RSA kryptering

Fra Euklid til sikkerhed på internettet

2025

RSA kryptering

Fra Euklid til sikkerhed på internettet

Morten S. Risager

Dette er kortfattede noter til et kort forløb om kryptering tiltænkt særligt interesserede gymnasieelever. Vi forklarer den teoretiske baggrund bag RSA-kryptering, som benyttes som sikkerhedssystem i mange moderne digitale systemer. Læseren forudsættes at have kendskab til de hele tal, til division med rest, have god logisk forståelse, interesse og entusiasme for at lære mere. For tekster der går mere i detaljer henviser vi til [3, 4].

1 Divisorer, Euklids algoritme, og primtal

Vi starter med nogle af de klassiske egenskaber ved de hele tal. Disse opdagelser går i høj grad tilbage til de gamle grækere. Især til bog VII af Euklids berømte bøger Elementer [1], skrevet i det 3. århundrede f.Kr.

1.1 Divisorer

Vi betegner

$$\mathbb{N} := \{1, 2, 3, \ldots\} \text{ de naturlige tal,}$$
$$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \ldots\} \text{ de hele tal.}$$

Definition 1.1. Lad $a, b \in \mathbb{Z}$ med $b \neq 0$. Vi siger at a *er divisibel med* b hvis der findes et $c \in \mathbb{Z}$ så $a = bc$. Vi skriver dette som $b \mid a$. Hvis der ikke findes et sådant c, siger vi at a *ikke er divisibel med* b, og skriver $b \nmid a$.

Der er mange andre måder at sige at a er divisibel med b. Vi siger også at b dividerer a, at b deler a, at b er en faktor i a, eller at a er et multiplum af b.

Bemærk at hvis $a \neq 0$ er divisibel med b så er $|a| = |b||c|$, og da $|c| \geq 1$ følger det at

$$|a| \geq |b|.$$

Det følger at de eneste divisorer af 1 er ± 1.

Definition 1.2. Lad $a, b \in \mathbb{Z}$ hvor ikke begge er 0. Det største naturlige tal som både er en divisor af a og b, kaldes den største fælles divisor af a og b og betegnes $\mathrm{sfd}(a, b)$, dvs.

$$\mathrm{sfd}(a, b) = \max\{d \in \mathbb{N} : d \mid a \text{ og } d \mid b\}.$$

Vi definerer $\mathrm{sfd}(0, 0) = 0$.

Eksempel 1.1

Vi har

$$\mathrm{sfd}(7,14) = 7, \quad \mathrm{sfd}(6,7) = 1$$

da tallet 7 har divisorerne 1 og 7, tallet 14 har divisorerne 1,2,7,14, og tallet 6 har divisorerne 1,2,3,6.

For små tal a, b er det ikke svært at finde alle divisorerne af a og b og derfra at afgøre hvilken af de fælles divisorer der er størst. Men for store tal er der en langt mere effektiv måde at finde den største fælles divisor. For at forklare hvordan, noterer vi først følgende egenskaber:

Proposition 1.3. *For alle $a, b \in \mathbb{Z}$ gælder*

$$\mathrm{sfd}(a,b) = \mathrm{sfd}(a,-b) = \mathrm{sfd}(-a,b) = \mathrm{sfd}(a, b \pm a) = \mathrm{sfd}(a \pm b, b)$$

Bevis. Vi viser at $\mathrm{sfd}(a,b) = \mathrm{sfd}(a, b+a)$ og overlader de andre tilfælde til Opgave 3.

Lad $d_1 = \mathrm{sfd}(a,b)$ og $d_2 = \mathrm{sfd}(a, b+a)$. Så er $d_1 \mid a$ og $d_1 \mid b$. Ifølge Opgave 2 gælder så at $d_1 \mid (b+a)$ dvs. d_1 er en fælles positiv divisor for a og $b+a$. Dermed er

$$d_1 \leq d_2$$

da den største fælles divisor for a og $b+a$ ikke kan være mindre end denne divisor. På samme måde gælder at $d_2 \mid a$ og $d_2 \mid b+a$. Som før får vi fra Opgave 2 at $d_2 \mid (b+a-a) = b$ dvs. d_2 er en positiv fælles divisor for både a og b. Dermed er d_2 mindre eller lig med den største fælles divisor af a og b dvs.

$$d_2 \leq d_1.$$

Disse to uligheder kan kun være opfyldte hvis $d_1 = d_2$ hvilket viser påstanden. □

1.2 Euklids algoritme

I folkeskolen lærer man at lave division med rest, dvs. at man givet $a, b \in \mathbb{Z}$ med $b \neq 0$, kan finde $q, r \in \mathbb{Z}$ så

$$a = bq + r, \quad \text{hvor } 0 \leq r < |b|.$$

Man kan vise at q og r der opfylder disse betingelser faktisk er entydige.

