Elliptic Curves Cryptography

Rizal Afgani

Seminar Matematika Universitas Andalas, Juni 2019

Outline

Kriptografi

Frame subtitles are optional. Use upper- or lowercase letters.

- "Cryptography is the design and analysis of mathematica techniques that enable secure communication in the presence of malicious adversaries"
- Contoh kasus:
  - Pembayaran online
    - Informasi kartu kredit
    - Akun palsu

Kriptografi

Frame subtitles are optional. Use upper- or lowercase letters.

- "Cryptography is the design and analysis of mathematica techniques that enable secure communication in the presence of malicious adversaries"
- Contoh kasus:
  - Pembayaran online
    - Informasi kartu kredit
    - Akun palsu

Kriptografi

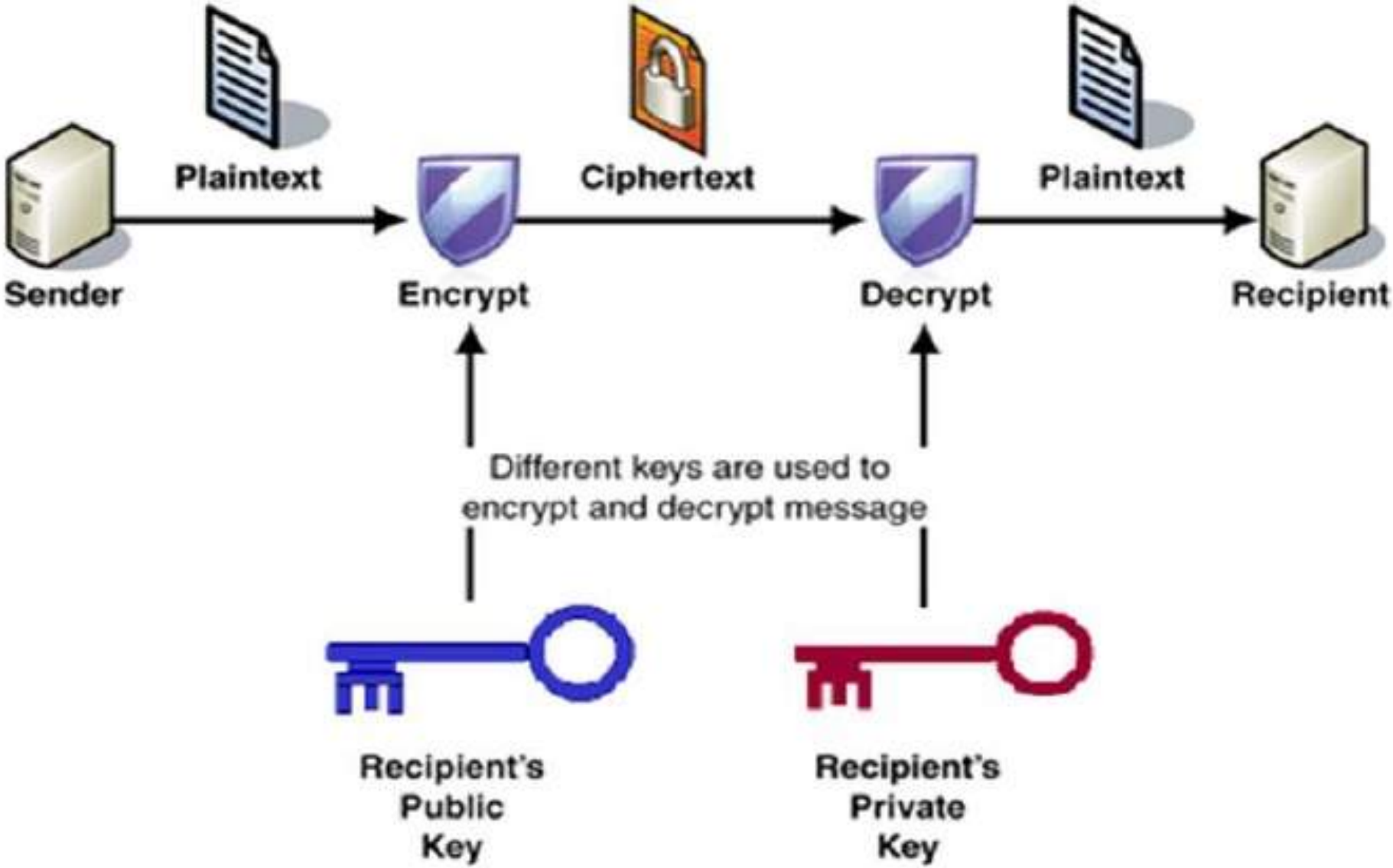
Frame subtitles are optional. Use upper- or lowercase letters.

