NTNU
Institutt for matematiske fag

TMA4140
Diskret matematikk

Øving 6

Høst 2023

Øvingen skal leveres inn digitalt på OVSYS, som én enkelt .pdf-fil.

1 I denne oppgaven skal du analysere et primitivt krypto-system for at Alice, som befinner seg i Singapore, og Bob som befinner seg i London, skal kunne dele en kode/nøkkel uten at det skal være lett for andre (Eva) å oppdage den.

Planen til Alice og Bob er som følgende. Alice skriver et stort antall lapper, alle med hvert sitt unike tall, og pakker dem inn i bokser. Hun nummererer så boksene og kontraherer et kontainerskip for å sende dem til London.

Når skipet ankommer London, velger Bob på tilfeldig vis en av boksene på skipet, for eksempel boks nummer i, og leser tallet som står skrevet på lappen i boksen. La oss si at dette tallet er k. Bob lukker så boksen igjen før han informerer kapteinen på skipet at han skal kommunisere tallet k til Alice. Da vil nemlig Bob og Alice begge dele koden i. Straks båten er tilbake i Singapore og Alice får vite tallet k vet hun også i, da hun husker hvor hun puttet lappene sine. Siden ingen så hvilken boks Bob åpnet, er det ikke noe farlig at tallet k kommer på aveie - så lenge Alice faktisk får vite tallet til slutt.

På vei tilbake til Singapore blir skipet kapret av den beryktede piraten Enarmede Eva. Kapteinen blir tvunget til å fortelle oppdraget sitt, men kan ikke hjelpe piraten med å finne tallet i, siden han bare kjenner k. Kapteinen forteller likevel hvilken strategi Alice og Bob ble enig om å bruke.

Eva tenker seg om og finner ut at den eneste måten hun kan finne i på er å åpne boksene helt til hun finner den som har lappen k inni seg.

a) Gitt at det er b bokser om bord og det tar t sekunder å åpne en boks, hvor lang tid vil det i snitt ta for piraten Eva å finne det hemmelige tallet i, om hun tilfeldig åpner boks etter boks helt til hun finner den som har lappen med tallet k inni seg?

b) Det tar rundt 6 uker for et vanlig kontainerskip å ta seg fra London til Singapore. Alice er på forhånd bekymret for at Eva kanskje vil kapre skipet på hjemturen fra London til Singapure. Samtidig vet hun at Bob nekter å bruke mer enn en time på å åpne en enkelt boks. Gitt at Bob og Alice er like kompetente boks-åpnere, hvor mange bokser ville du rådet Alice til å shippe til London, slik at Eva sannsynligvis ikke klarer å finne koden før skipet er trygt tilbake i havn i Singapore?

2 Denne oppgaven handler om Diffie-Hellman protokollen. Denne protokollen gir en mye bedre nøkkelutvekslingsalgoritme enn den upraktiske diskutert i oppgave 1 - men målet er det samme. Alice og Bob skal bli enig om et tall som det er vanskelig, men ikke umulig, for Eva å finne.

Det kan være lurt å se på side 3 og 4 i notatet om kryptologi før du løser denne oppgaven.

For å utføre Diffie-Hellmann må vi bestemme to paramtre q og g, hvor q er et primtall og g er et heltall mellom 2 og $q-2$. Disse tallene er begge offentlig kjent.

Her bruker vi tallene $q = 101$ og $g = 2$.

Under får du noen tall som kan være nyttige i diverse utregninger du må gjøre. Gitt tallene under garanterer vi at resten av oppgaven fint kan løses for hånd. Du er likevel veldig velkommen til bruke for eksempel Python eller andre digitale verktøy.

$$2^{68} \,\%\, 101 = 52 \tag{1}$$

$$2^{40} \,\%\, 101 = 36 \tag{2}$$

$$B^{34} \,\%\, 101 = 58 \tag{3}$$

$$A^{19} \,\%\, 101 = 28 \tag{4}$$

a) Si at Alice først trekker tallet $a = 69$. Regn ut $2^{69} \,\%\, 101$, (se om du kan bruke ligningene over til hjelp), og kall dette tallet A. Alice sender nå A til Bob, og vi antar at Eva kan lese av A.

b) Bob mottar A og trekker selv et tall $b = 38$. Regn ut $2^{38} \,\%\, 101$, kall dette tallet B. Bob sender så B til Alice, og Eva kan også lese dette tallet.

c) Alice regner nå ut $B^{69} \,\%\, q$. Vi kaller dette tallet K. Finn K.

d) Bob kan også regne ut K, som $A^{38} \,\%\, q$. Bekreft at

$$A^{38} \,\%\, q = B^{69} \,\%\, q$$

enten ved å bruke kongurensregning eller å ved å regne ut $A^{38} \,\%\, q$ og dermed sjekke likheten.

e) Eva vil nå prøve å regne ut K. Hun kjenner tallene A, B samt tallene $q = 101$ og $g = 2$. La oss si at hun har tilgang til et dataprogram P som lar henne regne ut diskrete logaritmer. Forklar hvordan hun ved hjelp av P kan regne ut K.