Ved hjælp af division med rest og Proposition 1 kan vi effektivt udregne $\mathrm{sfd}(a,b)$.

Eksempel 1.2

Lad $a = 998$ og $b = 498$. Hvis vi laver division med rest ser vi at $998 = 2 \cdot 498 + 2$. Ved at bruge Proposition 1.3 finder vi at

$$\mathrm{sfd}(998,498) = \mathrm{sfd}(998-498,498) = \mathrm{sfd}(998-2\cdot 498,498) = \mathrm{sfd}(2,498)$$

Vi kan nu lave division af 498 med 2 og får $498 = 249 \cdot 2 + 0$. Ved at bruge Proposition 1.3 igen får vi så $\mathrm{sfd}(2,498) = \mathrm{sfd}(2, 498 - 249\cdot 2) = \mathrm{sfd}(2,0)$. Men det er altid let at finde den største fælles divisor af et tal og 0, da alle tal går op i 0. Derfor er $\mathrm{sfd}(2,0) = 2$ og vi ser at

$$\mathrm{sfd}(998,498) = \mathrm{sfd}(2,498) = \mathrm{sfd}(2,0) = 2$$

Vi har altså udregnet $\mathrm{sfd}(998,498)$ uden at finde divisorerne af 998 og 498.

Den metode vi har brugt i eksemplet kan bruges på alle talpar, og kaldes Euklids algoritme. Nogle dataloger kalder denne fantastiske algoritme for *alle algoritmers bedstefar*.

Sætning 1.1: Euklids algoritme

Lad $a, b \in \mathbb{Z}$ med $b \neq 0$. Sæt $r_0 = a$ og $r_1 = b$. Lav nu division med rest:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, && \text{hvor } 0 \leq r_2 < |r_1| \\ r_1 &= q_2 r_2 + r_3, && \text{hvor } 0 \leq r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, && \text{hvor } 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + r_{n+1} && \text{hvor } r_{n+1} = 0 \end{aligned}$$

Da gælder

$$\operatorname{sfd}(a, b) = r_n. \tag{1}$$

Der udover gælder der at der findes $x, y \in \mathbb{Z}$ så

$$ax + by = \operatorname{sfd}(a, b) \tag{2}$$

Bevis. Bemærk først at eftersom restleddet bliver mindre i hvert skridt, stopper algoritmen efter et endeligt antal skridt. For at bevise at $\operatorname{sfd}(a, b) = r_n$ bemærker vi ifølge Proposition 1.3 at der for alle i gælder

$$\operatorname{sfd}(r_i, r_{i+1}) = \operatorname{sfd}(q_{i+1} \cdot r_{i+1} + r_{i+2}, r_{i+1}) = \operatorname{sfd}(r_{i+2}, r_{i+1}) = \operatorname{sfd}(r_{i+1}, r_{i+2}).$$

Det følger nu at

$$\operatorname{sfd}(a, b) = \operatorname{sfd}(r_0, r_1) = \cdots = \operatorname{sfd}(r_n, r_{n+1}) = \operatorname{sfd}(r_n, 0) = r_n$$

hvilket viser (1). For at vise (2) ser vi at for alle $i \in \{2, \cdots, n+1\}$ gælder der

$$r_i = -q_{i-1} r_{i-1} + r_{i-2}$$

Vi kan altså udtrykke r_n som et heltal gange r_{n-1} plus et andet heltal gange r_{n-2}. Men nu kan vi gøre det samme ved r_{n-1} og vi finder på den måde at r_n kan skrives som et heltal gange r_{n-2} plus et andet heltal gange r_{n-3}. Ved at fortsætte på samme måde får vi at der findes heltal x, y så

$$r_n = y r_1 + x r_0 = yb + xa$$

hvilket viser påstanden. □

Bemærk at beviset for Euklids algoritme også giver en opskrift til effektivt at finde x, y i (2).

Eksempel 1.3

Lad $a = 127$ og $b = 31$. Ved at lave division med rest finder vi

$$\begin{aligned} 127 &= 4 \cdot 31 + 3 \\ 31 &= 10 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Sætningen ovenfor siger nu at den største fælles divisor af 127 og 31 er 1, da det er den sidste rest inden vi får rest 0. Ved at lave baglæns substitution finder vi

$$\mathrm{sfd}(a,b) = 1 = 31 - 10 \cdot 3 = 31 - 10(127 - 4 \cdot 31) = -10 \cdot 127 + 41 \cdot 31 = -10 \cdot a + 41 \cdot b,$$

dvs. vi har (2) med $x = -10$, $y = 41$.

