Elliptic Curve Cryptography (ECC) - 1

Bahan Kuliah Keamanan Data

Sevi **Nurafni**

Fakultas Sains dan Teknologi
Universitas Koperasi Indonesia 2025

Get to Know

- Sebagian besar kriptografi kunci-publik (seperti RSA, ElGamal, Diffie-Hellman) menggunakan bilangan bulat yang sangat besar dalam komputasinya.
- Sistem seperti itu memiliki masalah yang signifikan dalam menyimpan, memproses kunci dan pesan, dan membutuhkan waktu komputasi yang lama.
- Sebagai alternatif adalah melakukan komputasi berbasis kurva eliptik (elliptic curve).
- Kriptografi yang menggunakan kurva eliptik dinamakan Elliptic Curve Cryptography (ECC).
- Komputasi dengan kurva eliptik menawarkan keamanan yang sama dengan algoritma-algoritma tersebut namun dengan ukuran kunci yang lebih kecil.

- ECC adalah kriptografi kunci-publik yang relatif lebih baru usianya.
- Dikembangkan oleh Neal Koblitz dan Victor S. Miller tahun 1985.
- Klaim: Panjang kunci ECC lebih pendek daripada kunci RSA, namun memiliki tingkat keamanan yang sama dengan RSA.
- Contoh: kunci ECC sepanjang 160-bit menyediakan tingkat keamanan yang sama dengan 1024-bit kunci RSA.
- Keuntungan: dengan panjang kunci yang lebih pendek, membutuhkan memori dan komputasi yang lebih sedikit.
- Cocok untuk piranti nirkabel, dimana prosesor, memori, umur batere terbatas.

Teori Aljabar Abstrak

- Sebelum membahas ECC, perlu dipahami konsep aljabar abstrak yang mendasarinya.

- Konsep aljabar abstrak:
    1. Grup (group)
    2. Medan (field)

Grup

- Grup (group) adalah sistem aljabar yang terdiri dari:
    - Sebuah himpunan G
    - Sebuah operasi biner $*$

Sedemikian sehingga untuk semua elemen a, b, dan c di dalam G berlaku aksioma berikut:

1. Closure: $a * b$ harus berada di dalam G
2. Asosiatif: $a * (b * c) = (a * b) * c$
3. Elemen netral: terdapat $e \in G$ sedemikian sehingga $a * e = e * a = a$
4. Elemen invers: terdapat $a' \in G$ sedemikian sehingga $a * a' = a' * a = e$

- Notasi $< G, * >$

- $< G, + >$ menyatakan sebuah grup dengan operasi penjumlahan.
- $< G, \cdot >$ menyatakan sebuah grup dengan operasi perkalian

Contoh-contoh grup:

1. $< \mathbb{R}, + >$: grup dengan himpunan bilangan riil dengan operasi $+$

   $e = 0$ dan $a' = -a$

2. $< \mathbb{R}^*, \cdot >$: grup dengan himpunan bilangan riil tidak nol (yaitu, $R^* = R - \{0\}$) dengan operasi kali ($\cdot$)

   $e = 1$ dan $a' = \dfrac{1}{a} = a^{-1}$

3. $< \mathbb{Z}, + >$ dan $< \mathbb{Z}, \cdot >$ masing-masing adalah grup dengan himpunan bilangan bulat (integer) dengan operasi $+$ dan $\cdot$

4. $< Z_n, \oplus >$: grup dengan himpunan integer modulo n, yaitu

$Z_n = \{0,1,2,\ldots,n-1\}$ dan $\oplus$ adalah operasi penjumlahan modulo n.

Contoh: $n = 5$, $Z_n = \{0,1,2,3,4\}$, $(3 \oplus 4) = (3 + 4)$ mod $5 = 2$

$< Z_p, \oplus >$: grup dengan himpunan integer modulo p, p adalah bilangan prima, yaitu

$Z_p = \{0,1,2,\ldots,p-1\}$ dan $\oplus$ adalah operasi penjumlahan modulo p.

$< Z^*_p , \otimes >$: dengan himpunan integer bukan nol, p adalah bilangan prima, yaitu

$Z^*_p = \{1,2,\ldots,p-1\}$dan $\otimes$ adalah operasi perkalian modulo p.