- "Cryptography is the design and analysis of mathematica techniques that enable secure communication in the presence of malicious adversaries"
- Contoh kasus:
  - Pembayaran online
    - Informasi kartu kredit
    - Akun palsu

Public-key cryptoraphy

- Masing-masing pihak memiliki public-key Q dan private-key d yang mana pasangan (Q, d) memenuhi aturan tertentu tetapi d sulit untuk dihitung jika Q diketahui.
- Ada operasi Enc_Q dan operasi Dec_d
- Operasi Enc_Q menggunakan data public key Q
- Operasi Dec_d menggunakan data private key d

Public-key cryptography



RSA public key encryption

- A akan mengirimkan pesan m ke B
- Pasangan public-key dan private-key (Q_B, d_B) memenuhi aturan berikut
  - pilih secara acak dua buah bilangan prima p dan q dan hitung $n = pq$ dan $\phi = (p-1)(q-1)$
  - $Q_B = (n, e)$ di mana e memenuhi $1 < e < \phi$ dan $gcd(e, \phi) = 1$
  - Hitung $1 < d_B < \phi$ yang memenuhi $ed \equiv 1 \pmod{\phi}$
- B menyimpan kunci privat d_B
- Pesan $0 < m < n$ dienkripsi menjadi $m^e \pmod{n}$.
- Tingkat keamanan dari enkripsi ini bergantung dari kekompleksan untuk mencari factor prima p, q dari n

RSA public key decryption

- Berdasarkan Fermat's little theorem

$$m^{ed} \equiv m \pmod{n}$$

- Pesan m^e dipecahkan dengan mengambil pangkat d dari m^e.

ElGamal public key encryption

- A akan mengirimkan pesan m ke B.
- B mempublikasikan kuncinya sebagai berikut
  - Sebuah grup abelian G
  - Sebuah elemen P di G yang memiliki order besar berupa bilangan prima p
  - Sebuah elemen $Q = sP$
- B menyimpan kunci privatnya sebuah bilangan bulat $s < p$
- Menemukan s jika diketahui G, P dan Q disebut sebagai discrete logarithm problem
- Tingkat keamanan kriptografi ini bergantung pada order dari elemen P di G.
- A mengirimkan $(kP, m + kQ)$ ke B di mana k adalah sebuah bilangan bulat yang disimpan rahasia oleh A. kP,$m + kQ \in G$

ElGamal public key decryption

- B menerima $(kP, m + kQ)$ di mana kP,$m + kQ \in G$
- B memecahkan $(kP, m + kQ)$ dengan mengurangkan $m + kQ$ dengan skP
- Karena $Q = sP$ maka $m + kQ - skP = m$

Outline

Aljabar

- Struktur Aljabar: Grup, Gelanggang, Lapangan
- Bekerja dengan sistem yang didefinisikan axiomatically namun sering muncul di dalam matematika.
- Apa gunanya?
  - Mendapatkan pemahaman yang lebih baik tentang kasus yang dihadapi
  - Dapat diaplikasikan secara lebih luas

Grup Abelian

- Himpunan G dengan satu operasi $\bullet$ disebut grup Abelian jika memenuhi syarat-syarat berikut:
  - untuk semua x, y, z elemen G berlaku $x \bullet (y \bullet z) = (x \bullet y) \bullet z$
  - untuk semua x, y elemen G berlaku $x \bullet y = y \bullet x$
  - terdapat elemen identitas e di G yaitu elemen G yang memenuhi $e \bullet x = x$ untuk seluruh x di G
  - untuk sembarang elemen x di G terdapat elemen y yang memenuhi $x \bullet y = e$
- Contoh: Himpunan bilangan bulat $\mathbb{Z}$, Himpunan bilangan rasional $\mathbb{Q}$, Himpunan bilangan real $\mathbb{R}$
- Jika G himpunan hingga orde dari G adalah jumlah elemen dari G. Orde dari sebuah elemen g di G adalah bilangan bulat terkecil k supaya $g^k = e$

