Eksamen i TMA4155 Kryptografi Intro — Høst 2004
Løsningsforslag

1 Frekvensanalyse forteller oss at J mest sannsynlig går til E. Det er to ord på tre bokstaver is chifferteksten, og hintet gir oss tre muligheter. Ordet RJI inneholder sannsynligvis bokstaven E, som passer med forslagene DER og MED.

Vi prøver hypotesen RJI=MED. Vi ser at bokstavene D og E tas til I og J, altså at to etterfølgende klartekstbokstaver går til etterfølgende chiffertekstbokstaver. Dermed er det naturlig å tenke på Cæsarchifferet. En kjapp telling gir et skift på 5, og dekrypteringen blir

LYKKE TIL MED RESTEN AV EKSAMEN

2a Vi ser at $p = 47$ er et primtall, og at $p - 1 = 2 \cdot 23$. Vi foreslår $g = 4$. Siden ordenen til et tall modulo et primtall p må dele $p-1$, kan 4 ha ordenen 1, 2, 23 eller 46 modulo 47. Ordenen kan ikke være 1 siden $4 \not\equiv 1 \pmod{47}$. Siden $4 = 2^2$ må $4^{23} \equiv 2^{2 \cdot 23} \equiv 2^{46} \equiv 1 \pmod{47}$. Derfor har 4 orden 23 modulo 47.

2b Alice og Bob har blitt enige om felles parametre p og g. Alice velger seg et tilfeldig tall a i $\{0, \ldots, p-1\}$, regner ut $x \equiv g^a \pmod{p}$ og sender x til Bob. Samtidig velger Bob et tilfeldig tall b i $\{0, \ldots, p-1\}$, regner ut $y \equiv g^b \pmod{p}$ og sender y til Alice. For å finne den delte hemmeligheten z regner Alice ut $z \equiv y^a \pmod{p}$ mens Bob regner ut $z \equiv x^b \pmod{p}$.

Alice velger $a = 7$ og regner ut $x \equiv 4^7 \equiv 28 \pmod{47}$. Bob velger $b = 11$ og regner ut $y \equiv 4^{11} \equiv 24 \pmod{47}$. Så regner Alice ut $24^7 \equiv 18 \pmod{47}$, mens Bob regner ut $28^{11} \equiv 18 \pmod{47}$.

2c I et mann-i-mellom-angrep sitter angriperen mellom Alice og Bob, og alle meldinger de sender går via angriperen. Når Alice sender x til Bob og Bob sender y til Alice stanser angriperen meldingene.

I stedet velger angriperen a' og b' tilfeldig fra $\{0, \ldots, p-1\}$, sender $x' \equiv g^{a'} \pmod{p}$ til Bob og $y' \equiv g^{b'} \pmod{p}$ til Alice. Alice eller Bob har ingen mulighet til å skille disse meldingen fra hva de egentlig forventet og godtar meldingene.

Alice vil nå regne ut den delte hemmeligheten $z_A \equiv (y')^a \equiv x^{a'} \mod p$, så angriperen kjenner z_A. Bob, derimot, vil regne ut den delte hemmeligheten $z_B \equiv (x')^b \equiv y^{b'} \mod p$, så angriperen kjenner z_B.

Angriperen kan nå dekryptere alt Alice krypterer med den delte hemmeligheten z_A, og rekryptere det ved hjelp av den delte hemmeligheten z_B, slik at Bob tror det kom fra Alice. Og omvendt.

3a Vi velger et tilfeldig tall 2 og vil først gjøre arbeid $B = 2$. Vi må altså regne ut $x \equiv 2^{2^8} \pmod{493}$, og deretter se om $\gcd(x-1, 493)$ er 1 eller en faktor i 493.

