Oversikt over kryptografi

Richard Williamson

3. desember 2014

Oppgave 1

Person A ønsker å sende meldingen «Ha det!» til person B, og ønsker å benytte RSA-algoritmen for å kryptere den. Den offentlige nøkkelen til person B er $(91, 43)$. Krypter meldingen.

Hvordan løse oppgaven?

Først oversetter vi meldingen fra symboler til heltall, ved å benytte Tabell 6.1 i forelesningsnotatene. Denne tabellen blir gitt ved behov på eksamen.

Vi ganske enkelt erstatter hvert symbol i meldingen «Ha det!» med dets tilsvarende heltall i tabellen. Det vil si: vi erstatter H med 8, A med 1, osv.

Tabellen nedenfor viser hele oversettelsen.

Symbol	Tilsvarende heltall
H	8
A	1
	0
D	4
E	5
T	20
!	42

Tabell 1: Oversettelsen av meldingen

Hva gjør jeg da?

Ganske enkelt: opphøy alle de oversatte heltallene i 43, altså i det andre naturlige tallet i den offentlige nøkkelen til person B. Vi får:

$$8^{43}\ 1^{43}\ 0^{43}\ 4^{43}\ 5^{43}\ 20^{43}\ 42^{43}.$$

Nå må vi erstatte disse heltallene med heltall som er kongruent til dem modulo det første naturlige tallet i den offentlige nøkkelen til person B, altså 91, og som i tillegg er mindre enn 91 og større enn eller like 0.

Hvordan gjør jeg det?

Hvis heltallet ikke er for stort, kan du bruke kalkulatoren din. Se oversikten over hvordan gjøre dette.

Ellers må du dele opp potensen.

Hva mener vi med det?

La oss for eksempel regne ut 8^{43}. Vi kan for eksempel begynne med å observere at

$$8^2 \equiv 64 \equiv -27 \pmod{91}.$$

Da er

$$8^4 \equiv (-27)^2 \equiv 90 \equiv -1 \pmod{91}.$$

Da er

$$8^{40} = \left(8^4\right)^{10} \equiv (-1)^{10} = 1 \pmod{91}.$$

Vi konkluderer med:

$$8^{43} = 8^{40} \cdot 8^3 \equiv 1 \cdot 8^3 = 8^3 \equiv 57 \pmod{91}.$$

Poenget nå er at jobber i denne utregningen med heltall som ikke er for store for kalkulatoren din: 8^2, $(-27)^2$, og 8^3.

En hvilken som helst måte å dele opp potensen kan benyttes. Kanskje hadde vi for eksempel begynt med å observe at 8^6 ikke er for stort for kalkulatoren, og deretter funnet at

$$8^6 \equiv 64 \pmod{91}.$$

Da er

$$8^{12} = \left(8^6\right)^2 \equiv 64^2 \equiv 1 \pmod{91}.$$

Vi konkluderer at

$$8^{42} = \left(8^{12}\right)^3 \cdot 8^6 \cdot 8 \equiv 1 \cdot 64 \cdot 8 = 512 \equiv 57 \pmod{91}.$$

Konklusjon

Som sagt, erstatter vi alle heltallene

$$8^{43} \;\; 1^{43} \;\; 0^{43} \;\; 4^{43} \;\; 5^{43} \;\; 20^{43} \;\; 42^{43}$$

med heltall som er kongruent til dem modulo 91 men som er mindre enn like 91 og større enn eller like 0. Nå vet vi hvordan gjøre dette. Vi får:

$$57 \;\; 1 \;\; 0 \;\; 4 \;\; 47 \;\; 6 \;\; 42.$$

Er det riktig å få det samme heltallet som jeg begynte med?

I dette eksempelet får vi 4 når vi erstatter 4^{43} med et heltall som er kongruent til det modulo 91, og som er mindre enn 91 og større enn eller like 0. Det samme er tilfellet for 42. Er dette riktig?

Ja! Ikke bekymr deg for dette: det kan godt hende.

Imidlertid har du gjort noe feil om du får det samme heltallet fra to ulike heltall opphøyde i 31.

Oppsummering

Å kryptere er ikke noe dypt! Vi gjør følgende.

(1) Oversett fra symboler til heltall.

(2) Opphøy hvert heltall vi får etter å ha oversatt i det andre naturlige tallet i den offentlige nølkkelen til person B.

(3) Erstatt heltallene vi får etter å ha fullført (2) med heltall som er kongruent til dem modulo det første naturlige tallet i den offentlige nøkkelen til person B, og som er mindre enn dette naturlige tallet og større enn eller like 0.

Hva er en offentlig nøkkel for noe?

Å si at $(91, 43)$ er den offentlige nøkkelen til person B er å si:

(1) Det finnes et par primtall slik at vi får 91 når vi ganger dem. I dette eksempelet er de to primtallene 7 og 13.

(2) Vi har: $\mathsf{sfd}(43, (7-1)(13-1)) = 1$, altså $\mathsf{sfd}(43, 72) = 1$. Her er 7 og 13 de to primtallene fra (1).

Verken (1) eller (2) er viktig når vi krypterer: det er når vi dekrypterer at de er relevante.

Alle i verden vet den offentlige nøkkelen til person B, og dermed kan sende person B en melding som har blitt kryptert av RSA-algoritmen.

