RSA-KRYPTOGRAFI
TILLEGGSPENSUM I MA104

1. En generalisering av Eulers teorem

Lemma 1.1. *La a og n være hele tall, $n \geq 1$, og sett $d = \gcd(a, n)$. Da gjelder ekvivalensen*

$$\gcd(d, n/d) = 1 \Leftrightarrow a^{\phi(n)+1} \equiv a \pmod{n}$$

Bevis. Anta at $\gcd(d, n/d) = 1$. Da er også $\gcd(a, n/d) = 1$. [Hvis $r \geq 1$ er slik at $r|a$ og $r|(n/d)$, har vi at $r|a$ og $r|n$, det vil si $r|d$, men da gjelder $r|\gcd(d, n/d)$, og vi har $r = 1$.] Av Eulers teorem får vi da

$$a^{\phi(n/d)} \equiv 1 \pmod{n/d}$$

Men $\phi(n/d)|\phi(n)$ siden $(n/d)|n$ (se oppgave 13, seksjon 7.2 i Burton). Derfor blir

$$a^{\phi(n)} \equiv 1 \pmod{n/d}$$

eller

$$a^{\phi(n)} = 1 + k \cdot n/d$$

for passende $k \in \mathbb{Z}$. Multiplikasjon med a gir

$$a^{\phi(n)+1} = a + \frac{ka}{d} \cdot n$$

det vil si

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

som forlangt.

Anta omvendt at

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

holder. Vi setter $r = a/d$, $s = n/d$. Vi kan da skrive

$$a^{\phi(n)}dr = dr + hds$$

for passende $h \in \mathbb{Z}$. Dermed vil $s|r(a^{\phi(n)} - 1)$. Vi har at s og r er relativt primiske, følgelig gjelder $s|a^{\phi(n)} - 1$, det vil si

$$a^{\phi(n)} - 1 = ts$$

for passende $t \in \mathbb{Z}$. Det følger av denne formelen at hvis r' er en felles divisor for d og $s = n/d$, så vil $r'|1$, det vil si $\gcd(d, n/d) = 1$. □

Vi sier at et naturlig tall $n > 1$ er **kvadratfritt** hvis n ikke er delelig med noe kvadrattall større enn 1.

Oppgave. Vis følgende: n er kvadratfritt hvis og bare hvis $\gcd(d, n/d) = 1$ for enhver divisor d i n.

Dermed kan vi vise følgende:

Teorem 1.2. *La n være et naturlig tall, $n > 1$. Da gjelder $a^{\phi(n)+1} \equiv a \pmod{n}$ for alle heltall a hvis og bare hvis n er kvadratfritt.*

Bevis. Hvis n er kvadratfritt og a er et vilkårlig helt tall, får vi $\gcd(d, n/d) = 1$ der $d = \gcd(a, n)$, og lemmaet gir at $a^{\phi(n)+1} \equiv a \pmod{n}$ som forlangt.

Vi antar nå at $a^{\phi(n)+1} \equiv a \pmod{n}$ for alle heltall a. La p være en primfaktor i n. Med $a = p$ får vi

$$p^{\phi(n)+1} = p + kn$$

for passende k. Vi vet at $\phi(n) + 1 \geq 2$. Hvis vi derfor antar at $p^2 | n$, ser vi at vi får $p^2 | p$, en selvmotsigelse. Altså har vi $p^2 \nmid n$ for ethvert primtall p, og n er kvadratfritt. □

Merknad. Et primtall er selvsagt kvadratfritt, så hvis n er et primtall gir hvis-delen avdette teoremet at

$$a^n \equiv a \pmod{n}$$

for alle hele tall n, det vil si vårt resultat inneholder Fermats lille teorem som vårt spesialtilfelle.