Definition 1.4. Vi siger at $n, m \in \mathbb{Z}$ er *indbyrdes primiske* hvis $\mathrm{sfd}(m,n) = 1$.

Proposition 1.5. *Antag at n, m er indbyrdes primiske og at de begge deler c. Så deler deres produkt også c. Dvs.*

$$\textit{hvis } n \mid c \textit{ og } m \mid c \textit{ så gælder } nm \mid c.$$

Bevis. Ifølge antagelsen findes der $l, k \in \mathbb{Z}$ så $c = nk$ og $c = ml$. Da $\mathrm{sfd}(m,n) = 1$ giver Sætning 1.1, (2) at der findes $x, y \in \mathbb{Z}$ så $1 = xn + ym$. Tilsammen får vi derfor

$$c = c(xn + ym) = cxn + cym = mlxn + nkym = nm(lx + ky)$$

hvilket viser påstanden. □

Eksempel 1.4

Vi viste i eksemplet ovenfor at $\mathrm{sfd}(127, 31) = 1$, dvs. 127 og 31 er indbyrdes primiske. Vi siger også at 127 er indbyrdes primisk med 31, eller at 31 er indbyrdes primisk med 127.

1.3 Primtal

Definition 1.6. Et heltal $p > 1$ kaldes et *primtal*, hvis de eneste positive divisorer af p er 1 og p.

Eksempel 1.5

Vi bemærker at de positive divisorer af 2 er præcist tallene 1 og 2. Dermed er 2 et primtal. Det er ikke svært at se at 2 er det eneste lige primtal. I Opgave 11 skal I finde alle primtal under 20. Det størst kendte primtal er $2^{136.279.841} - 1$ og har over 40 millioner cifre. Det blev fundet i 2024.

Lemma 1.7 (Euklids lemma)**.** *Lad p være et primtal og $m, n \in \mathbb{Z}$. Antag $p \mid mn$. Så er $p \mid m$ eller $p \mid n$.*

Bevis. Hvis $p \mid m$ er vi færdige. Antag derfor $p \nmid m$. Vi skal så vise at $p \mid n$. Da de eneste divisorer af p er 1 og p er $\mathrm{sfd}(p,m) = 1$, og ifølge (2) findes der $x, y \in \mathbb{Z}$ så $xp + ym = 1$. Ganger vi med n får vi

$$n = xpn + ymn.$$

Da p deler begge led i højresiden må $p \mid n$, hvilket færdiggør beviset. □

Det næste resultat er strengt taget ikke nødvendigt for at forstå hvordan kryptering virker, men eftersom resultatet er en af de vigtigste om heltallene og primtal ser vi på det alligevel.

Sætning 1.2: Aritmetikkens fundamentalsætning

Ethvert naturligt tal $n > 1$ kan skrives som et produkt af primtal. Denne opskrivning er entydigt op til ombytning af faktorerne.

Bevis. Lad os antage at der findes naturlige tal større end 1 som ikke kan skrives som produkter af primtal. Antag at $n > 1$ er det mindste med denne egenskab. Så kan n ikke være et primtal, så det har andre divisorer end 1 og n, dvs. $n = mk$ for $1 < m, k < n$. Da n er det mindste tal der ikke kan skrives som produkter af primtal kan m, k skrives som produkter af primtal. Men da $n = mk$ kan n nu også skrives som et produkt af primtal. Det vil altså sige at n både kan skrives som et produkt af primtal og ikke kan skrives som et produkt af primtal. Men det er en logisk modstrid, og der kan derfor slet ikke eksistere et sådant n. Dvs. alle $n > 1$ kan skrives som produkter af primtal.

For at bevise entydigheden antager vi at n er det mindste $n > 1$ der kan skrives som produktet af primtal på 2 essentielt forskellige måder, dvs.

