Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 10

Eksamen H2016 oppgave 3 Vi skal lage et RSA-nøkkelpar der vi bruker $p = 89$ og $q = 157$ som de to hemmelige primtallene og $e = 5$ som krypteringseksponent. Vi setter $n = pq = 13973$ og får $\phi(n) = (p-1)(q-1) = 13728$. Vi finner en invers til e modulo $\phi(n)$ ved Euklids algoritme:

$$\begin{aligned} 13728 &= 2745 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned} \qquad \begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2(13728 - 2745 \cdot 5) - 5 \\ &= 2 \cdot 13728 - 5491 \cdot 5 \end{aligned}$$

Vi ser at -5491 er en invers til 5 modulo 13728. Siden vi skal ha $0 < d < \phi(n)$ får vi $d = -5491 + 13728 = 8237$. Den offentlige nøkkelen er $(n, e) = (13973, 5)$. Den private nøkkelen kan skrives enten som $(p, q, d) = (89, 157, 8237)$ eller som $(n, d) = (13973, 8237)$.

Eksamen H2017 oppgave 4 Modulusen er $n = pq = 37 \cdot 53 = 1961$, og dekrypteringseksponenten er $d = 41$. Det vi må regne ut er $c^d \pmod{n}$, det vil si $310^{41} \pmod{1961}$. Vi kan skrive dekrypteringseksponenten som en sum av potenser av 2 slik:

$$d = 41 = 2^5 + 2^3 + 2^0$$

Det betyr at $310^{41} = 310^{32} \cdot 310^8 \cdot 310$, altså holder det at vi regner ut 310 opphøyd i $2^1, 2^2, 2^3, 2^4$ og 2^5 modulo 1961:

$310^2 \equiv 96100 \equiv 11 \pmod{1961}$

$310^4 \equiv 11^2 \equiv 121 \pmod{1961}$

$310^8 \equiv 121^2 \equiv 14641 \equiv 914 \pmod{1961}$

$310^{16} \equiv 914^2 \equiv 835396 \equiv 10 \pmod{1961}$

$310^{32} \equiv 10^2 \equiv 100 \pmod{1961}$

Dermed får vi at

$$c^d \equiv 310^{41} \equiv 310^{32} \cdot 310^8 \cdot 310 \equiv 100 \cdot 914 \cdot 310 \equiv 1472 \pmod{1961}$$

Altså er den dekrypterte meldingen 1472.

Eksamen H2014 oppgave 5 Den offentlige krypteringsnøkkelen til person B er $(n, e) = (187, 53)$. Vi ser at $n = 187 = 11 \cdot 17$, så $p = 11$ og $q = 17$. Dermed kan vi regne ut $\phi(n) = (p-1)(q-1) = 10 \cdot 16 = 160$. Dette kan vi bruke til å finne dekrypteringseksponenten d, som er gitt ved at $ed \equiv 1 \pmod{160}$. Vi kunne benyttet Euklids algoritme, men vi kan også se direkte at $53 \cdot 3 = 159$, som er kongruent med -1

modulo 160. Dermed er $53 \cdot (-3) \equiv 53 \cdot 157 \equiv 1 \pmod{160}$, så dekrypteringsnøkkelen er $d = 157$.

Så for å finne den dekrypterte meldingen må vi regne ut $25^{157} \pmod{187}$. Her kan vi bruke hintet fra oppgaven, som var at $25^7 \equiv (-2) \pmod{187}$. Det betyr nemlig at:

$$25^{157} \equiv (25^7)^{22} \cdot 25^3 \equiv (-2)^{22} \cdot 25^3 \equiv 81 \cdot 104 \equiv 9 \pmod{187}$$

Når vi oversetter 9 til et symbol ved hjelp av tabellen som er oppgitt på eksamen, får vi at den dekrypterte meldingen svarer til symbolet I.

Eksamen K2019 oppgave 7 **a)**

I den offentlige krypteringsnøkkelen $(n, e) = (209, 49)$ er $n = pq$ gitt ved produktet av to primtall. Vi ser at $209 = 11 \cdot 19$, som betyr at $p = 11$ og $q = 19$. Nå er dekrypteringseksponenten d gitt som inversen til e modulo $\phi(n) = (10 \cdot 18) = 180$. Altså finner vi d ved å løse kongruensen $49d \equiv 1 \pmod{180}$.

$$\begin{aligned} 180 &= 3 \cdot 49 + 33 & \qquad 1 &= 33 - 2 \cdot 16 \\ 49 &= 1 \cdot 33 + 16 & &= 33 - 2(49 - 33) = 3 \cdot 33 - 2 \cdot 49 \\ 33 &= 2 \cdot 16 + 1 & &= 3(180 - 3 \cdot 49) - 2 \cdot 49 \\ 16 &= 16 \cdot 1 + 0 & &= 3 \cdot 180 - 11 \cdot 49 \end{aligned}$$

Dermed ser vi at -11 er en invers til 49 modulo 180, og vi får at $d = -11 + 180 = 169$. Den hemmelige dekrypteringseksponenten er altså 169.

b)

Hvis (n, e) er den offentlige krypteringsnøkkelen og (n, d) er den hemmelige dekrypteringsnøkkelen, så har vi per konstruksjon at $de \equiv 1 \pmod{\phi(n)}$. Det betyr at det finnes et heltall k slik at $de = k\phi(n) + 1$. Merk at $k \geq 1$ siden $d > 1$ og $e > 1$ per antakelse. Siden $n = pq$, hvor p og q er ulike primtall, er n et kvadratfritt naturlig tall. Dermed kan vi bruke hintet som er gitt i oppgaven til å si at

$$(M^e)^d \equiv M^{de} \equiv M^{k\phi(n)+1} \equiv M \pmod{n},$$

som var det vi ville vise.