2. Kryptografi - Anvendelse av Eulers teorem

Vi skal i dette avsnittet se nærmere på en anvendelse av tallteori innen kryptografi. Bakgrunnen er blant annet sikkerhetsproblemene knyttet til den masseoverføring av informasjon som er blitt mulig i vår elektroniske tidsalder. La oss for eksempel se på problemene til en storbank med 10 000 kunder som jevnlig har behov for å sende graderte opplysninger til banken. Den klassiske løsning ville her være å opprette et kurérsystem, men det er åpenbart at dette både praktisk og økonomisk er en håpløs ordning. En forbedring ville være at banken avtalte et kodesystem med hver enkelt kunde, men dette ville betinge at banken hadde et eget kodekontor og hadde kapasitet til å avholde de 10 000 nødvendige møtene med de aktuelle kunder for å kunne utveksle kodenøkler. En tredje mulighet (i vårt eksempel) er å la banken publisere **en** chiffreringsnøkkel (kodenøkkel) som kan brukes av **alle** til å sende meldinger til banken. Poenget er at en slik melding i praksis skal være umulig å dechiffrere for andre enn banken, dette til tross for at chiffreringsnøkkelen er offentlig kjent!

Den matematiske hovedideen som trengtes til å etablere et slikt system ble utviklet av Diffie, Merkle og Hellman i 1975.

Grunnideen er som følger: Meldingen som skal sendes omsettes først på avtalt og gjerne offentlig kjent måte til et naturlig tall M (hvis man for eksempel setter A= 01, B= 02, C= 03, ... og ønsker å sende ordet ABBA, blir M = 01020201). Man anvender en såkalt fall-lem-enveisfunksjon E på M og beregner $E(M)$. Poenget er nå at kjennskap

til $E(M)$ ikke er til praktisk nytte for å gjenvinne M på grunn av at det ikke er praktisk mulig å beregne inversfunksjonen til E uten å ha helt spesielle tilleggsopplysninger. Selvsagt er det i vårt eksempel bare banken som har disse. Den offentlig kjente chiffreringsnøkkel gir de opplysninger som trengs for å vite hvordan E ser ut og dermed hvordan $E(M)$, det chiffrerte budskap, ser ut. (E - første bokstav i det engelske *encipher* = chiffrere) Hva angår navnet fall-lem-enveisfunksjon (*trap door one-way function*) skulle anologien med personen som detter gjennom en fall-lem og ned i et lukket rom være klar nok. Uten ekstra informasjon (trykk på en bestemt murstein, skyv på et bestemt panel eller lignende) er det umulig å komme seg ut. Det er spesielt to slike fall-lem-enveissystemer som er blitt tatt i bruk. Det ene, utviklet av Merkle og Hellman ved Stanford university, er det såkalte ryggsekksystemet (*knapsack system*): Poenget er her at sender danner en sum M ved hjelp av addender fra en mengde $\{a_1, a_2, \ldots, a_m\}$ av naturlige tall og sender summen M. For den som vil bryte koden er det nødvendig å gjenvinne de addender som inngår i summen. Det andre systemet, som vi skal studere mer i detalj, ble utviklet i 1977 [1] av Rivest, Shamir og Adleman ved Massachusetts Institute of Technology (MIT), vi skal kalle det **RSA-systemet** etter opphavsmennene. Det er til nå ingen som har greidd å knekke RSA-systemet, mens Shamir selv viste i 1982 at ryggsekksystemet var løsbart, det vil si at M kunne beregnes ut fra $E(M)$ **uten** tilleggsinformasjon med rimelig bruk av datamaskintid.

Før vi går løs på RSA-systemet skal vi gjøre unna en enkel formalitet: For å oversette meldinger til tall, vil vi bruke følgende alfabetoversettelse:

Blank/mellomrom= 00, A= 01, B= 02, C= 03, D= 04, E= 05, F= 06, G= 07, H= 08, I= 09, J= 10, K= 11, L= 12, M= 13, N= 14, O= 15, P= 16, Q= 17, R= 18, S= 19, T= 20, U= 21, V= 22, W= 23, X= 24, Y= 25, Z= 26.

Dette kan selvsagt fortsettes for å få med andre tegn, sifre, med mere. Denne alfabetoversettelsen er offentlig og tjener kun en hensikt: å konvertere et budskap til et tall. Det klassiske Shakespeare-sitatet

IT'S ALL GREEK TO ME

overføres eksempelvis til

$$M = 09201900011212000718050511002015001305$$

eller hvis vi for leselighetens skyld bryter det opp i blokker på 4 sifre og eventuelt etterfyller siste blokk med en blank (00):

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

[1] I følge nye opplysninger som har kommet fram så oppdaget britiske matematikere som jobbet for topp hemmelige Government Communications Headquarters denne metoden allerede i 1973.

