

Diffie-Hellman

$$3. A = g^a \pmod{q}, B = g^b \pmod{q}$$

1. Primtall q og grunntall g

$$4. K \equiv g^{a \cdot b} \pmod{q}$$

2. Velg a og b mellom $2, q-2$

$$\equiv A^b \equiv B^a \pmod{q}$$

Høyre vs venstre inves. Veldef fra $V_f \rightarrow D_f$.

Venstre: f er injektiv Høyre: f er surjektiv

$$g(f(x)) = x$$

$$f(g(y)) = y$$

$$- A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$- A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$

$$- A \wedge (B \vee C \vee D) = (A \wedge B) \vee (A \wedge C) \vee (A \wedge D)$$

$$- (A \vee B) \wedge (C \vee D) = (A \wedge C) \vee (A \wedge D) \\ \vee (B \wedge C) \vee (B \wedge D)$$

$$- \neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$$

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$$

$$- A \wedge (B \wedge C) = (A \wedge B) \wedge C$$

$$- A \wedge B = \neg(\neg A \vee \neg B)$$

$$- A \Rightarrow B = \neg B \Rightarrow \neg A$$

$$- A \Rightarrow B \Leftrightarrow \neg A \vee B$$

$$- \neg(A \Rightarrow B) \Leftrightarrow A \wedge \neg B$$

$$- \neg \neg A \Rightarrow B \Leftrightarrow A \vee B$$

$$- A \Rightarrow \neg B \Leftrightarrow \neg A \vee \neg B$$

Delelighet

$$- m | a - b \rightarrow a \equiv b \pmod{m}$$

$$- \gcd(a, b) = \gcd(a - b, b) \\ = \gcd(a + b, b)$$

$$- a \bmod m = b \bmod m$$

$$\text{RSA} \quad (N, e), (c = m^e \pmod{N})$$

$$- n = p \cdot q \quad (c^d \equiv m)$$

$$- e \text{ velges som } e \perp \phi(n)$$

$$- d \cdot e \equiv 1 \pmod{\phi(n)}$$

$$- c \equiv m^e \pmod{n}$$

$$- m \equiv c^d \pmod{n}$$

Injektivitet

Dersom $f(a) = f(b)$ For alle $b \in B$ finnes en

$$\text{må } a = b \quad a \in A \mid f(a) = b$$

Primtall 1-100: Sjekke for alle $n \leq \sqrt{p}$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41

43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

- Multi ∞ , Pseudo \mathbb{P} , Enkle

$$- \exists y \forall x P(x, y) \Rightarrow \forall x \exists y P(x, y)$$

$$- \forall x \exists y P(x, y) \not\Rightarrow \exists y \forall x P(x, y)$$

$$- \neg(\forall x \exists y P(x, y)) \Rightarrow \neg(\exists y \forall x P(x, y))$$

$$- \neg(\exists y \forall x P(x, y)) \Rightarrow \neg(\forall x \exists y P(x, y))$$

$$- \neg \forall x P(x) \Leftrightarrow \exists x \neg P(x)$$

$$- \neg \exists x P(x) \Leftrightarrow \forall x \neg P(x)$$

$$- \forall x P(x) \Leftrightarrow \neg \exists x \neg P(x) \Leftrightarrow \neg(\exists x \neg P(x))$$

$$- \exists x P(x) \Leftrightarrow \neg \exists x \neg P(x) \Leftrightarrow \neg(\forall x \neg P(x))$$

$$- \exists x [P(x) \vee Q(x)] \Leftrightarrow \exists x P(x) \vee \exists x Q(x)$$

$$- \exists x [P(x) \wedge Q(x)] \not\Rightarrow \exists x P(x) \wedge \exists x Q(x)$$

$$- \forall x [P(x) \wedge Q(x)] \Leftrightarrow \forall x P(x) \wedge \forall x Q(x)$$

$$- \forall x [P(x) \vee Q(x)] \not\Rightarrow \forall x P(x) \vee \forall x Q(x)$$

Fermat faktor

$$1. a^2 - n = b^2, \text{ sett } a = \sqrt{n+1} - \text{Alle } \mathbb{C} \text{ er } \mathbb{C}: \forall x (\dots \Rightarrow \dots)$$

$$2. a^2 - n \text{ er kvadrat}/a+1. \quad - \text{Det finnes noe som både}$$

$$3. n = (a+b)(a-b)$$

$$\text{Shank: } b \equiv g^e \pmod{p} \quad (g \mid a)$$

$$1. n = \sqrt{p+1}, c \cdot g^n \equiv 1 \pmod{p}$$

$$2. \text{Sjekk } g^i \pmod{p} \text{ for } 0 \leq i < n$$

$$3. \text{Sjekk } b \cdot c^i \pmod{p} \text{ for } 0 \leq i < n$$

$$4. Finn like \rightarrow e = i \cdot n + j$$

$$- \text{Det finnes noe som er slik at: } \neg \exists x (\dots) \text{ eller } \forall x \neg (\dots)$$