- Sebuah grup $< G, * >$ dikatakan group komutatif atau grup abelian jika berlaku aksioma komutatif $a * b = b * a$ untuk semua a, b elemen G

- $< R, + >$ dan $< R, \cdot >$ adalah abelian
- $< Z, + >$ dan $< Z, \cdot >$ adalah abelian

- tetapi, $< M, \cdot >$, dengan M adalah himpunan matriks 2 x 2 dengan determinan $\neq 0$ bukan abelian (tanya kenapa?)

Medan (Field)

- Medan (*field*) adalah himpunan elemen (disimbolkan dengan F) dengan dua operasi biner, biasanya disebut penjumlahan $(+)$ dan perkalian $(\cdot)$.
- Sebuah struktur aljabar $< F, + , \cdot >$ disebut medan jika dan hanya jika:
  1. $< F, + >$ adalah grup abelian
  2. $< F - \{0\}, \cdot >$ adalah grup abelian
  3. Operasi · menyebar terhadap operasi + (sifat distributif)

     Distributif: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

     $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$

- Jadi, sebuah medan memenuhi aksioma: *closure*, komutatif, asosiatif, dan distributif

- Contoh medan:
  - medan bilangan bulat, $< \mathbb{Z}, +, \cdot >$
  - medan bilangan riil, $< \mathbb{R}, +, \cdot >$
  - medan bilangan rasional $(\frac{p}{q})$ $< \mathbb{Q}, +, \cdot >$

- Sebuah medan disebut berhingga (*finite field*) jika himpunannya memiliki jumlah elemen yang berhingga.

  Jika jumlah elemen himpunan adalah n, maka notasinya F_n

  Contoh: F_2 adalah medan dengan elemen 0 dan 1

- Medan berhingga sering dinamakan juga Galois Field, untuk menghormati Evariste Galois, seorang matematikawan Perancis (1811 – 1832)

Medan Berhingga F_p

- Kelas medan berhingga yang penting adalah F_p
- F_p adalah adalah medan berhingga dengan himpunan bilangan bulat $\{0,1,2,\ldots,p-1\}$ dengan p bilangan prima, dan dua operasi yang didefinisikan sbb:
    1. Penjumlahan

       Jika $a, b \in F_{p,}$ maka $a + b = r$, yang dalam hal ini

       $r = (a + b)$ mod p, $0 \leq r \leq p - 1$
    2. Perkalian

       Jika $a, b \in F_{p,}$ maka $a \cdot b = s$, yang dalam hal ini

       $s = (a \cdot b)$ mod p, $0 \leq s \leq p - 1$

Contoh: F_{23} mempunyai anggota $\{0,1,2,\cdots,22\}$

Contoh operasi aritmatika:

$12 + 20 = 9$ (karena $12 + 20 = 32$ mod $23 = 9$}

$8 \cdot 9 = 3$ (karena $8 \times 9 = 72$ mod $23 = 3$}

$5 + 4 = \cdots$

$7 \cdot 4 = \cdots$

Medan Galois (*Galois Field*)

- Medan Galois adalah medan berhingga dengan p^n elemen, p adalah bilangan prima dan $n \geq 1$.
- Notasi: $GF(p^n)$
- Kasus paling sederhana: bila $n = 1 \rightarrow GF(p)$, yang dalam hal ini elemen-elemennya dinyatakan di dalam himpunan $\{0,1,2,\ldots, p-1\}$ dan operasi penjumlahan dan perkalian dilakukan dalam modulus p.

$p = 2 \rightarrow$ $GF(2)$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$p = 3 \rightarrow$ $GF(3)$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- Contoh: Bentuklah tabel perkalian untuk $GF(11)$, kemudian tentukan solusi untuk $x^2 \equiv 5(\bmod 11)$

·	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	4	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

$x^2 \equiv 5 \pmod{11}$

Maka:

$x^2 = 16 \rightarrow x_1 = 4$

$x^2 = 49 \rightarrow x_2 = 7$

Cara lain: cari elemen diagonal = 5, lalu ambil elemen mendatar atau elemen Vertikalnya (dilingkari).

