Kryptografie založená na eliptických křivkách

Grupy

Grupa

Grupou rozumíme čtveřici $(G, *, e, ^{-1})$ takovou, že $e \in G$, $* : G \times G \to G$, $^{-1} : G \to G$ a splňuje následující axiomy:

- $\forall x \in G : x * e = e * x = x$ (Existence neutrálního prvku)
- $\forall x \in G \; \exists y \in G : x * y = y * x = e$ (Existence inverzního prvku)
- $\forall x, y, z \in G : x * (y * z) = (x * y) * z$ (Asociativita)
  Zkráceně značíme pouze G.

Example

- Celá čísla $\mathbb{Z}$ s operací sčítání.
- Reálná čísla $\mathbb{R}$ s operací sčítání.
- Racionální čísla bez nuly $\mathbb{Q}^*$ s operací násobení.
- Zbytky po dělení n (třídy kongruence).
- Grupa symetrií 5-úhelníku D_5.
- Grupa rotací Rubikovy kostky.
- Grupa permutací 3-prvkové množiny S_3.

Abelovská grupa

Grupa G je abelovská, pokud je grupou a zároveň splňuje:

- $\forall x, y \in G : x * y = y * x$ (Komutativita)

Example

Až na poslední 2 jsou z předchozích příkladů všechny grupy abelovské.

Podgrupa

Podgrupou rozumíme $H \subseteq G$ takovou, že je uzavřená na operaci z původní grupy G. To, že H je podgrupou G značíme $H \leq G$.

Example

- $\mathbb{Z}_7 < \mathbb{Z}$
- $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$
- $D_5 < S_5$

Řád prvku

Řádem prvku x rozumíme přirozené číslo $ord(x)$ takové, že $x^{ord(x)} = e$ a je nejmenší netriviální takové. Pokud žádné takové číslo není, pak má řád 0.

Example

Mějme grupu $\mathbb{Z}_6$. Pak 4 má řád 3., 3 má řád 2, 1 má řád 6.

Generátor

Mějme prvky $x_1, \dots x_n \in G$. Pak nejmenší podgrupu H takovou, že $x_i \in H$ nazýváme grupou generovanou $x_1, \dots x_n$. Značíme jí $\langle x_1, \dots, x_n \rangle$.

Cyklická grupa

Grupa je cyklická, pokud existuje prvek $x \in G$ takový, že $\langle x \rangle = G$.

Example

$\mathbb{Z}_6$ je generovaná prvkem 5.

Věta o cyklických grupách

Každá cyklická grupa je abelovská.

Cvičení

Rozhodněte, zda následující struktury jsou grupa, a pokud ano, pak určete, zda je abelovská, cyklická a jaké jsou její generátory:

- $\mathbb{Z}_{130}$
- $\mathbb{Z}_8^*$
- Symetrie pravidelného čtyřstěnu.
- $\mathbb{R}$ s násobením.

Šifrovací algoritmy

Alice a Bob spolu chtějí komunikovat. Aby mohli použít symetrickou kryptografii, potřebují si sdělit klíč. Jenže neumí to tak, aby je u toho nikdo neodposlouchával. Takže potřebují nějakou krabičku z asymetrické kryptografie.

Diffie-Hellman

DH slouží ke generování klíče k symetrické kryptografii pomocí autentizovatelného kanálu.
Klasické fungování DH:

- Alice a Bob si veřejně sdělí nějaké prvočíslo p a nějaký prvek $g \in \mathbb{Z}_p^*$.
- Alice a Bob si každý zvolí nějaká čísla $a, b \in \mathbb{Z}_{p-1}$.
- Alice spočítá $x = g^a$, Bob $y = g^b$ a vymění si tyto hodnoty.
- Alice spočte $s = y^a$, Bob $s = x^b$. Nyní oba mají stejné číslo s, které znají pouze oni dva a nikdo jiný.

DH + RSA + AES

Chceme zkombinovat vlastnosti RSA a DH, abychom dokázali komunikovat bezpečněji.
Alice chce poslat Bobovi zprávu x. Chce, aby přišla opravdu Bobovi a neposlala ji někomu jinému.

- Bob má svůj soukromý a veřejný klíč RSA, g a p.
- Bob si zvolí b, $B = g^b$, $RSA_s(B)$. Alici pošle $(B, RSA_s(B))$.schéma
- Alice ověří podpis pomocí $RSA_v(B)$.
- Alice zvolí a, $A = g^a$, $k = B^a$. Alice pošle Bobovi $(A, AES(x))$.
- Bob si z DH dopočítá klíč k, rozšifruje $AES(x)$ a přečte zprávu.
- Oba zapomenou a, b, k.
  Tohle má krásnou vlastnost, že ikdyž někdo zjistí Bobův soukromý klíč, tak si už nepřečte, co Alice poslala Bobovi. Nazývá se *perfect forward secrecy*.