Oppgave 2

Person B har fått meldingen

$$57 \;\; 47 \;\; 9 \;\; 42$$

fra person A. Meldingen har blitt krypert av RSA-algoritmen. Den offentlige nøkkelen til person B er $(91, 43)$. Den private nøkkelen til person B er $(7, 13)$. Dekrypter meldingen.

Hva er en privat nøkkel for noe?

Dette består av de to primtallene som gir 91 når vi ganger dem: krav (1) ovenfor som må oppfylles av en offentlig nøkkel sier at det finnes et slikt par primtall. Rekkefølgen av primtallene i den private nøkkelen har ikke noe å si.

Hvordan løse oppgaven?

Hvordan dekryptere ligner mye på hvordan kryptere, men vi må først gjennomføre et steg til.

Hva er dette steget?

Vi må finne en invers til 43 modulo $(7-1)\cdot(13-1)$, altså modulo 72. Det vil si: vi ønsker å finne et naturlig tall x slik at

$$43x \equiv 1 \pmod{72}.$$

Hvordan gjør jeg det?

Å finne et slikt x er å løse en lineær kongruens. Se oversikten over hvordan gjøre dette. Husk at vi alltid kan benytte Euklids algoritme om vi ikke kommer fort til en annen måte å finne en løsning.

Vi kommer fram til at $x = -5$ er en løsning til kongruensen

$$43x \equiv 1 \pmod{72}.$$

Da må vi erstatte -5 med et naturlig tall som er kongruent til det modulo 72, for eksempel 67.

For å oppsummere: 67 er en invers til 43 modulo 72.

Noe vi må være klart over

Når vi finner inversen til 43, jobber vi modulo 72, ikke modulo 91. Ellers jobber vi modulo 91 når vi krypterer og dekrypterer.

Det andre kravet som må oppfylles av en offentlig nøkkel

Det er dette kravet som garanterer at

$$43x \equiv 1 \pmod{72}$$

har en løsning, altså at det finnes en invers til 43 modulo 7.

Hva gjør jeg når vi har funnet inversen til 43 modulo 91?

Opphøy alle de heltallene i meldingen i 67, altså i inversen til 43 modulo 72.

Vi får:

$$57^{67}\ \ 47^{67}\ \ 9^{67}\ \ 42^{67}.$$

Akkurat som når vi krypterer, må vi ersatte hvert av disse heltallene med et heltall som er kongruent til det modulo 91, og som er i tillegg mindre enn 91 og større enn eller likt 0.

Vi kommer fram til:

$$8\ \ 5\ \ 9\ \ 42.$$

Konklusjon

Nå oversetter vi fra heltall til symboler, ved å benytte Tabell 6.1 i forelesningsnotatene. Tabellen nedenfor viser oversettelsen.

Symbol	Tilsvarende heltall
8	H
5	E
9	I
42	!

Tabell 2: Oversettelsen av meldingen

Dermed er meldingen fra person A: «Hei!».

Oppsummering

Når vi dekrypterer, gjør vi følgende.

(1) Finn en invers modulo $(p-1)(q-1)$ til det andre naturlige tallet i den offentlige nøkkelen til person B, hvor (p, q) er den private nøkkelen til person B.

(2) Opphøy hvert heltall i den krypterte meldingen i inversen vi fikk i (1).

(3) Erstatt heltallene vi får etter å ha fullført (2) med heltall som er kongruent til dem modulo det første naturlige tallet i den offentlige nøkkelen til person B, og som er mindre enn dette naturlige tallet og større enn eller like 0.

Hvorfor virker dette?

Med andre ord: hvorfor får vi tilbake meldingen som har blitt kryptert når vi dekrypterer sånn? Dette følger fra Eulers teorem, som du kan lese om i forelesningsnotatene.

Hvorfor er RSA-algoritmen sikker?

Mens alle i verden vet den offentlige nøkkelen til person B, er det kun person B, eller noen person B stoler på, som vet hans eller huns private nøkkel. Noen som vet den private nøkkelen vet at det er 72 som vi bør jobbe mdoulo når vi finner inversen til 43, og deretter kan finne denne inversen og dekryptere meldingen.

Poenget er at, når vi har et produkt av to store primtall, finnes det ikke en effektiv algoritme for å komme fram til de to opprinnelige primtallene gitt produktet. Det er dette som fører til at RSA-algoritmen er sikke: hvis noen finner en effektiv algoritme for å komme fram til de to opprinnelige primtallene gitt produktet, blir RSA-algoritmen usikker, og en annen måte å kryptere og dekryptere meldinger må finnes!

Oppgave 3

Person B har fått meldingen

$$57 \;\; 47 \;\; 9 \;\; 42$$

fra person A. Meldingen har blitt krypert av RSA-algoritmen. Den offentlige nøkkelen til person B er $(91, 43)$. Knekk koden.

Hvordan løse oppgaven?

Den eneste forskjellen mellom denne oppgaven og Oppgave 2 er at den private nøkkelen til person B står ikke i oppgaven. Du må finne selv de to primtallene som gir 91 når vi ganger dem, altså 7 og 13. Deretter dekrypterer vi meldingen akkurat som i Oppgave 2.