2.1. **RSA-systemet.** Den som ønsker å motta chiffererte meldinger, person **A**, velger to primtall p og q og danner $n = p \cdot q$. Da n skal offentliggjøres mens p og q hemmeligholdes, velges p og q av størrelsesorden 10^{100}. For n av størrelsesorden 10^{200} vil det med dagens raskeste datamaskiner ta millioner av år å faktorisere n. (Vi skal selvsagt i eksempler og oppgaver holde oss til små verdier av n slik at vi ikke drukner i regning.) **A** finner så $\phi(n)$:

$$\phi(n) = (p-1)(q-1)$$

Han velger så et naturlig tall e slik at $1 < e < \phi(n)$ og $\gcd(\phi(n), e) = 1$. Ligningen

$$ex \equiv 1 \pmod{\phi(n)}$$

har da en entydig løsning d, $1 < d < \phi(n)$. **A** regner ut denne d. **A** bør velge e slik at d blir relativt stor (forklaring kommer nedenfor).

A plasserer så $\{n, e\}$ som offentlig chiffreringsnøkkel i et offentlig register. Den hemmelige dechiffreringsnøkkelen $\{n, d\}$ beholder han for seg selv.

Den som vil sende en melding M til **A** leter nå opp $\{n, e\}$ i det offentlige registeret og beregner $E(M) = N$ som det entydig bestemte tall N slik at

$$M^e \equiv N \pmod{n}$$

med $0 \leq N < n$. Så sendes N til **A**. **A** dechiffrerer nå på følgende måte: Han beregner $D(N)$ som det entydige bestemte tall slik at

$$N^d \equiv D(N) \pmod{n}$$

med $0 \leq D(N) < n$. Vi skal om et øyeblikk vise at $D(N)$ uten vansker leder oss tilbake til M, **vi får alltid** $D(N) = M$**.** Vi gjør først en praktisk observasjon: Vi må ha $0 \leq M < n$ for å unngå flertydighet. Er M større enn eller lik n, bryter vi M opp i mindre blokker (jamfør eksempelet foran): $M_1, M_2, \ldots, M_k$ og sender $E(M_1), E(M_2), \ldots, E(M_k)$. La oss nå i det følgende anta at $M < n$.

2.2. **Riktighet av dechiffrering.** Vi minner om den generaliserte versjonen av Eulers teorem: $a^{\phi(n)+1} \equiv a \pmod{n}$ for alle heltall a hvis og bare hvis n er kvadratfritt. Multipliserer vi her begge sider med $a^{\phi(n)}$ får vi

$$a^{2\phi(n)+1} \equiv a^{\phi(n)+1} \equiv a \pmod{n}$$

Et enkelt induksjonsbevis gir oss generelt

$$a^{k\phi(n)+1} \equiv a \pmod{n}$$

for alle $k \geq 1$.

I RSA-systemet er n kvadratfri da n er produkt av to forskjellige primtall. Vi har $ed \equiv 1 \pmod{\phi(n)}$, det vil si $ed = k\phi(n) + 1$ for en passende $k \geq 1$. Formelen over gir da straks

$$D(N) \equiv N^d \equiv M^{ed} \equiv M^{k\phi(n)+1} \equiv M \pmod{n}$$

Siden $0 \leq M < n$ og $0 \leq D(N) < n$, følger det straks at $D(N) = M$.

Merknad. Det er viktig at tallet d er stort slik at en utenforstående ikke kan bryte koden ved å suksessivt å sjekke $N^2 \pmod{n}$, $N^3 \pmod{n}$, $N^4 \pmod{n}$, ... og i løpet av kort maskintid få ut et budskap med mening. Derfor er den fornuftige framgangsmåten **først** å velge en **stor** $d < \phi(n)$ slik at $\gcd(d, \phi(n) = 1$ og deretter bestemme e slik at $e \cdot d \equiv 1 \pmod{\phi(n)}$

Hvis man ønsker å bryte RSA-systemet, er det nødvendig å bestemme d. Dette greier vi hvis vi kan faktorisere n eller finne $\phi(n)$. Å finne $\phi(n)$ er essensielt like vanskelig som å finne p og q i lys av følgende: p og q er kjent hvis og bare hvis $\phi(n)$ er kjent. (Kjenner vi $\phi(n)$ kan vi finne p og q fra uttrykkene $p + q = n - \phi(n) + 1$ og $(p - q)^2 = (p + q)^2 - 4n$.)

