1 Oppgaver i 11174 Datasikkerhet til uke 39

Et utvalg av disse oppgavene vil bli gjennomgått torsdag 26.09.02 kl. 12.15-13.00.

Oppgave 1

(a) Finn alle løsningene til kongruenslikningen $8x \equiv 4 \pmod{28}$.

(b) Finn $\gcd(1529, 14039)$ ved å bruke Euklids algoritme.

(c) Bruk Euklids algoritme til å finne $17^{-1} \mod 101$.

(d) Lag en multiplikasjonstabell for $\mathbb{Z}_{18}^*$.

(e) Finn $155 \mod 19$ og $-221 \mod 23$.

(f) Finn $\text{ind}_{6,11}7$.

Oppgave 2

Anta at vi koder det engelske alfabetet på følgende måte: A er 0, B er 1, ..., Z er 25, og at vi krypterer meldinger tegn for tegn ved å bruke formelen $f(x) = (7x + 10) \mod 26$. (Dette betyr at hvis x er koden til en bokstav i klartekstmeldingen, så er $f(x)$ koden til det tilsvarende tegnet i den krypterte meldingen.)

(a) Krypter ordet MEET ved hjelp av denne krypteringsformelen.

(b) Finn dekrypteringsfunksjonen $g(y)$. (Dette er den inverse funksjonen til $f(x)$, dvs. hvis $y = f(x)$, så er $x = g(y)$. Likningen $y = (7x + 10) \mod 26$ skal altså løses med hensyn på x.)

(c) Sjekk om dekrypteringsfunksjonen er riktig ved å anvende den på den krypterte versjonen av MEET. (Da skal du få tilbake meldingen MEET.)

Oppgave 3

Denne oppgaven er et lite regneeksempel i bruk av RSA-krypteringsmetoden. Først litt generelt om RSA-krypteringsmetoden: Ola Nordmann velger seg et tallpar (n, e) hvor n er et produkt av to primtall p og q, og e er et helt tall slik at $\gcd(e, \phi(n)) = 1$. (For at RSA-systemet skal være sikkert, må n og e tilfredstille en del tilleggsbetingelser, men dette tar vi ikke hensyn til her). Tallparet (n, e) kalles for krypteringsnøkkelen til Ola Nordmann fordi alle som skal sende en kryptert melding til Ola Nordmann ved hjelp av RSA, må bruke tallparet (n, e). Ola Nordmann offentliggjør (n, e) slik at alle som ønsker det, skal kunne sende en kryptert melding til ham. Så beregner han dekrypteringsnøkkelen d og holder denne hemmelig slik at bare han kan dekryptere krypterte meldinger.

Krypteringen skjer da blokk for blokk ved bruk av følgende formel

$$C = M^e \mod n$$

hvor M er koden til den blokken vi krypterer, og C er koden til det tilsvarende blokken i den krypterte meldingen.

Dekrypteringen skjer blokk for blokk ved bruk av formelen

$$M = C^d \mod n$$

hvor d er dekrypteringsnøkkelen, C er koden til ei blokk i den krypterte meldingen, og M er koden til den tilsvarende blokken i den opprinnelige meldingen.

Hvis $d = e^{-1} \mod \phi(n)$, har vi at

$$C^d \equiv (M^e)^d \equiv M^{1+k\phi(n)} \equiv M \cdot \left(M^{\phi(n)}\right)^k \equiv M \pmod{n}$$

ifølge Eulers teorem. Dette viser at vi får tilbake den originale meldingen når vi dekrypterer den krypterte meldingen.

I vårt regneeksempel lar vi $n = 2537$, $e = 13$, og vi lar hver blokk bestå av to bokstaver og koder hver bokstav som i oppgaven ovenfor. Da koder vi ST som 1819 og OP som 1415.

(a) Faktoriser tallet n.

(b) Krypter meldingen STOP. Her er det en fordel å bruke algoritmen for hurtig modular eksponensiering på side 176-177 i læreboka. Denne algoritmen går i korthet ut på å skrive eksponenten som en sum av toerpotenser og regne ut grunntallet opphøyd i en toerpotens ved gjentatt kvadrering. F.eks. er

$$a^{17} = a^{2^4+2^0} = a^1 \cdot a^{2^4} = a \cdot \left(\left((a^2)^2\right)^2\right)^2.$$

For hver multiplikasjon eller kvadrering reduserer vi modulo n slik at vi aldri behøver å regne med større tall enn $(n-1)^2$.

(c) Finn dekrypteringsnøkkelen $d = e^{-1} \pmod{\phi(n)}$.

(d) Dekrypter den krypterte meldingen du fant i (a), dvs. vis at vi får tilbake den originale meldingen STOP. NB! Her er det helt nødvendig å bruke algoritmen for hurtig modular eksponensiering!

Bemerkning: I vårt regneeksempel er n produktet av primtallene $p = 43$ og $q = 59$. For at RSA-krypteringen skal gi tilstrekkelig sikkerhet, dvs. være (nesten) umulig å knekke, må primtallene p og q ha minst 100 desimal sifre og tilfredstille en del tillegsbetingelser, og de må være hemmelige. (Hvis en kjenner p og q i tillegg til den offentlige nøkkelen (n, e) er det lett å regne ut dekrypteringsnøkkelen d.) I tillegg er det viktig at antallet forskjellige verdier M kan anta, er (nesten) like stort som n; noe som oppnås ved at vi bruker blokker med mange tegn når vi krypterer.