Schnorrova grupa

Grupu $\langle g \rangle \leq \mathbb{Z}_p^*$ nazýváme Schnorrovu. Řád prvku g budeme do konce kapitoly značit q.

Generování klíče pro Schnorra

Zvolíme tajné $s \in \mathbb{Z}_q^*$. Spočteme $v = g^s$. $k_s = (s, p, q, g)$, $k_v = (v, p, q, g)$.

Schnorrovo identifikační schéma

Alice chce Bobovi ukázat, že je opravdu Alice. Bob zná veřejný klíč Alice k_v.

- Alice zvolí nonci $r \in \mathbb{Z}_q^*$, spočte $R = g^r \mod p$ a pošle to Bobovi. (Závazek)
- Bob zvolí nepředvídatelně e a pošle ho Alici. (Výzva)
- Alice spočte $y = r - se \mod q$ a y pošle Alici. (Odpověď)
- Bob spočte $v^e g^y \mod p = R$. (Ověření)

Schnorrovo podpisové schéma

Modifikace předchozího algoritmu, abychom mohli podepsat zprávu, kterou jsme poslali.
Podpis:

- Zvolíme nonci $r \in \mathbb{Z}_q^*$, spočteme $R = g^r \mod p$
- $e = hash(R||x) \in \mathbb{Z}_q$
- $y = r - se \mod q$

1. (e, y)
2. (R, y)
   Ověření:
3. $hash((v^e g^y \mod p)||x) = e$
4. $v^{hash(R||x)} g^y \mod p = R$
   Síla používání těchto šifer stojí na problému diskrétního logaritmu, tj že pokud dostaneme nějaké $v = g^s$, pak je velice těžké určit s.

Eliptické křivky

Těleso

Matematickou strukturu $(T, +, *, 0, 1, -, ^{-1})$ nazýváme *tělesem*, pokud splňuje následující podmínky:

- $(T, +, 0, -)$ je abelovská grupa
- $(T \setminus \{0\}, *, ^{-1})$ je grupa
- $\forall x, y, z \in T : a(b + c) = ab + ac$ (distributivita)
- $\forall x, y, z \in T : (b + c)a = ba + ca$

Konečné těleso

Konečné těleso má konečný počet prvků.

Example

- $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$
- $\mathbb{Z}_2$, $\mathbb{F}_{128}$
  V tělesech můžeme dělit a obecně jsou velmi hezké objekty.

Projektivní rovina

Projektivní rovina je takový prostor $(X, L(X))$ bodů a přímek, který splňuje následující axiomy:

- Každé dva různé body leží na právě jedné přímce
- Každé dvě různé přímky se protínají právě v jednom bodě
- Existují alespoň 4 různé body, z nichž žádné tři neleží na přímce
- Existují alespoň 4 různé přímky, z nichž žádné tři se neprotínají v bodě.
  Zpravidla se projektivní roviny konstruují z těles, kde vezmeme vektorový prostor dimenze 3, kde podprostory dimenze 1 tvoří body a podprostory dimenze 2 tvoří přímky.

Example

- Fanova rovina
- Komplexní projektivní rovina

Křivka

Křivka v naší přednášce je množina bodů splňující $f(x, y) = 0$, kde f je polynom ve dvou proměnných. Stupněm křivky rozumíme nejvyšší z součtů mocnin x a y v každém členu z polynomu f. Značíme ho $deg(f)$.

Věta o křížení křivek

Mějme křivky definované f a g. Pak počet křížení bude odpovídat $deg(f) * deg(g)$.

Example

- Křížení kružnice s přímkou.

Eliptická křivka

Eliptickou křivkou rozumíme křivkou definovanou polynomem tvaru: $x^3 + ax + b - y^2$. Budeme jí nazývat E.

Systém trojic na eliptické křivce

Mějme dva body na eliptické křivce E: A, B. Pak $A * B$ rozumíme bod, který dostaneme jako třetí průsečík E a přímky procházející A a B.

Grupa nad eliptickou křivkou

Abychom vyrobili grupu, potřebujeme vzít jeden referenční bod, naprosto libovolný. Budiž to bod 0. Pak $A + B = (A * B) * 0$. Pak $(E, +, 0, -)$ tvoří abelovskou grupu.

Použití

Máme takto vygenerovanou grupu. Ta může být trochu divoká. V ní si vybereme bod A. Z něho vyrobíme podgrupu $\langle A \rangle$. Tato grupa je Schnorrova a můžeme ji tak používat v DH, Schnorrově podpisovém a identifikačním schématu a ElGamalovi.