$$n = p_1 p_2 \cdots p_l = q_1 q_2 \ldots q_k.$$

Her er alle p_i og q_j primtal, og det ene sæt af primtal er ikke bare er en ombytning af det andet sæt af primtal. Ifølge (2) finder vi da $p_1 \mid q_1 q_2 \cdots q_k$ og derfor må $p_1 \mid q_j$ for et j_0. Men da q_{j_0} er primtal og $p_1 > 1$ må $p_1 = q_{j_0}$. Ved eventuelt at omnavngive $q_j$erne kan vi antage $p_1 = q_1$. Hvis $l = k = 1$ er de 2 primtalsfaktoriseringer ens, hvilket vi har antaget at de ikke er. Hvis $l = 1, k > 1$ er $1 = q_2 \cdots q_k$ hvilket ikke kan være rigtigt da $q_2 > 1$. Derfor må $k > 1$ og $l > 1$ og vi får derfor

$$p_2 \cdots p_l = q_2 \ldots q_k,$$

som er 2 forskellige primtalsopskrivninger. Men det strider logisk mod at n var det mindste $n > 1$ der har 2 forskellige primtalsopskrivninger. Der kan altså slet ikke eksistere et sådant n hvilket beviser at opskrivningen er entydig op til ombytning af primtalsfaktorerne. □

2 Kongruensregning og Fermats lille sætning.

Konceptet i kongruensregning har eksisteret længe i forskellige former, og går tilbage til det antikke Grækenland og Kina. Det er senere blevet brugt i stor stil af matematikere som Fermat, Euler, Leibniz og mange andre. Den moderne teori er etableret af Gauss i starten af 1800-tallet i [2]. Nogle af resultaterne i dette afsnit kan formuleres mere elegant ved hjælp af gruppeteori, men for ikke at kræve for mange forudsætninger fra læseren formulerer vi de fleste resultater uden gruppeteori i samme stil som i Gauss' oprindelige tekst.

2.1 Kongruens modulo m

Lad m være et naturligt tal. Vi siger at $a, b \in \mathbb{Z}$ er *kongruente modulo* m hvis $m \mid a - b$. I dette tilfælde skrive vi

$$a \equiv b \bmod m$$

Vi bemærker at $a \equiv b \bmod m$ gælder præcist hvis $a = b + km$ for et $k \in \mathbb{Z}$, så vi kan komme fra b til a ved at tilføje et heltalsmultiplum af m. Vi bemærker også at $a \equiv b \bmod m$ hvis og kun hvis a og b har samme rest ved division med m.

Nogle af de simple egenskaber ved $\equiv$ er følgende:

Proposition 2.1. *For alle $a, b, c \in \mathbb{Z}$ gælder der at*

1. $a \equiv a \bmod m$.
2. *Hvis* $a \equiv b \bmod m$ *så er* $b \equiv a \bmod m$.
3. *Hvis* $a \equiv b \bmod m$ *og* $b \equiv c \bmod m$ *så er* $a \equiv c \bmod m$.

Bevis. Øvelse. □

På nogen måder opfører $\equiv$ sig lidt som et almindeligt lighedstegn. F.eks. kan man vise at hvis $a \equiv b \bmod m$ og $c \equiv d \bmod m$ så gælder

$$\begin{aligned} a + c &\equiv b + d \bmod m, \\ ac &\equiv bd \bmod m \end{aligned} \tag{3}$$

Bemærk at ved at bruge (3) flere gange finder vi at

$$\text{hvis } a \equiv b \bmod m \text{ så er } a^n \equiv b^n \bmod m \text{ for all } n \in \mathbb{N}. \tag{4}$$

Vi ser også udfra (3) at der gælder at hvis $b \equiv c \bmod m$, så er $ab \equiv ac \bmod m$. Under passende betingelser kan vi også gå den modsatte vej ved at bruge følgende sætning.

Sætning 2.1: Forkortningsreglen

Antag at a og m er indbyrdes primiske. Da gælder at hvis

$$ab \equiv ac \bmod m$$

så er

$$b \equiv c \bmod m$$

Bevis. Da a og m er indbyrdes primiske giver Sætning 1.1, (2) at der eksisterer $x, y \in \mathbb{Z}$ så $ax + my = 1$. Da $ab \equiv ac \bmod m$ er $ab - ac$ divisibel med m, dvs.

$$a(b - c) = km \text{ for et } k \in \mathbb{Z}$$

Vi kan nu gange denne lighed med x og får så at

$$xkm = xa(b - c) = (1 - my)(b - c)$$

hvilket ved omrokering bliver til

$$b - c = xkm + my(b - c)$$

Da højresiden har m som faktor, ser vi at $b \equiv c \bmod m$ hvilket var det vi ville vise. □

Vi er nu klar til at vise den vigtigste sætning i teorien:

Sætning 2.2: Fermat's lille sætning

Et heltal $p > 1$ er et primtal hvis og kun hvis, der for alle heltal a, som ikke er divisible med p, gælder at

$$a^{p-1} \equiv 1 \bmod p$$

Bevis. Antag først at p er et primtal, og lad $a \in \mathbb{Z}$ som ikke er divisibel med p. Betragt listen

$$1, 2, 3, \ldots p-1 \tag{5}$$

For et element n fra denne liste kan vi lave division med rest af $a \cdot n$, dvs. vi skriver $a \cdot n = q_n p + r_n$ hvor $0 \leq r_n < p$. Bemærk at r_n ikke kan være 0. Hvis den var, ville an jo være divisibel med p, og ifølge Euklids lemma (Lemma 1.7) ville vi have enten $p \mid a$ eller $p \mid n$. Men vi har antaget at a ikke er divisibel med p, og n kan heller ikke være det da $1 \leq n < p$. Så r_n kan ikke være 0 og dermed er $1 \leq r_n \leq p-1$. Betragt nu listen

$$r_1, r_2, r_3, \ldots r_{p-1} \tag{6}$$

Vi påstår at listen (6) er identisk med listen (5), men muligvist skrevet i en anden rækkefølge. For at bevise dette bemærker vi at $1 \leq r_n \leq p-1$, så det er nok at vise at tallene er forskellige, dvs. at hvis $n_1 \neq n_2$ så er $r_{n_1} \neq r_{n_2}$. Hvis det er tilfældet må listen (6) være identisk med listen (5). Vi antager derfor at $r_{n_1} = r_{n_2}$, og vil gerne vise at $n_1 = n_2$. Hvis $r_{n_1} = r_{n_2}$, følger det af definitionen af r_n at

$$an_1 \equiv an_2 \bmod p.$$

Men så følger det af forkortningsreglen (Sætning 2.1) at $n_1 \equiv n_2 \bmod p$, dvs. $n_1 - n_2$ er divisibel med p. Men $-(p-1) \leq n_1 - n_2 \leq p-1$ og det eneste tal som er divisibelt med p i dette interval er 0, og dermed er $n_1 = n_2$. Vi har dermed vist at listen (6) må være identisk med listen (5).

Vi kan bruge dette til at konkludere at $1 \cdot 2 \cdots (p-1) = r_1 \cdots r_{p-1}$. Ved at bruge $r_n \equiv an \bmod p$ og (3) følger det at

$$1 \cdot 2 \cdots (p-1) \equiv a^{p-1} 1 \cdot 2 \cdots (p-1) \bmod p$$

Vi kan se ud fra Euklids lemma at tallet $1 \cdot 2 \cdots (p-1)$ ikke er divisibel med p, og at det derfor er indbyrdes primisk med p. Vi kan så igen bruge forkortningsreglen (Sætning 2.1) til at konkludere at $1 \equiv a^{p-1} \bmod p$ hvilket var det vi gerne ville vise.

For den anden implikation antag at $a^{p-1} \equiv 1 \bmod p$ for alle a der ikke er divisible med p. For at vise at p er et primtal antager vi at dette ikke er tilfældet og udleder en modstrid. Hvis p ikke er et primtal har det en faktor a, hvor $1 < a < p$. Men da a ikke er divisibelt med p (det er jo mindre end p) må der altså ifølge antagelsen gælde $a^{p-1} \equiv 1 \bmod p$, dvs. $a^{p-1} = 1 + kp$ for et heltal k. Men da både a^{p-1} og p er divisible med a følger det at 1 er divisibel med a hvilket er en modstrid da $a > 1$. Dermed må antagelsen om at p ikke er et primtal være forkert, og vi er færdige. □

2.2 Eulers φ funktion.

Definition 2.2. For $n \in \mathbb{N}$ definerer vi Eulers φ funktion som antallet af heltal m hvor $1 \leq m \leq n$ som er indbyrdes primiske med n dvs.

$$\varphi(n) = \#\{1 \leq m \leq n : \text{sfd}(m, n) = 1\}. \tag{7}$$

Eksempel 2.1

Hvis vi vil udregne $\varphi(6)$ kan vi udregne alle de relevante største fælles divisorer som

m	1	2	3	4	5	6
$\text{sfd}(m,6)$	1	2	3	2	1	6

hvorfra vi kan finde $\varphi(6)$, da det er antallet af 1-taller i nederste række. Vi har altså $\varphi(6) = 2$.