Modular Number

- $a \equiv b \bmod q$ berarti ada bilangan bulat n yang memenuhi $a - b = n.q$.
- Himpunan bilangan bulat modular dilambangkan dengan $\mathbb{Z}/q\mathbb{Z}$
- Contoh: jam dinding ($\mathbb{Z}/12\mathbb{Z}$)

Gelanggang komutatif

- Himpunan R dengan dua buah operasi $+$ dan $\times$ disebut gelanggan komutatif jika:
  - $(R, +)$ adalah grup Abelian
  - Untuk sembarang elemen x, y, z di R berlaku $x \times (y \times z) = (x \times y) \times z$
  - Untuk sembarang elemen x, y di R berlaku $x \times y = y \times x$
  - terdapat elemen tunggal 1 di R yang memenuhi $1 \times x = x$ untuk seluruh elemen x di R
  - untuk seembarang elemen x, y, z di R berlaku $x \times (y + z) = (x \times y) + (x \times z)$
- Contoh: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Lapangan(fields)

- Misalkan k adalah lapangan
- Operasi penjumlahan $(+, 0)$ dan operasi perkalian $(\times, 1)$
- Setiap elemen $a \in k$ memiliki balikan penjumlahan $-a$
- Setiap elemen $a \in k$ kecuali 0 memiliki balikan perkalian $\frac{1}{a}$
- Contoh: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ untuk p bilangan prima.

Geometri

- Sulit untuk mendefinisikan apa itu geometry
- Konsep: titik, garis, bidang, kurva, surface, ...
- Irisan garis dengan garis, kurva dengan kurva, kurva dengan surface, ...

Topik-topik Geometri

- Geometri Euclid
- Topology
- Geometri diferensial
- Riemannian Geometry
- Complex Geometry
- Algebraic Geometry
- Symplectic Geometry
- Noncommutative Geometry

Outline

Algebraic Geometry

- Algebraic Geometry mempelajari solusi persamaan polyomial
- Polynomial: $5x + 1, 5x^2 + 6x + 7, y^2 + 9x^3 + 8x + 7$
- Misalkan $f(x, y)$ adalah polynomial dalam dua variabel x, y. Solusi dari f adalah himpunan titik-titik $(a, b) \in k \times k$ yang memenuhi $f(a, b) = 0$.
- Polynomial yang kita tinjau bisa memiliki lebih dari dua variabel. Kita juga bisa meninjau solusi dari dua atau lebih polynomial.

Algebraic Geometry

- Himpunan polynomial dengan n buah variabel $x_1, \ldots, x_n$ dan koefisien di k membentuk sebuah gelanggang yang dilambangkan dengan $k[x, \ldots, x_n]$
- Untuk setiap solusi persamaan polynomial kita asosiasikan sebuah gelanggang R yang dibangun dari $k[x_1, \ldots, x_n]$.
- Terdapat sebuah cara untuk menerjemahkan sifat-sifat aljabar dari R ke dalam sifat-sifat geometri dari solusi persamaan polynomial tersebut.
- Polynomial dipandang sebagai fungsi pada k^n. Kita sebut funsi regular
- Di samping polynomial, kita juga menggunakan fungsi rasional, yaitu fungsi yang berbentuk $\frac{f(x,y)}{g(x,y)}$ di mana f, g adalah polynomial
- Kita gunakan panah putus-putus $\dashrightarrow$ untuk menyatakan fungsi rasional $\frac{f}{g} : X \dashrightarrow k$.

