NTNU
Institutt for matematiske fag

TMA4140
Diskret matematikk

Plenumsregning 8

Høst 2024

1 Regn ut dekrypteringsnøkkelen for en RSA-instans med $p = 6737$, $q = 7079$ og eksponent $e = 3$ og krypter beskjeden 4140.

2 Vi skal samle inn en meningsmåling om hvilket TMA-emne ved NTNU som er mest interressant og bestemmer oss for å bruke RSA for å holde ting skjult fra utenomforstående. Vi setter $e = 3$ og genererer n som produktet av to store tilfeldige primtall p og q slik at $3 \nmid (p-1)(q-1)$ og regner ut d som den modulære inversen til e modulo $(p-1)(q-1)$. Deltagerene bruker den firesiffrede fagkoden m og regner ut $c = m^e$ som de sender til oss.

a) Ta rollen som en av deltagerene. La oss si at du finner c til en av de andre deltagerene. Drøft hvordan du kan prøve å finne ut hvilket fag vedkommende har valgt.
(Hint: Se hva som skjer hvis du simulerer en meningsmåling med tre deltakere og to mulige fagkoder)

b) Hva gjør at angrepet fungerer? Kan du gjøre noe med m før kryptering for å hindre angrepet?

3 Når vi velger primtall for RSA er det viktig at disse er tilfeldige slik at de ikke kan gjettes. Det tar tid å generere tilfeldighet, så det er fristende å spare litt på dette, for eksempel ved å kun generere det første primtallet tilfeldig og så velge det neste påfølgende primtallet.

a) La $q = k + p$ hvor q og p er ukjente primtall og k er et kjent partall. Forklar hvordan du kan faktorisere $n = pq$.

b) La p være et tilfeldig primtall og q det neste primtallet etter p. Hvordan kan vi prøve å faktorisere $n = pq$? (Hint: Avstanden mellom nabo-primtall er i gjennomsnitt liten sammenlignet med primtallene)

4 I denne oppgaven bruker vi notasjonen

$$\prod_{p|n} f(p),$$

som er produktet av $f(p)$ for alle unike primtallsfaktorer p av n. Vi har for eksempel at

$$12 \prod_{p|12} \left(1 - \frac{1}{p}\right) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

a) Vis at hvis $n = p_1^{k_{p_1}} \cdot p_2^{k_{p_2}} \cdot \ldots \cdot p_r^{k_{p_r}}$ for forskjellige primtall p_i så er

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

hvor $\prod_{p|n}$ er produktet over alle primtallsdivisorer p av n.

b) Vis at

$$\gcd(a, b)\phi(a)\phi(b) = \phi(\gcd(a, b))\phi(ab)$$

for alle positive heltall a og b.