Metoden vi brugte i dette eksempel bliver hurtigt besværlig. Heldigvis er der en lettere metode:

Sætning 2.3

Lad p og q være forskellige primtal. Så er

$$\varphi(p) = p - 1 \tag{8}$$
$$\varphi(pq) = (p-1)(q-1) \tag{9}$$

Bevis. Påstanden i (8) er Opgave 13. For at bevise (9) bemærker vi at de tal $1 \leq m \leq pq$ som *ikke* er indbyrdes primiske med pq er dem som *har* en fælles faktor med pq som er skarpt større end 1. Det betyder at p er en faktor, eller at q er en faktor, eller at begge er en faktor. Der er kun 1 af tallene som har både p og q som faktorer nemlig pq De tal som har p men ikke q som faktor er præcist de $q-1$ tal

$$p, 2p, 3p, \ldots (q-1)p.$$

De tal som har q men ikke p som faktor er præcist de $p-1$ tal

$$q, 2q, \ldots (p-1)q.$$

Dermed er antallet af tal $1 \leq m \leq pq$ som er indbyrdes primiske med pq lig

$$pq - 1 - (q-1) - (p-1) = (p-1)(q-1)$$

hvilket viser påstanden. □

Der er formler for Eulers φ funktion for alle naturlige tal, men eftersom vi senere kun har brug for formlen når n er et produkt af 2 forskellige primtal nøjedes vi med det tilfælde. Men her er formlen: hvis $n = p_1^{k_1} \cdots p_l^{k_l}$ hvor $p_1, \ldots, p_l$ er forskellige primtal og $k_i \in \mathbb{N}$ så gælder

$$\varphi(n) = n(1 - p_1^{-1}) \cdots (1 - p_l^{-1}).$$

Overvej hvorfor dette stemmer overens med sætningen ovenfor når $n = pq$ og p, q er forskellige primtal.

Vi har nu alle redskaberne til at bevise den fundamentale sætning som ligger til grund for at RSA-kryptering virker

Sætning 2.4

Antag at $n = p_1 p_2$ er et produkt af 2 forskellige primtal. Antag desuden at $m \equiv 1 \bmod \varphi(n)$. Så gælder der

$$a^m \equiv a \bmod n, \qquad \text{for alle } a \in \mathbb{Z}.$$

Bevis. Da p_1 og p_2 er *forskellige* primtal er de indbyrdes primiske. Vi vil vise, under de givne antagelser, at der for alle $a \in \mathbb{Z}$, gælder at $a^m \equiv a \bmod p_i$ for $i = 1, 2$. Dvs. både p_1 og p_2 deler $a^m - a$. Heraf følger det fra Proposition 1.5 at $p_1 p_2 = n$ deler $a^m - a$ hvilket præcist er det vi gerne vil vise. Det er altså nok at vise at $a^m \equiv a \bmod p_i$ hvilket vi nu beviser: Betragt først p_1.

Hvis a er divisibel med p_1 er det klart at $a^m - a$ også er divisibel med p_1 så $a^m \equiv a \bmod p_1$.

Hvis a ikke er divisibel med p_1 må a være indbyrdes primisk med p_1, da de eneste divisorer af p_1 jo er 1 og p_1. Vi bemærker nu ved hjælp af Sætning 2.3, at $m - 1 = k(p_1 - 1)(p_2 - 1)$ for et $k \in \mathbb{Z}$, så

$$a^{m-1} = (a^{p_1-1})^{k(p_2-1)}$$

Ifølge Fermat's lille sætning (Sætning 2.2) er $a^{p_1} \equiv 1 \bmod p_1$ Det følger nu af (4) at

$$\begin{aligned} a^{m-1} &\equiv (a^{p_1-1})^{k(p_2-1)} \bmod p_1 \\ &\equiv 1^{k(p_2-1)} \bmod p_1 \\ &\equiv 1 \bmod p_1 \end{aligned}$$

Ved at gange dette igennem med a får vi at $a^m \equiv a \bmod p_1$.

Man kan nu gøre præcist det samme med det andet primtal p_2, og finder at der for alle a gælder $a^m \equiv a \bmod p_2$, hvilket afslutter beviset. □

3 RSA-kryptering

RSA-kryptering er en krypteringsalgoritme som bruges i mange digitale systemer primært til kommunikation over internettet. Den blev opfundet i 1970'erne af Ron Rivest, Adi Shamir og Leonard Adelman [6], (RSA er deres forbogstaver). Systemet fungerer ved at konstruere to sæt nøgler, hvor den ene nøgle er offentlig og den anden nøgle holdes hemmelig. Vi starter med at forklare hvordan man konstruere et sådant nøglepar.

