Analisis Pohlig-Hellman Attack untuk Menentukan Kekuatan Elliptic Curve Cryptography

Rexy Gamaliel Rumahorbo – 13519010
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): rexygamalielr@gmail.com

***Abstract*— ECC merupakan salah satu algoritma kriptografi yang banyak digunakan karena efisiensinya dalam kebutuhan komputasi yang lebih sedikit. Elliptic Curve Discrete Logarithm Problem merupakan teori yang mendasari keandalan ECC. Teori ini menyatakan bahwa jika diberikan suatu grup berhingga E(Fp) serta persamaan kurva eliptik tertentu, serta diketahui titik P dan Q pada kurva eliptik sehingga P = kQ, maka sangat sulit untuk menentukan k dari persamaan tersebut. Namun, pada konfigurasi ECC perlu diperhatikan karena dapat mempengaruhi kekuatan ECC tersebut. Pohlig-Helmann Attack merupakan salah satu serangan pada ECC yang mengeksploitasi konfigurasi ECC yang lemah, tepatnya bilangan prima p yang digunakan dalam membentuk medan terbatas pada ECC.**

Keywords—kurva eliptik; ECDLP; Pohlig-Hellman attack;

I. PENDAHULUAN

Kriptografi merupakan salah satu ilmu yang penting dalam perkembangan teknologi digital. Semakin berkembangnya kebutuhan akan informasi didampingi dengan kebutuhan akan keamanan dalam pertukaran informasi digital. Kriptografi merupakan ilmu yang memplejarai proses pengamanan informasi dengan menubgah suatu pesan yang bermakna menjadi suatu pesan acak yang disebut cipherteks, yang dapat dikembalikan menjadi pesan semula. Hal ini dilakukan dengan tujuan agar pihak yang tidak berwenang tidak dapat mendapatkan informasi dari pesan tersebut. Oleh sebab itu, kriptografi umumnya digunakan untuk mengamankan pesan digital yang ditransmisikan melalui media tertentu seperti internet agar pertukaran informasi antara dua pihak dapat berlangsung dengan aman.

Hingga saat ini, telah banyak algoritma kriptografi yang dikembangkan. Saat ini, kita telah memasuki masa kriptografi modern, yakni kriptografi yang didukung dengan penggunaan komputer. Hal ini didukung dengan berkembang pesatnya teknologi komputasi dengan komputer sehingga kriptografi menjadi semakin efektif dan semakin aman. Salah satu algoritma kriptografi modern yang saat banyak digunakan adalah kriptografi kunci publik dengan menggunakan kurva eliptik. Hal ini disebut juga sebagai kriptografi kurva eliptik (ECC). Kriptografi kurva eliptik merupakan salah satu algoritma kriptografi yang paling efisien dan aman, sehingga banyak digunakan.

Namun begitu, selain mengembangkan keamanan algoritma kriptografi ini, para ilmuwan juga berusaha mencari titik kelemahan kriptografi kurva eliptik dalam rangka meningkatkan keamanan kriptografi kurva eliptik yang digunakan. Berbagai algoritma dikembangkan untuk memecahkan kekuatan ECC, salah satunya adalah *Pohlig-Hellman attack*. Pada makalah kali ini akan dibahas bagaimana algoritma Pohlig-Hellman digunakan untuk menentukan kekuatan suatu kriptografi kurva eliptik.

II. LANDASAN TEORI

A. Algoritma Kriptografi Kunci Publik

Algoritma kriptografi kunci publik merupakan algoritma kriptografi yang menggunakan sepasang kunci berbeda yang biasa disebut kunci privat dan kunci publik. Sesuai namanya, kunci privat hanya diketahui pihak yang memilikinya sementara kunci publik dapat diketahui publik. Kriptografi kunci publik termasuk ke dalam kriptografi kunci asimetris karena kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda.

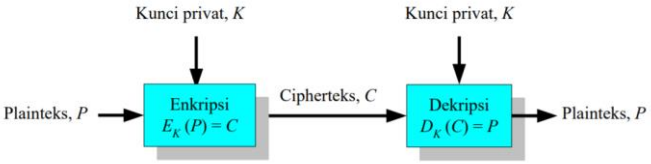

Fig. 1. Skema Kriptografi Kunci publik. *(figure caption)*

Setiap pihak yang terlibat dalam kriptografi kunci publik memiliki sepasang kunci: kunci publik untuk mengenkripsi pesan dan kunci privat untuk mendeskripsi pesan. Dalam skenario dunia nyata, pihak pengirim pesan mengekripsi pesan yang akan dikirim dengan kunci publik penerima pesan sehingga menghasilkan sebuah cipherteks. Setelah itu, penerima pesan mendekripsi cipherteks tersebut dengan kunci privat yang dimilikinya.

Makalah mengenai kriptografi kunci publik berjudul "New Directions in Cryptography" pertama kali ditulis oleh Whitfield Diffie dan Martin E. Hellman pada tahun 1976.