$$- \text{Det finnes ingen som er slik at: }$$

$$- \exists x (\dots) \text{ eller } \forall x \neg (\dots)$$

$$\text{Merk: } (\forall \text{ og } \Rightarrow) \text{ eller } (\exists \text{ og } \wedge)$$

$$- \text{Kantet (veikrets) = Nodur (sti, sykkel)}$$

$$- \text{To mengder er like } A \subseteq B \text{ og } B \subseteq A$$

- $m \mid a$ så er $a^m \bmod m = 0$
 - Fungerer alltid \rightarrow Binær metode
 - Fermat: $\text{mod}(p)$ og $p \nmid a$
 $a^{p-1} \equiv 1 \pmod{p}$
 - Euler: $\text{mod}(m)$ og $a \perp m$
 $a^{\phi(m)} \equiv 1 \pmod{m}$
 - Kvadrat: m kvadratfri og $(a \perp m)$
 $a^{\frac{\phi(m)}{2}+1} \equiv a \pmod{m}$
 - $\phi(p^k) = p^k - p^{k-1}$
 - Anti-sym: Dersom xRy og yRx er $x=y$
 - $\text{gcd}(a,b) \cdot \text{lcm}(a,b) = a \cdot b$
 - Diofantiske løsninger hvis $\text{gcd}(a,b) \mid c$ ($ax + by = c$)
 - $a \cdot b \equiv [a \% k] \cdot [b \% k] \pmod{k}$
 - $f_{i+j} = f_i \cdot f_{j+1} + f_j \cdot f_{i-1}$
 - Hvis $a = b+c \rightarrow a \equiv b+c \pmod{k}$
 - Ekivalens $[x]_n = \{y \in M \mid y \sim x\}$ Mengden av ekvivalens-kvotientmenge M/n under \sim
 - G logiske konsepter $F: F \Rightarrow G$, $F \models G$
 - Ekvklasse \rightarrow må være ekvrelasjon
 - Ekivalens: Refl, Sym, Trans
 - Partiell: Refl, Anti-Sym, Trans
 - A er tellbar
 $f: A \rightarrow \mathbb{N}$ eller $f: \mathbb{N} \rightarrow A$ bisjektiv
 $f: A \rightarrow \mathbb{N}$ injektiv, $f: \mathbb{N} \rightarrow A$ surjektiv
 - Total: Først partiell. For alle $a, b \in S$ må a og b ha en relasjon aRb eller bRa
 - A og B er ekvivalente: Samme (A \equiv B) sannhetsverdi for alle tilordninger (A \Leftrightarrow B)
 - Språk: $(\{0\} \cup \{1\} \cup \dots \cup \{9\})^* (\{0\} \cup \{2\} \cup \dots \cup \{8\})^*$
 - Utrykk: $(0|1|2|3|\dots|9)^* (0|2|4|1|8)$
- Kinesisk restteorem m_1, m_2, \dots, m_n
- ↑
Obs: Konflikt
Felles faktor
Flere moduluser
 \rightarrow velg høyeste
- $X = [a, k_1, M_1] + \dots + [a, k_n, M_n] \pmod{M}$
- $M_1 = m_2 m_3 \dots m_n = M / m_1$
- $M_i \cdot k_i \equiv 1 \pmod{m_i}$
- Kongruensligning
- $ax \equiv b \pmod{m} \rightarrow \text{gcd}(a, m) \mid b \rightarrow \text{gcd}(a, m)$ løsninger
- Binomial
- $a/c \equiv b/c \pmod{\frac{m}{c}}$
- $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ $+ b \rightarrow$ ingen løsninger
- $\binom{n}{k} = \binom{n}{n-k}$
- Tallene foran $(x)^{n-k} \cdot (y)^k$ er $\binom{n}{k}$
- Opptellingsproblemer
- | | ordnet
rekkefølge viktig
ikke identisk | Uordnet
rekkefølge ikke viktig
er identisk |
|------------------------------------|---|---|
| n /repetisjon
alle funksjoner | n^k | $\binom{n+k-1}{k}$ |
| n /repetisjon
kun injektiv | $n^P_k = \frac{n!}{(n-k)!}$
Måter å trekke k elementer fra n | $\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$
Antall delmengder av n med k elementer |
- Kongruens \rightarrow ikke dele bort felles faktor modulus
 - Komb \rightarrow ikke tell noe 2 ganger
 - Iso morfi er bijektiv f slik at dersom u og v er nabover i A er f(u), f(v) nabover i B ikke \rightarrow antall noder av en viss grad / antall sykler av en viss lengde
 - Antall funksjoner = V^d
 - Noder med odde grad (0 - eukl. vei og ekrets, 2 - ikke eukl. vei, andre - ikke e vei eller ekrets)
 - Forfining: Alle $a \in X$ er delmenge av en $b \in Y$.
 - $[1]_n = [2]_n = \{1, 2\}$ hvis $1 \sim 2$ os $2 \sim 1$
 - $A = g^a \pmod{q} \rightarrow a = \log_g A \pmod{q}$
 - $\sum_{v \in V} \deg(v) = 2 |E|$