3.1 Konstruktion af RSA-nøglepar

RSA nøglepar konstrueres på følgende måde:

1. Vælg hemmeligt 2 store primtal p_1, p_2.
2. Beregn hemmeligt $n = p_1 p_2$ and $\varphi(n) = (p_1 - 1)(p_2 - 1)$.
3. Vælg et "tilfældigt " tal $1 < e < \varphi(n)$ som er indbyrdes primisk med $\varphi(n)$.
4. Beregn i hemmelighed et heltal d så $ed \equiv 1 \bmod \varphi(n)$.
   Dette kan gøres ved at bruge (2) da $\mathrm{sfd}(e, \varphi(n)) = 1$.
5. Talparret (e, n) er den offentlige nøgle som kan gøres offentlig.
6. Talparret (d, n) er den hemmelige nøgle som holdes hemmelig.

Eksempel 3.1

Alice vil gerne lave et en offentlig og en hemmelig nøgle som ovenfor og gør derfor følgende:

1. Vælger primtallene $p_1 = 43$, $p_2 = 67$.
2. Udregner $n = 43 \cdot 67 = 2881$, $\varphi(n) = 42 \cdot 66 = 2772$.
3. Vælger $e = 1003$.
4. $1003x \equiv 1 \pmod{2772}$ har løsning 655.
5. Alice's offentlige nøgle er nu $(e, n) = (1003, 2881)$.
6. Alice's private nøgle er $(d, n) = (655, 2881)$.

3.2 Kryptering og dekryptering af beskeder

Alice vil gerne bruge sine nøgler til at modtage beskeder fra sin ven Bob. Hun sender nu den offentlige nøgle til Bob. Da de ikke har aftalt noget på forhånd er de nødt til at kommunikere over en usikker kanal (email/telefon/besked-tjeneste eller andet), hvor andre i princippet kan opsnappe kommunikationen. Hvis Bob gerne vil sende Alice tallet a (antag at $1 \leq a < n$) så udregner han, ved hjælp af den offentlige nøgle, restklassen af a^e ved division med n. Vi betegner denne som

$$a^e \bmod n.$$

Dette er *den krypterede besked* som han nu sender til Alice over den usikre kanal. I princippet kan deres fjende Charlie opsnappe beskeden, men Charlie har svært ved at finde a da han kun kender restklassen af a^e ved division med n (altså $a^e \bmod n$.)

Alice har den hemmelige nøgle og kan nu udregne restklassen af $(a^e \bmod n)^d$ ved division med n. Der gælder nu at

$$\begin{aligned}(a^e \bmod n)^d &\equiv a^{ed} \bmod n \\ &\equiv a \bmod n\end{aligned}$$

hvor vi i første $\equiv$ har brugt (4), og i anden $\equiv$ har brugt at $ed \equiv 1 \bmod \varphi(n)$ så udsagnet følger af Sætning 2.4. Da Alice ved at Bob er startet med et tal som er mellem 1 og n kan hun finde altså finde a ved at finde restklassen af $(a^e \bmod n)^d$. Hun har altså nu *dekrypteret den krypterede besked*, og har dermed modtaget Bobs besked. Charlie kender ikke den hemmelige nøgle (d, n) og kan derfor ikke lave udregningen ovenfor.

Eksempel 3.2

Alice beregnede i det Eksempel 3.1 den offentlige nøgle $(1003, 2881)$ og den hemmelige nøgle $(655, 2881)$. Bob vil gerne sende hende tallet 1330, da han gerne vil aftale at mødes med hende kl 13:30 næste dag på deres hemmelige sted. Han kender jo hendes offentlige nøgle og kan derfor beregne $1330^{1003} \equiv 2259 \bmod 2881$, Han sender nu Alice tallet 2259. Hun beregner $2259^{655} \equiv 1330 \bmod 2881$, og nu ved hun at Bob gerne vil mødes med hende kl 13.30.

I et mere realistisk setup vil de indgående primtal typisk være flere hundrede cifre lange. Det bliver derfor vigtigt at have en effektiv måde at finde primtal af denne størrelse. I praksis kan

man gøre det ved at bruge Miller-Rabins algoritme, som er en mindre videreudvikling af Fermat's lille sætning, dvs. Sætning 2.2.

For at få RSA-kryptering til at være praktisk anvendelig er det også vigtigt at have en effektiv måde at udregne $a^e \bmod n$, da metoden jo involverer mange udregninger af denne type. Dette gøres ved hjælp af en teknik der hedder modulær eksponentiering. Denne fungerer ved at skrive e i base 2, og bruge forskellige potensregneregler. Dette gør at man effektivt og hurtigt kan udregne $a^e \bmod n$.

Både Miller-Rabin og modulær eksponentiering er beskrevet i mere detalje i [5].

