

Koder

Kristian Ranestad

8. Mars 2005

Kryptering

Feilrettingskoder

Kongruensregning

Kongruensregning i kryptering

Kongruensregning i feilrettingskoder

Litteratur

En hemmelig melding

Kari sender til Ole den hemmelige meldingen:

J MPWF V

siden responsen er litt treg prøver hun påny med:

U EVOL I

Nå kommer svaret raskere.....

Klartekst

Meldingen er selvsagt

I LOVE U

De to eksemplene viser to prinsipper for koding, nemlig **substitusjon** og **permutasjon**.

substitusjon

Substitusjon erstatter bokstavene med andre bokstaver eller tegn.

Hvis **E,I,L,O,U,V** erstattes med **%,+,,=,*,@,&** vil den kodete meldingen bli

+ = * & % @

permutasjon

Permutasjon går ut på å bytte om på rekkefølgen på bokstavene, for eksempel å lese baklengs

U EVOL I

eller

E VULI O

Koding med tall

I praksis brukes både substitusjon og permutasjon.

Substitusjon: bokstaver $\mapsto$ tall.

Permutasjon: bytter om tall.

ASCII

Datamaskiner bruker ASCII koden:

$a \mapsto 1100001$

$A \mapsto 1000001$

$\& \mapsto 0100110$

.....

Kodenøkkel

Vi skal holde oss til de 6 bokstavene

EILOUV

som vi substituerer

E	I	L	O	U	V
↓	↓	↓	↓	↓	↓
1	2	3	4	5	6

Denne substitusjonstabellen kaller vi en **kodenøkkel**

Kodet melding

Meldingen

I LOVE U

blir med denne kodenøkkelen kodet til

234615

Krypteringsnøkkelen

For å gjøre meldingen hemmelig koder vi en gang til med permutasjonen.

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
6	4	1	3	2	5

Denne kalles **krypteringsnøkkelen**

Dekrypteringsnøkkelen

Permutasjonen

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
6	4	1	3	2	5

bytter 1 med 6, 2 med 4, o.s.v. Den omvendte permutasjonen

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
3	5	4	2	6	1

bytter tilbake og kalles derfor **dekrypteringsnøkkelen**.

Krypteringsprosedyre

MELDING:

I LOVE U

KODENØKKEL (ÅPEN):

E	I	L	O	U	V
↓	↓	↓	↓	↓	↓
1	2	3	4	5	6

KODET MELDING:

234615

Kryptering

KODET MELDING:

234615

KRYPTERINGSNØKKEL (HEMMELIG):

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
6	4	1	3	2	5

KRYPTERT MELDING:

413562

Dekrypteringsprosedyre

KRYPTERT MELDING:

413562

DEKRYPTERINGSNØKKEL (HEMMELIG):

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
3	5	4	2	6	1

DEKRYPTERT MELDING:

234615

Dekoding

DEKRYPTERT MELDING:

234615

DEKODENØKKEL (ÅPEN):

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓
E	I	L	O	U	V

DEKODET MELDING:

I LOVE U

Problem

Krypteringsnøkkelen kan lett bli lange og vanskelige å huske.
Vi trenger metoder til å lage gode permutasjoner som er lettere å huske.

Til dette kan vi bruke “moduloregning” eller kongruensregning, som vi skal komme tilbake til.

Feilretting av data

I overføring av data oppstår det feil.
Hvis dataene er kodet med en **feilrettingskode** kan mottakeren korrigere feilene.
Slik får vi gode data (TV-bilder og god lyd) likevel.

Strekkode

Strekkodene på varer i butikken er feilrettingskoder.

Feilrettingskode

En feilrettingskode er en kodenøkkel som er slik at det er mulig å oppdage feil i den kodete meldingen uten at en kjenner den opprinnelige meldingen.

Eksempel

Med alfabetet **EILOUV** og kodenøkkelen

E	I	L	O	U	V
↓	↓	↓	↓	↓	↓
11	22	33	44	55	66

blir meldingen

I LOVE U

kodet til

223344661155

Oppdaget feil

Dersom den mottatte meldingen er

223244661155

ser mottakeren at det er oppstått en feil i den andre bokstaven i meldingen (det skulle ha vært 22 eller 33, altså en **I** eller en **L**).

Strekkoden

Strekkoden.

Strekkodene "oppdager" feil, når den ikke får kodene til å passe med listen av kodete varer.

To strekkoder er alltid forskjellige på minst to plasser for at feil på en plass skal oppdages.

Eksempler

ISBN-numre og fødselsnumre er også kodet med en feilrettingskode.

Regning modulo t

La t være et naturlig tall. Dersom vi deler et helt tall med t , har vi t mulige rester: $0, 1, 2, \dots, t - 1$.

Vi kan regne med tallene $0, 1, 2, \dots, t - 1$ ved bare å bruke disse restene. Det vil si at hver gang vi har to av disse tallene kan vi legge dem sammen eller multiplisere dem og få et nytt tall, nemlig ved først å addere eller multiplisere på vanlig måte og så ta resten etter divisjon med t .

