur man döljer innehållet i ett meddelande genom att ersätta dess bokstäver med andra bokstäver på ett sådant sätt att den som inte är insatt i alla aspekter av förfarandet inte kan få reda på innehållet. Men givetvis skall den behörige mottagaren, den för vilken meddelandet är avsett, enkelt kunna ta fram vad avsändaren menat.

Med dekryptering avser vi den omvända processen, dvs att ur en given kryptotext, med full kännedom om hur avsändaren förfarit för att tillverka denna, ta fram den bakomliggande klartexten. Om den som gör detta inte exakt vet hur krypteringen har gått till talar vi om forcering.

Caesar-krypto

Det enklaste kryptot kallas Caesar-kryptot, benämnt efter den romerske härskaren med samma namn. Det går till så här:

Texten i ett meddelande skall ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg längre fram i alfabetet, säg tills vidare tre steg, Om den första klartextbokstaven är *h* blir den första kryptobokstaven *K*.

Det tal som styr krypteringen behöver inte vara just tre utan vilket annat heltal som helst mellan 1 och 28; vi kallar detta tal för kryptonyckeln och betecknar den med N, $1 < N < 28$. Den som bestämmer nyckeln får överlämna den till den andra personen på ett säkert sätt t ex vid ett personligt möte.

Med en matematisk formel kan man beskriva krypteringsförfarandet så här:

$$C = K + N \pmod{29}$$

där (mod 29) här betyder att vi subtraherar 29 om summan blir större eller lika med 29. Talet 29 står för antalet bokstäver i det svenska alfabetet, *W* medräknat. Vi behöver en översättningstabell mellan bokstäver och 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

Låt oss nu kryptera klartexten *Tjuven stal båten* med kryptonyckeln N = 9. Kom ihåg att räkna (mod 29). Fortsätt att fylla i följande tabell:

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21											
Addera nyckel	9	9	9	9											
Kryptotext m. tal	28	18	0	1											
Kryptotext	Ö	S	A	B											

Om man vill *dekryptera* en text, dvs återföra kryptotexten till klartext, utför man proceduren omvänt, alltså subtraheras kryptonyckeln från kryptotexten i talform bokstav för bokstav. Men det kan vara intressant att notera att inversen till addition med N (mod 29) kan utföras som addition med 29 - N (mod 29), eller i formler:

$K = C - N \pmod{29} = C + (29 - N) \pmod{29}$.

Använd denna metod för att dekryptera kryptotexten i föregående exempel. Dekrypteringsnyckeln blir 29 - 9 = 20.

Kryptotext	Ö	S	A	B											
Kryptotext m. tal	28	18	0	1											
Addera nyckel	20	20	20	20											
Klartext m. tal	19	9	20	21											
Klartext	t	j	u	v											

Om man i stället vill arbeta med det internationella 26-bokstavsalfabetet, alltså utan *å*, *ä* och *ö*, kan man använda metoderna ovan utan problem. Krypterings- respektive dekrypteringsformlerna blir då

$C = K + N \pmod{26}$

där $0 < C, K < 26$ och kryptonyckeln N uppfyller $0 < N < 26$ och

$K = C + (26 - N) \pmod{26}$.

Kryptering med multiplikation

Hur blir det om vi ersätter Caesar-kryptots addition med multiplikation? Låt oss undersöka det. Krypteringsformeln skulle i så fall se ut så här:

$C = N \times K \pmod{29}$
där $0 < C, K < 29$ och kryptonyckeln N uppfyller $2 < N < 29$.
(Fundera på varför vi undantar N = 1.)

Vi kan behöva subtrahera talet 29 några gånger så att resultatet hamnar i rätt intervall: från 0 till 28. En krypteringstabell ser ut så här för N = 4:

Klar	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
Klar m. tal	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
Krypto m. tal	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
Krypto	A	E	I	M	Q	U	Y	Ö	D	H	L	P	T	X	Ä	C	G	K	O	S	W	Å	B	F	J	N	R	V	Z

Det här ser ju bra ut. Alla bokstäver förekommer i kryptoraden en och endast en gång. Det är tillräckligt för att vi skall kunna kryptera alla bokstäver och dekryptera entydigt. Detta kan man bevisa enkelt för alla nycklar, inte bara för N = 4. Om två klartextbokstäver K_1 och K_2 krypterade med nyckeln N skulle ge samma kryptobokstav skulle vi ha

$N \times K_1 = N \times K_2 \pmod{29}$ eller
$N \times (K_1 - K_2) = 0 \pmod{29}$, vilket är det samma som att
$N \times (K_1 - K_2) = m \times 29$ för något heltal m.

Eftersom 29 är ett primtal måste då någon av faktorerna i vänsterledet vara delbar med 29. Men så är inte fallet. Båda är ju högst 28 i absolutbelopp.

Låt oss gå över till dekryptering. Det omvända till multiplikation är ju division, men det verkar ju inte helt glasklart hur man skall beräkna C/N (mod 29). I fallet med Caesar-kryptot kunde vi ersätta subtraktion med addition; kan vi ersätta division med multiplikation? Vi försöker först med N =4.

$C = 4 \times K \pmod{29}$ och vi söker dekrypteringsnyckeln D, så att
$K = D \times C \pmod{29}$. Insättning ger
$K = D \times 4 \times K \pmod{29}$ och det skall gälla för alla K.

Detta kan vi uppnå om vi kan hitta ett heltal D så att

$D \times 4 = 1 \pmod{29}$ eller
$D \times 4 - 1 = m \times 29$ för något heltal m.