4 Sikkerhed

Sikkerheden i RSA kryptering ligger i at Alice er den eneste der har adgang til hendes hemmelige nøgle. Hvis Charlie kendte eller kunne finde d ville han kunne lave den samme udregning som Alice for at dekryptere Bobs besked. Hvis han skal finde d skal han løse ligningen

$$ex \equiv 1 \bmod \varphi(n)$$

Problemet for Charlie er at han ikke kender $\varphi(n)$, men kun e og n som han har opsnappet over den usikre kanal som Alice og Bob brugte. Hvis han kendte $\varphi(n)$ ville han kunne bruge Euklids algorithme til at finde x og y så $ex + y\varphi(n) = 1$, han ville så kunne bruge dette x til at dekryptere med.

Men hvordan kan han så finde $\varphi(n)$?

- Han kan gå til definition (7) og finde alle de m mellem 1 og n der er indbyrdes primiske med n. Antallet af disse er så $\varphi(n)$. Hvis n har flere hundrede cifre er dette praktisk umuligt med de metoder vi kender til.
- Han kan bruge formlen fra Sætning 2.3, (9) til at udregne $\varphi(n)$, men den kræver at han kender p_1 og p_2, dvs. at han kan primtalsfaktorisere n. Vi kender ikke på nuværende tidspunkt metoder der er hurtige nok til at primtalsfaktorisere store tal til at dette er muligt. Hvis vi finder ud af hvordan man bygger tilstrækkeligt store kvantecomputere kan dette ændre sig.

Som vi kan se bryder vi RSA-kryptering hvis vi kan finde en måde hvorpå man effektivt kan udregne $\varphi(n)$. Man kan vise at hvis man effektivt kan finde $\varphi(n)$ udfra n så kan man også primtalsfaktorisere n, da p_1 og p_2 så er rødderne til polynomiet

$$x^2 + (\varphi(n) - n - 1)x + n$$

På nuværende tidspunkt ved vi faktisk ikke om der kunne være andre måder at bryde RSA kryptering end ved at primtalsfaktorisere n (eller hvad der ifølge kommentaren ovenfor kommer ud på det samme: at finde $\varphi(n)$).

Litteratur

[1] Euklid. *Elementer, Bind 1-4.* Oversat Af Claus Glunk, Hanne Eggert Strand, Chr. Marinus Taisbak Og Chr. Gorm Tortzen. Gyldendal, 2023.

[2] Carl Friedrick Gauss. *Disquisitiones Arithmeticae.* 1801.

[3] Johan P. Hansen. *Tal og mængder.* Aarhus Universitetsforlag, 2012.

[4] Johan P. Hansen and Henrik G. Spalk. *Algebra og talteori.* Gyldendal Uddannelse, 2002.

[5] Morten S. Risager. *Introduction to Number Theory.* Lecture Notes. 79 Pages. `http://www.math.ku.dk/~risager/introtal/main.pdf` 2025.

[6] Ron L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

Opgaver

Nedenfor er en række opgaver. Nogle af opgaverne er markeret med ☆. Disse har mere bevisteoretisk karakter, og vil af mange opleves som lidt sværere end de øvrige. Men måske også sjovere.

Opgave 1. Find alle divisorerne af 2,3,4,5,6,7,8,9,10.

Opgave 2. Bevis at hvis $d \mid a$ og $d \mid b$ så er $d \mid a + b$ og $d \mid a - b$. ☆

Opgave 3. Bevis nogle af de resterende tilfælde af Proposition 1.3.☆

Opgave 4. Vis at resten af 207 ved division med 99 er 9.

Opgave 5. Find resten af 355 ved division med 51.

Opgave 6. Find $x, y \in \mathbb{Z}$ så $\mathrm{sfd}(314, 50) = x \cdot 314 + y \cdot 50$.

Opgave 7. Vis at hvis $d \mid a$ og $d \mid b$ så er $d \mid \mathrm{sfd}(a, b)$☆.

Opgave 8. Vis at $\mathrm{sfd}(440, 77) = 11$.

Opgave 9. Vis at 2003 og 1100 er indbyrdes primiske.

Opgave 10. (svær) Vis at hvis a, b begge er indbyrdes primiske med n, så er ab og n også indbyrdes primiske. ☆

Opgave 11. Find alle primtal mindre end 20.

Opgave 12. Udregn $\varphi(5)$ og $\varphi(7)$ på samme måde som udregningen af $\varphi(6)$ i eksemplet før Sætning 2.3.

Opgave 13. Bevis (8), på samme måde som du fandt resultaterne i Opgave 12. ☆

Opgave 14. Find $\varphi(323)$.
Hint: Prøv at primtalsfaktorisere 323. Start med at kigge på de primtal du fandt i Opgave 11.