Projective Geometry

- Titik-titik pada $\mathbb{P}_k^n$ adalah garis-garis pada k^{n+1}.
- Pada $\mathbb{P}_k^n$ kita menggunakan homogenous coordinate.
  - Koordinat sebuah titik $p \in \mathbb{P}_k^n$ adalah $(a_1 : \ldots : a_n)$ di mana tidak semua $a_i = 0$
  - $(\lambda a_1 : \lambda a_2 : \ldots : \lambda a_n)$ dan $(a_1 : a_2 : \ldots : a_n)$ memberikan titik yang sama untuk semua $0 \neq \lambda \in k$
- $\mathbb{P}_k^2 = \{(a_1 : a_2 : a_3) | a_i \in k \text{ dan tidak semua } a_i = 0\}$
-

$$\begin{aligned} \{(a_1 : a_2 : a_3) | a_i \in k, a_3 = 1\} &\rightarrow k \times k \\ (a_1 : a_2 : a_3) &\mapsto (a_1, a_2) \end{aligned}$$

adalah bijeksi dan isomorphisma.

Projective Geometry

- Polynomial tidak memberikan fungsi pada $\mathbb{P}_k^n$.
- Fungsi rasional $\frac{f}{g}$ di mana f dan g adalah homogeneous polynomial dengan $deg\, f = deg\, g$ memberikan fungsi rasional pada $\mathbb{P}_k^n$.

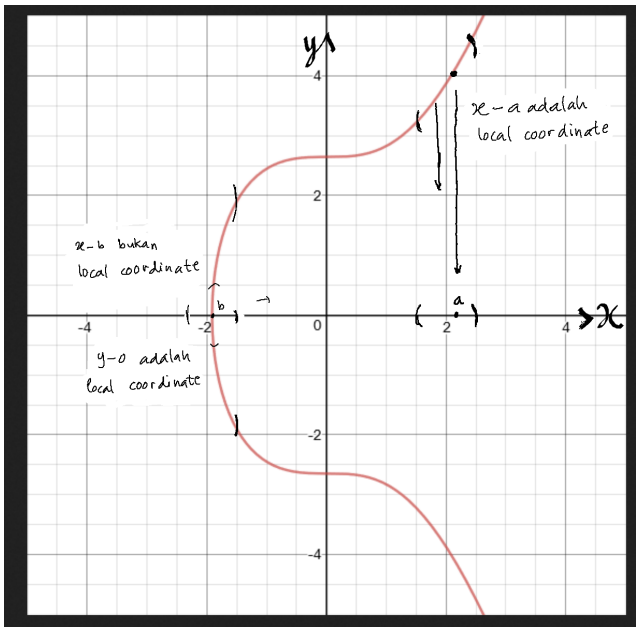
Kurva Eliptik

- Kurva eliptik adalah subhimpunan $E(k) \subset \mathbb{P}_k^2$ yang memenuhi $a_2^2 a_3 - a_1^3 - A a_1 a_3^2 - B a_3^3 = 0$ di mana $A, B \in k$ adalah konstanta yang memenuhi $4A^3 + 27B^2 \neq 0$.
- Kurva elliptik adalah kurva di dalam $k \times k$ yang didefinisikan oleh persamaan berbentuk

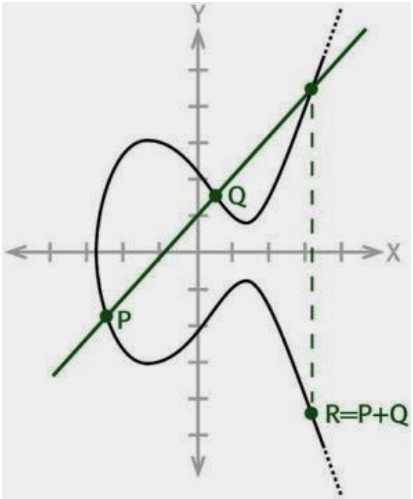
$$\left(\frac{y}{z}\right)^2 = \left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B$$

digabung dengan sebuah titik di ketakhinggaan yang kita notasikan dengan ∞.

Local Coordinate

- $E(k)$ adalah kurva eliptik dan $p \in E(k)$. Local koordinat di sekitar titik p adalah fungsi rasional $z : E(k) \dashrightarrow k$ yang bersifat satu-satu pada sebuah subhimpunan buka $U \subseteq E(k)$ yang mengandung p
- 

Operasi grup pada kurva eliptik



Diberikan dua buah titik P dan Q pada kurva eliptik $E(k)$. Terdapat sebuah garis unik λ yang menghubungkan P dan Q. λ dan $E(k)$ beririsan pada 3 buah titik yaitu $P, Q, -R$. $P + Q$ didefinisikan sebagai R di mana R adalah refleksi dari $-R$ terhadap sumbu x.

