RSA - oppsummert

Lage systemet:

(1) Velg to ulike primtall p og q, dann tallet $n = pq$

(2) Velg et tall $1 < e < \phi(n) = (p-1)(q-1)$ med $\gcd(e, \phi(n)) = 1$

(3) Finn tallet $1 < d < \phi(n)$ med $ed \equiv 1 \pmod{\phi(n)}$

(4) Tallparet $\{n, e\}$ er den offentlige nøkkelen, tilgjengeliggjøres for alle.
Tallparet $\{n, d\}$ er den hemmelige nøkkelen, tilgjengelig bare for den som lager systemet.

Kryptere: Alt som trengs for å kryptere en melding M (M er et tall $1 \leq M \leq n$) er den offentlige nøkkelen $\{n, e\}$:

(1) Finn $1 \leq c \leq n$ som tilfredsstiller $M^e \equiv c \pmod{n}$

(2) Send den krypterte meldingen c. Det gjør ikke noe om den plukkes opp av andre.

Dekryptere: Alt som trengs for å dekryptere c tilbake til M er den hemmelige nøkkelen $\{n, d\}$:

(1) Finn $1 \leq \bar{M} \leq n$ med $c^d \equiv \bar{M} \pmod{n}$

(2) Da er $\bar{M} = M$!

Eksempel: (1) Eksamen K2016, oppg 4:

RSA-system med $n = 13 \cdot 17 = 221$ og offentlig nøkkel $\{n, e\} = \{221, 5\}$.

(a) Finn den hemmelige nøkkelen $\{n, d\}$

(b) Krypter meldingen $m = 5$.

For (a): siden $1 < d < \phi(n)$ og $ed \equiv 1 \pmod{\phi(n))}$ må vi løse $ex \equiv 1 \pmod{\phi(n)}$

dvs $5x \equiv 1 \pmod{12 \cdot 16}$, dvs $5x \equiv 1 \pmod{192}$

$$\left.\begin{aligned} 192 &= 38 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}\right\} \quad 1 = 5 - 2 \cdot 2 = 5 - 2(192 - 38 \cdot 5) = 5 \cdot 77 - 2 \cdot 192$$

$$\Rightarrow 192 \mid (5 \cdot 77 - 1)$$

Løsningen av $5x \equiv 1 \pmod{192}$ er derfor

$$x \equiv 77 \pmod{192}$$

Siden $1 < 77 < 192 = \phi(n)$ er $d = 77$, så den hemmelige nøkkelen er

$$\{n, d\} = \{221, 77\}$$

For (b): må finne c med $1 \le c \le n$ og $m^e \equiv c \pmod n$, dvs

$$1 \le c \le 221 \text{ og } 5^5 \equiv c \pmod{221}$$

Har $5^4 \equiv 625 \equiv 183 \pmod{221}$ så $5^5 \equiv 5 \cdot 183 \equiv 915 \equiv 31 \pmod{221}$

så $c = 31$. Den krypterte meldingen er altså

$$c = 31$$

Oppgave: Dekrypter $c = 31$ og sjekk at vi da får tilbake $m = 5$:

$$31^{77} \equiv 5 \pmod{221}$$

(2) Eksamen H2005, oppg 3:

(a) Et RSA-system har hemmelig nøkkel $\{n, d\} = \{91, 29\}$. Finn den offentlige nøkkelen $\{n, e\}$.

(b) Du mottar den hemmelige (krypterte) meldingen 9. Dekrypter.

For (a): Har $91 = 7 \cdot 13$ så $\phi(91) = 6 \cdot 12 = 72$. Må finne $1 < e < 72$ med $29e \equiv 1 \pmod{72}$, dvs $ed \equiv 1 \pmod{\phi(n)}$. Merk at $d = 29$ tilfredsstiller $1 < d < \phi(n)$ og $\gcd(d, \phi(n)) = 1$. Euklid:

$$\left.\begin{aligned} 72 &= 2 \cdot 29 + 14 \\ 29 &= 2 \cdot 14 + 1 \end{aligned}\right\} \quad \begin{aligned} 1 &= 29 - 2 \cdot 14 = 29 - 2(72 - 2 \cdot 29) \\ &= 29 \cdot 5 - 2 \cdot 72 \end{aligned}$$

Får da $72 \mid (29 \cdot 5 - 1)$, dvs $29 \cdot 5 \equiv 1 \pmod{72}$, dvs $e = 5$. Den offentlige nøkkelen er da

$$\{n, e\} = \{91, 5\}$$

For (b): Må redusere 9^d modulo n, dvs 9^{29} modulo 91:

$$9^2 \equiv 81 \equiv -10 \pmod{91} \implies 9^3 \equiv -90 \equiv 1 \pmod{91} \implies$$

$$9^{27} \equiv (9^3)^9 \equiv 1^9 \equiv 1 \pmod{91} \implies 9^{29} \equiv 9^2 \cdot 9^{27} \equiv 81 \pmod{91}.$$

Så den dekrypterte meldingen er

$$M = 81$$

Oppgave: Krypter $M = 81$ og sjekk at vi da får $c = 9$:

$$81^5 \equiv 9 \pmod{91}$$

Sikkerhet: Hvorfor regnes systemet som trygt? For å finne d må man løse $ed \equiv 1 \pmod{\phi(n)}$. Men alle får jo vite n og e, kan man ikke da bare regne ut $\phi(n)$ og så løse

$$ex \equiv 1 \pmod{\phi(n)}\ ?$$

Formodning: Å finne $\phi(n)$ gitt n er like vanskelig som å faktorisere n (dvs finne p og q).

Argument: Hvis vi kjenner p og q har vi jo $\phi(n) = (p-1)(q-1)$, så da finner vi $\phi(n)$ lett. Anta motsatt at n og $\phi(n)$ er kjent. Man vet også at $n = pq$. Har

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$$

$$\Longrightarrow p + q = n - \phi(n) + 1$$

Videre er

$$(p-q)^2 = p^2 - 2pq + q^2 = (p^2 + 2pq + q^2) - 4pq$$

$$= (p+q)^2 - 4pq = (n - \phi(n) + 1)^2 - 4n$$

$$\Longrightarrow p - q = \sqrt{(n - \phi(n) + 1)^2 - 4n}$$

Så når n og $\phi(n)$ er kjent får man regnet ut hva $p+q$ og $p-q$ er. Da finner man lett p og q!

Konklusjon: Man regner derfor med at det å finne d (gitt n og e) er like vanskelig som å faktorisere n. Når p og q (og da n) er store, er dette vanskelig.