Denne regningen med tallene $0, 1, 2, \dots, t - 1$ kaller vi kongruensregning eller regning modulo t .

Kongruens

To tall a og b har samme rest modulo t hvis og bare hvis differansen $a - b$ er delelig med t . I så fall sier vi at de to tallene a og b er kongruente modulo t og skriver $a \equiv b \pmod{t}$.

Derfor kalles også den regningen vi har beskrevet **kongruensregning**.

Regning modulo 2

partall + partall = partall, oddetall + oddetall = partall

partall + oddetall = oddetall

Addisjonstabellen og multiplikasjonstabell modulo 2:

+	0	1	·	0	1
0	0	1	0	0	0
1	1	0	1	0	1

Regning modulo 3

Addisjonstabellen og multiplikasjonstabell modulo 3:

+	0	1	2	·	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

modulo 7

Multiplikasjon med 5 modulo 7 blir:

·	0	1	2	3	4	5	6
5	0	5	3	1	6	4	2

$3 \cdot 5 \equiv 1$ modulo 7 fordi $15 : 7$ gir 2 med rest 1.

Kryptering modulo 7

Multiplikasjon med 5 modulo 7 gir en permutasjon:

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓,
5	3	1	6	4	2

mens multiplikasjon med 3 gir den omvendte permutasjonen

1	2	3	4	5	6
↓	↓	↓	↓	↓	↓.
3	6	2	5	1	4

Hvorfor?

invers modulo 7

Hvis jeg starter med et tall x og multipliserer det først med 5 og deretter med 3 modulo 7 får jeg

$$x \cdot 5 \cdot 3 = x \cdot (5 \cdot 3) \equiv x \cdot 1 = x \pmod{7}.$$

Det vil si at hvis jeg først krypterer ved å multiplisere med 5, så kan jeg dekryptere ved å multiplisere med 3 modulo 7.

Lett å knekke

Multiplikasjon modulo 7 er lettere enn å huske en lange permutasjoner, men siden dekrypteringsnøkkelen er av samme type så er disse krypteringsnøkklene er ikke særlig sikre.

Potenser

Litt sikrere krypteringsnøkler får en ved å ta potenser. I vårt eksempel tar vi potenser modulo 7:

x	1	2	3	4	5	6
3^x	3	2	6	4	5	1

Dekrypteringsnøkkelen er ikke av samme type. En må rett og slett skrive opp den omvendte permutasjonen

RSA og AES

De mest brukte krypteringsoppskriftene som brukes idag er RSA og AES.

RSA bruker potenser modulo store tall som er produkt av to primtall som krypteringsnøkkel.

AES er laget i Belgia og bruker litt mer avansert algebra i en effektive og sikker krypteringsalgoritme.

ISBN-koden

Alle bøker klassifiseres med ISBN-koden (International Standard Book Number). Denne koden består av et 10-sifret tall representert i 11-tallsystemet.

La oss kalle sifrene $x_1 x_2 \dots x_{10}$. Da er sifrene i en ISBN-kode alltid slik at

$$x_1 + 2x_2 + 3x_3 + \dots + 10x_{10} \equiv 0 \pmod{11}. \quad (11).$$

Denne ligningen kalles **kontrolligningen**, og brukes til å kontrollere om et 10-sifret tall i 11-tallsystemet er et ISBN-tall. Kontrolligningen oppdager feil i en posisjon, og korrigerer feilen! Den oppdager også om to sifre er byttet om!

Norske personnummer

I Norge har vi et personnummersystem som i ulik sammenheng blir brukt til å identifisere personer.

Når vi blir født, får vi tildelt et 11-sifret tall.

De seks første sifrene er fødselsdatoen.

De neste tre er vårt personlige nummer, som skal skille mennesker født på samme dato.

De siste to sifrene er kontrollsifre.

Kontrolligningen

Dersom de første ni sifrene er $x_1x_2 \dots x_9$, så er de tiende sifferet

$$x_{10} \equiv 8x_1 + 4x_2 + 5x_3 + 10x_4 + 3x_5 + 2x_6 + 7x_7 + 6x_8 + 9x_9 \quad (11)$$

mens det ellefte sifferet er bestemt ved

$$x_{11} \equiv 6x_1 + 7x_2 + 8x_3 + 9x_4 + 4x_5 + 5x_6 + 6x_7 + 7x_8 + 8x_9 + 9x_{10} \quad (11)$$

Les videre i

1. B. Johnsen: Kryptografi - en gammel disiplin med moderne anvendelser, i Per Hag & Ben Johnsen (red.): *Fra Matematikkens Spennende Verden*, Tapir, 1993, 123-134.
2. Jacobus H. van Lint: Kompaktskivans matematik, *Normat*, **48** (2000), 115-122.
3. L. Nilsen: Modulære kvadratrøtter og moderne kryptologi, *Normat*, **40** (1992), 75-89.
4. K. Ranestad: Koder i klasseromet,
<http://www.matematikk.org/pub/html/temahefter/>.
5. S. Singh: Koder, Aschehoug 2000