Order dari Kurva Elliptik

- Menghitung order dari sebuah kurva eliptik sangat penting dalam membangun sebuah sistem kriptografi karena tingkat keamanan sistem tersebut bergantung pada orde dari elemen $P \in G$
- Teorema Hasse memberikan perkiraan akan orde dari kurva elliptik.
- Pembuktian teorema Hasse menggunakan konsep divisor.

Divisor

- Pilih sebuah kurva elliptik $E(k)$. Sebuah divisor adalah jumlah formal dari titik-titik di $E(k)$ dengan kata lain sebuah divisor D pada $E(k)$ dapat ditulis sebagai

$$\sum_{1 \leq i \leq I} n_i [P_i]$$

  di mana $n_i \in \mathbb{Z}$ dan $P_i \in E(k)$.
- $Div\, E(k)$ adalah grup dengan anggota adalah divisor-divisor pada $E(k)$.
- $Div\, E(k)$ adalah grup yang sangat besar dan tidak menarik untuk dipelajari.
- Grup yang menarik untuk dipelajari adalah $Cl(E(k))$ yang diperoleh dari $Div\,(E(k))$ dengan menjadikan principal divisor sebagai identitas 0.
- $Cl(E(k))$ disebut sebagai divisor class group

Principal divisor

- Jika $f(P) \neq 0$ maka $ord_P f = 0$. Jika $f(P) = 0$ maka $f = z^n.g(z)$ dan $ord_P f = n$. Untuk fungsi rasional $\frac{f}{g}$, $ord_P \frac{f}{g} = ord_P f - ord_P g$.
- Setiap fungsi rasional f memberikan sebuah divisor

$$div(f) = \sum ord_P(f)[P]$$

- Jika $D = div\,(f)$ untuk sebuah fungsi rasional f, kita sebut D sebagai principal divisor.
- $Cl(E(k)) := Div(E(k))/\{\text{principal divisors}\}$
- Ada sebuah grup homomorphisma $deg : Div(E(k)) \to \mathbb{Z}$, $\sum_{1 \leq i \leq l} n_i[P_i] \mapsto \sum_{1 \leq i \leq l} n_i$. Grup homomorfisma ini kemudian dapat didefinisikan pada $Cl(E(k))$.

Contoh principal divisor

Diberikan dua buah titkik $P_0 \neq P, Q \in E(k)$. Kita dapatkan garis λ yang didefinisikan oleh persamaan $ax + by + cz$ dan sebuah titik R yang merupakan irisan garis λ dengan kurva eliptik $E(k)$. Fungsi rasional $f = \frac{z}{ax+by+cz}$ bernilai 0 pada titik $(0 : 1 : 0)$ dan pole pada P, Q, R. Jika $b \neq 0$ maka $(0 : 1 : 0)$ bukanlah elemen dari λ sehingga $ord_{P_0} f = 3$ dan

$$div(f) = 3[P_0] - [P] - [Q] - [R]$$

sehingga di dalam $Cl(k)$ kita dapat menuliskan $[P] + [Q] + [R] = 3[P_0]$. Jika $b = 0$ maka λ adalah garis paralel dengan sumbu y dan $(0 : 1 : 0)$ adalah elemen dari garis λ dan Q adalah refleksi dari P terhadap sumbu x sehingga

$$div(f) = 2[P_0] - [P] - [-P].$$

Degree 0 divisor dan operasi grup pada kurva eliptik

- Definisikan $Cl(E(k))^0 := ker(deg : Cl(E(k) \to \mathbb{Z})$.
- Operasi grup pada $Cl(E(k))^0$ mendeskripsikan operasi grup pada $E(k)$.

Theorem

Pemetaan $E(k) \to Cl(E(k))^0, P \mapsto [P] - [P_0]$ *adalah sebuah grup isomorfisma.*

Degree 0 divisor dan operasi grup pada kurva eliptik

Proof.

Karena $[P] + [Q] + [-(P+Q)] = 3[P_0]$ dan $[P+Q] + [-(P+Q)] = 2[P_0]$ maka

$$([P] - [P_0]) + ([Q] - [P_0]) = ([P+Q] - [P_0])$$