Vi får $2^{2^0} \equiv 2 \pmod{493}$, $2^{2^1} \equiv 4 \pmod{493}$, $2^{2^2} \equiv 16 \pmod{493}$, $2^{2^3} \equiv 256 \pmod{493}$, $2^{2^4} \equiv 460 \pmod{493}$, $2^{2^5} \equiv 103 \pmod{493}$, $2^{2^6} \equiv 256 \pmod{493}$, $2^{2^7} \equiv 460 \pmod{493}$ og $2^{2^8} \equiv 103 \pmod{493}$

Til slutt er $\gcd(102, 493) = 17$, så $493 = 17 \cdot 29$.

3b Vi vet at $n = pq$, og at $ed \equiv 1 \pmod{(p-1)(q-1)}$. Dette er sammenhengen mellom n, e og d.

En passende d er da 299.

3c Digitale signaturer er en merkelapp på et elektronisk dokument som er lett å verifisere ved hjelp av en offentlig nøkkel, og lett å lage med en privat nøkkel. Det skal være vanskelig å lage en signatur som verifiserer på en ny melding uten å kjenne den private nøkkelen (en forfalskning), selv om man kjenner mange andre gyldige signaturer.

Vi kan bruke RSA til å signere en melding $m \in \{0, \ldots, n-1\}$ ved å regne ut signaturen $s \equiv m^d \pmod{n}$. Enhver som kjenner den offentlige nøkkelen kan sjekke at signaturen er riktig ved å sjekke at $m \equiv s^e \pmod{n}$.

For å signere meldingen $m = 2$ må vi regne ut $s \equiv 2^{299} \pmod{493}$. Vi bruker $299 = 256 + 32 + 8 + 2 + 1$ og fra utregningene i deloppgave a. finner vi at

$$2^{299} \equiv 103 \cdot 103 \cdot 256 \cdot 4 \cdot 2 \equiv 229 \pmod{493}.$$

4a Vi får

$$\begin{aligned} g^{u_1} y^{u_2} &\equiv g^{s^{-1}m} g^{as^{-1}r} \equiv g^{km(m+ar)^{-1} + kar(m+ar)^{-1}} \\ &\equiv (g^k)^{(m+ar)(m+ar)^{-1}} \equiv g^k \pmod{p}. \end{aligned}$$

Derfor er $g^{u_1} y^{u_2} \bmod p \equiv r \pmod{q}$.

4b Vi har signaturene (m_1, r_1, s_1) og (m_2, r_2, s_2), og observerer at $r_1 = r_2 = 3152$. Det betyr at samme tilfeldige tall k ble brukt til å lage de to signaturene, med meget stor sannsynlighet.

Vi får altså ligningene $s_1 \equiv k^{-1}(m_1 + ar) \pmod{q}$ og $s_2 \equiv k^{-1}(m_2 + ar) \pmod{q}$. Det er to ligninger med to ukjente (a og k^{-1}). Vi finner at $s_2 - s_1 \equiv k^{-1}(m_1 - m_2) \pmod{q}$, eller $k^{-1} \equiv 662 - 4401 \equiv 1264 \pmod{5003}$.

Setter vi inn for k^{-1} får vi at $a \equiv (ks_1 - m_1)r^{-1} \pmod{q}$. En invers til k er 1888 og en invers til r er 2738. Det gir oss $a \equiv (1888 \cdot 4401 - 17) \cdot 2738 \equiv 4444 \pmod{5003}$.

5a En MAC (Message Authentication Code) er en merkelapp på et melding som lages av en MAC-algoritme som tar inn en hemmelig nøkkel sammen med meldingen. Det skal være vanskelig å lage en MAC på en ny melding uten å kjenne den private nøkkelen (en forfalskning), selv om man kjenner mange andre MAC-verdier for samme hemmelige nøkkel.

5b Hvis man kjenner MAC-verdien $MAC(k, m)$ til meldingen $m = m_1 \in \{0,1\}^n$ (meldingen består av bare én blokk) kan man lett finne MAC-verdien til meldingen $m' = m_1||m_2 \in \{0,1\}^{2n}$ (meldingen består av to blokker), siden $MAC(k, m') = h'(h'(k, m_1), m_2) = h'(MAC(k, m), m_2)$. Derfor er MAC-algoritmen usikker.