Heller ikke ser det ut til å være noen snarvei til å finne d; dette ser ut til å være like vrient somå faktorisere n. Det lar seg vise at p og q kjent er ekvivalent med at et multiplum $k\phi(n)$ er kjent ($k \geq 1$). (Kjenner vi e og d er jo $ed - 1 = k\phi(n)$ for passende k.) Så matematisk sett er kjennskap til den hemmelige nøkkelen $\{n, d\}$ ekvivalent med kjennskap til p og q.

2.3. **Talleksempel.** La oss se på et talleksempel der vi har valgt p og q så små at en vanlig kalkulator ikke blir overanstrengt.

La $p = 47$, $q = 59$, $n = p \cdot q = 2773$. Vi har $\phi(n) = 46 \cdot 58 = 2668$. **A** velger $d = 157$. Vi har at d er primtall, $p < d$ og $q < d$ (og $d < 1668$), så $\gcd(d, \phi(n)) = 1$. Vi bestemmer så e, $1 < e < \phi(n)$, slik at

$$157 \cdot e \equiv 1 \pmod{2668}$$

Vi har nå $2668 = 16 \cdot 157 + 156$, $157 = 1 \cdot 156 + 1$ og dermed

$$1 = 17 \cdot 157 - 2668$$

Av dette får vi straks $e = 17$.

Den offentlige nøkkelen til **A** er altså $\{2773, 17\}$, mens den hemmelige nøkkelen er $\{2773, 157\}$.

Her er p og q valgt slik at vi for enkelhets skyld i dette eksempelet kan sende meldinger i blokker på 4 sifre (2 bokstaver), vi har jo ZZ= $2626 < 2773$. hvis vi derfor vil sende

IT'S ALL GREEK TO ME

til **A**, må vi sende $E(0920)$, $E(1900)$, $E(0112)$, $E(1200)$, $E(0718)$, $E(0505)$, $E(1100)$, $E(2015)$, $E(0013)$, $E(0500)$.

Første M-verdi er altså $M = 920$. Litt regning gir oss

$$920^{17} \equiv 948 \pmod{2773}$$
$$1900^{17} \equiv 2342 \pmod{2773}$$
$$112^{17} \equiv 1084 \pmod{2773}$$
$$200^{17} \equiv 1444 \pmod{2773}$$
$$718^{17} \equiv 2663 \pmod{2773}$$
$$505^{17} \equiv 2390 \pmod{2773}$$
$$1100^{17} \equiv 778 \pmod{2773}$$
$$2015^{17} \equiv 774 \pmod{2773}$$
$$13^{17} \equiv 219 \pmod{2773}$$
$$500^{17} \equiv 1655 \pmod{2773}$$

A mottar altså følgende $N = E(M)$-verdier: 940, 2342, 1084, 1444, 2663, 2390, 778, 774, 219, 1655.

A anvender så dechiffreringsnøkkelen, det vil si $\{n, d\}$ og beregner

$$948^{157} \equiv 920 \pmod{2773}$$

det vil si $D(948) = 920$,

$$2342^{157} \equiv 1900 \pmod{2773}$$

så $D(2342) = 1900$, og videre $D(1084) = 112$, $D(1444) = 1200$, $D(2663) = 718$, $D(2390) = 505$, $D(778) = 1100$, $D(774) = 2015$, $D(219) = 13$, $D(1655) = 500$. **A** får rekonstruert meldingen ved hjelp av 00 =blank, 01 =A, og så videre.

Merknad. I praksis må man selvsagt aldri sende et budskap brutt opp i 4-siffers-blokker, for da kan den chiffrerte melding dechiffreres **uten** kjennskap til d ved å beregne $E(0001)$, $E(0002)$, ..., $E(2626)$, i alt 728 kalkulasjoner, og så bruke lista som kommer fram som leksikon.