Latihan

- Bentuklah tabel perkalian untuk $GF(7)$, kemudian tentukan solusi untuk $x^2 \equiv 4 \pmod 7$

Galois Field $GF(2^m)$

- Disebut juga medan berhingga biner
- $GF(2^m)$ atau F_2^m adalah ruang vektor berdimensi m pada $GF(2)$. Setiap elemen di dalam $GF(2^m)$ adalah integer dalam representasi biner sepanjang maksumal m bit.
- String biner $a_{m-1}a_{m-2}\cdots a_1a_0$ $a_i \in \{0,1\}$, dapat dinyatakan dalam polinom $a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$
- Jadi, setiap $a \in GF(2^m)$ dapat dinyatakan sebagai

$$a = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0$$

- Contoh: $m = 4 \rightarrow a = 1101$ dapat dinyatakan dengan $x^3 + x^2 + 1$

Operasi aritmetika $GF(2^m)$

- Misalkan $a = (a_{m-1} \cdots a_1 a_0)$ dan $b = (b_{m-1} \cdots b_1 b_0) \in$ GF(2^m)
- **Penjumlahan**:

  $a + b = c = (c_{m-1} \cdots c_1 c_0)$ yang dalam hal ini $c_i = (a_i + b_i)$ mod 2, $c \in GF(2^m)$
- **Perkalian**: $a \cdot b = c = (c_{m-1} \cdots c_1 c_0)$ yang dalam hal ini c adalah sisa pembagian polinom $a(x) \cdot b(x)$ dengan irreducible polynomial derajat m, $c \in GF(2^m)$

Contoh: Misalkan $a = 1101 = x^3 + x^2 + 1$ dan $b = 0110 = x^2 + x$

a dan $b \in GF(2^4)$

(i) $a + b = (x^3 + x^2 + 1) + (x^2 + x) = x^3 + 2x^2 + x + 1 \pmod 2$

Bagi tiap koefisien dengan 2,
lalu ambil sisanya

$= x^3 + 0x^2 + x + 1$

$= x^3 + x + 1$

Dalam representasi biner:

1101

0110 +

1011 → sama dengan hasil operasi XOR

$\therefore\ a + b = 1011 = a$ XOR b

Latihan

Diberikan dua elemen dari $GF(2^4)$:

- $a = 1101 = x^3 + x^2 + 1$
- $b = 0110 = x^2 + x$

Hitung $a + b$ di $GF(2^4)$. Tuliskan dalam bentuk biner dan polinomial

(ii) $a \cdot b = (x^3 + x^2 + 1) \cdot (x^2 + x) = x^5 + 2x^4 + x^3 + x^2 + x \pmod 2$

$= x^5 + x^3 + x^2 + x = 10110$

Karena $m = 4$ hasilnya direduksi menjadi derajat < 4 oleh sebuah *irreducible polynomial* $f(x) = x^4 + x + 1$

Proses pembagiannya ditunjukkan sebagai berikut:

$$\begin{array}{r|l} & x \\ \hline x^4 + x + 1 & x^5 + x^3 + x^2 + x \\ & x^5 + \phantom{x^3 +{}} x^2 + x \quad - \\ \cline{2-2} & \qquad x^3 \quad \rightarrow \text{ sisa pembagian} \end{array}$$

Jadi, $(x^5 + x^3 + x^2 + x) \bmod f(x) = x^3 = 1000$

$\therefore\ a \cdot b = 1000$

Note: Sebuah polinom dikatakan tidak dapat direduksi (*irreducible*) jika ia tidak dapat dinyatakan sebagai perkalian dari dua buah polinom lain (kecuali 1 dan dirinya sendiri).
Polinom $x^2 + 1$ dan $x^4 + x + 1$ adalah *irreducible* di dalam $GF(2^n)$, tetapi polinom $x^5 + x^2 + x + 1$ *reducible* karena
$x^5 + x^2 + x + 1 = (x^5 + x^2 + 1) \cdot (x^2 + 1)$

Latihan

Diberikan dua elemen dari $GF(2^4)$:

- $a = 1011 = x^3 + x + 1$
- $b = 0101 = x^2 + 1$

Dengan *irreducible polynomial* $f(x) = x^4 + x + 1$

Hitung $a \cdot b$ mod $f(x)$ di $GF(2^4)$. Tuliskan dalam bentuk biner dan polinomial

SELAMAT BELAJAR