Den som är hemma i användningen av Euklides algoritm kan pröva med den. Annars går det bra att testa med några olika värden på m och se om *D* blir ett inte för stort heltal. Då finner man att m = 3 ger D = 22.

Om vi krypterar genom att multiplicera med 4, kan vi alltså sedan dekryptera med multiplikation med 22. Och så gäller det att subtrahera 29 tillräckligt många gånger så att resultatet håller sig inom intervallet från 0 till 28. Med samma teknik kan vi hitta den multiplikativa inversen till varje N (mod 29).

Men kan vi lika lätt använda ett sådant här multiplikationskrypto om vi begränsar oss till det internationella 26-bokstavsalfabetet? Vi kanske erinrar oss att för beviset om kryptots en-entydighet utnyttjades att 29 är ett primtal. Och talet 26 kan uppdelas $26 = 2 \times 13$. Låt oss se vad som händer om vi försöker med krypteringsformeln

$C = 4 \times K \pmod{26}$.

Motsvarande krypteringstabell skulle bli

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
Klar med tal	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
Krypto m. tal	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
Kryptobokstav	A	E	I	M	Q	U	Y	C	G	K	O	S	W	A	E	I	M	Q	U	Y	C	G	K	O	S	W

Det här blir inget krypto. Funktionen är inte en-entydig. Exempelvis ger båda klartextbokstäverna *h* och *u* kryptobokstaven C. Det går inte att dekryptera, vilket inte är så förvånande. När vi multiplicerar med det jämna talet 4 så förblir produkten jämn hur många gånger vi än subtraherar det jämna talet 26.

Talet 13 kan vi inte heller ha som nyckel. Då får vi bara kryptobokstäverna *A* och *B*. Generellt får en kryptonyckel för multiplikationskryptot med 26-bokstavsalfabetet inte ha någon primfaktor som finns i 26, dvs 2 eller 13. Som möjlig kryptonyckel återstår det endast 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, och 25.

Enkel substitution

Låt oss gå ett steg till och definiera ett krypto där kryptotabellens alfabet för kryptobokstäver är slumpmässigt utplacerade. Kryptonyckeln består i den substitution/funktion som tabellen definierar. Här är ett exempel.

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

Låt oss kryptera texten *Ada och Kal badar* med denna nyckel.

Klartext	a	d	a	o	c	h	k	a	l	b	a	d	a	r
Kryptotext	Q	C	Q	Ö	M	H	L	Q	A	G	Q	C	Q	Å

Om man vill beskriva enkel substitution med en formel kommer man inte längre än till att skriva

$C = \mathcal{N}(K)$ för kryptering och $K = \mathcal{N}^{-1}(C)$ för dekryptering

Där $\mathcal{N}$ är funktionen som definieras av substitutionstabellen och $\mathcal{N}^{-1}$ dess invers.

Forcering

Kan den som snappat upp en kryptotext härleda den tillhörande klartexten utan att på förhand känna till den använda nyckeln? Eller med andra ord, hur lätt är det att knäcka de krypton som beskrivits ovan?

Caesar-kryptot har bara 28 olika nycklar. Det är bara att provdekryptera med dessa nycklar och den som ger läsbar klartext är den rätta. Hur detta arbete kan utföras praktiskt på ett enkelt sätt beskrivs i studiematerialet. Multiplikationskryptot har ännu färre nycklar, så det är inte svårare att knäcka.

Läsaren har nog redan märkt en annan svaghet i de multiplikationskrypton som vi behandlat hittills. Klartextbokstaven a blir alltid kryptobokstaven A oberoende av vilken nyckel som används. Det kan man undvika genom att använda två nyckeltal, N_1 och N_2 och krypteringsformeln $C = N_1 \times K + N_2 \pmod{29}$. Då blir det visserligen några fler nycklar att pröva, men forceringsarbetet blir endast obetydligt svårare.

Hur svårt är det att forcera enkel substitution? Låt oss först beräkna hur många nycklar som kryptot har. I substitutionstabellen som definierar kryptonyckeln kan vi placera ut kryptobokstaven *A* på 29 ställen. Då återstår 28 platser för *B*. Dessa två kan alltså sättas ut på 29×28 olika sätt. För C finns nu 27 platser och för de tre första $29 \times 28 \times 27$ sätt. Så fortsätter vi och finner att det finns $29 \times 28 \times 27 \times \ldots \times 2 \times 1 = 29!$ (29-fakultet) olika möjliga nycklar. Antalet möjliga nycklar är alltså ungefär 9×10^{30}, alltså en nia med trettio siffror efter sig.

Så många prövar man inte igenom i brådrasket. Men enkel substitution har en annan svaghet. Frekvensen hos klartextens bokstäver lyser igenom i kryptotexten. Det ser man tydligt i exemplet med Ada och Kal. I normalsvenskan är bokstaven *a* vanligast. I kryptotexten är Q vanligast. Man kan börja med att gissa att dessa bokstäver hör ihop. Och så fortsätter man med de övriga bokstäverna. Man brukar räkna med att en skicklig forcör klarar av att forcera enkel substitution om textlängden är 50 bokstäver eller fler.

För att konstruera svårforcerbara krypton behöver man alltså öka antalet möjliga nycklar tillräckligt mycket för att det inte skall gå att pröva igenom alla. Det måste dessutom gå till på ett sådant sätt att forcören inte kan ta några genvägar i sitt sökande efter den rätta nyckeln. För den som vill veta mer om de matematiska aspekterna av krypto rekommenderas Bruce Schneier: *Applied Cryptography, Second Edition*, John Wiley & Sons, 1996.