B. Teorema Grup/Group Theory

1) Grup

Sebuah grup merupakan sebuah sistem aljabar yang terdiri dari sebuah himpunan G dan operasi biner ·

(dinotasikan dengan $< G,\cdot >$) sedemikian sehingga untuk semua elemen $a, b, c \in G$ berlaku aksioma:

- *Closure*.
  Hasil dari $a \cdot b$ ada di dalam G
- Asosiatif.
  $$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
- Elemen identitas.
  Terdapat elemen identitas $e \in G$ sedemikian sehingga
  $$e \cdot a = a \cdot e = a$$
- Elemen invers.
- Untuk elemen setiap a terdapat elemen invers $a' \in G$ sedemikian sehingga
  $$a \cdot a' = a' \cdot a = e$$

2) Orde

Orde sebuah grup G (dinotasikan dengan $|G|$) merupakan banyaknya elemen pada himpunan elemen grup G. Sebuah grup berhingga memiliki banyak elemen yang berhingga.

3) Subgrup

Sebuah subgrup H dari grup $< G,\cdot >$ merupakan grup yang elemen-elemennya merupakan subhimpunan dari himpunan elemen G. Akibatnya, elemen identitas $e \in G$ juga terdapat pada H dan untuk $h_1, h_2 \in H$ maka $h_1 \cdot h_2 \in H$ dan untuk setiap $h \in H$ terdapat elemen invers $h' \in H$.

4) Grup Siklik

Grup siklik atau grup monogen merupakan grup yang dibangkitkan oleh sebuah elemen. Pada sebuah grup siklik G dengan operasi $\cdot$ terdapat elemen g sedemikian sehingga setiap elemen pada G dapat dinyatakan sebagai g^k, $k \in N$, yakni setiap elemen pada G dapat diperoleh dengan menerapkan operasi $\cdot$ terhadap g secara berulang sebanyak k kali. Sebuah subgroup yang dibangkitkan oleh g dinotasikan sebagai $\langle g \rangle$. Sebuah grup siklik dengan orde n terdiri atas elemen-elemen $\{e, g, g^2, g^3, \dots, g^{n-1}\}$, dalam hal ini $|\langle g \rangle| = \#\langle g \rangle = n$.

5) Grup Abelian

Sebuah grup G dengan operasi $\cdot$ dikatakan sebagai grup Abelian atau grup komutatif jika untuk setiap elemen $a, b \in G$ berlaku $a \cdot b = b \cdot a$.

C. Medan/Field

1) Definisi

Sebuah medan F merupakan himpunan elemen dengan dua operasi biner yang terdefinisi pada himpunan tersebut: operasi penjumlahan $+$ dan operasi perkalian $\cdot$

Untuk setiap a, b, c pada sebuah medan F berlaku aksioma:

- Asosiatif.
  $$a + (b + c) = (a + b) + c$$
  $$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$
- Komutatif.
  $$a + b = b + a$$
  $$a \cdot b = b \cdot a$$
- Elemen identitas. Terdapat dua buah elemen berbeda 0 dan 1 sedemikian sehingga
  $$a + 0 = 0 + a = a$$
  $$a \cdot 1 = 1 \cdot a = a$$
- Elemen invers.
  Untuk setiap elemen a terdapat elemen $-a$ sedemikian sehingga
  $$a + (-a) = 0$$
  Untuk setiap elemen a terdapat elemen
  $$\frac{1}{a} = a^{-1} \neq 0$$
  sedemikian sehingga
  $$a^{-1} \cdot a = 1$$
- Distributif.
  Berlaku sifat distributif operasi perkalian terhadap penjumlahan, yakni
  $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

2) Medan Galois/Galois Field

Medan Galois/*Galois Field* merupakan medan dengan banyak elemen berhingga. Orde/banyak elemen pada medan Galois adalah p^k untuk sebuah bilanga prima p dan bilangan bilangan asli k.

Salah satu contoh medan Galois adalah F_p, yang merupakan medan yang dibentuk dari modulo p, di mana p adalah sebuah bilangan prima. Elemen-elemen F_p pada adalah $\{0,1,2,3, \dots, p-1\}$.

D. Kriptografi Kurva Elliptic/Elliptic Curve Crptography

Kriptografi Kurva Eliptik/*Elliptic Curve Cryptography* (ECC) merupakan kriptografi yang menggunakan kurva eliptik sebagai dasar algoritma kriptografinya.

1) Kurva Eliptik

Kurva eliptik merupakan kurva yang dibentuk dari persamaan

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

pada sebuah medan F.

2) Titik pada Kurva Eliptik

$E(F)$ menyatakan himpunan semua titik yang memenuhi persamaan kurva eliptik pada medan F, atau dengan kata lain

$$E(F) = \{(x, y) \in F^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

di mana O merupakan sebuah titik pada tak hingga sekaligus merupakan elemen identitas pada $E(F)$.

Namun, dalam hal ini karakteristik medan F bernilai >3 sehingga persamaan kurva eliptik tersebut dapat disederhanakan menjadi

$$y^2 = x^3 + ax + b$$

sehingga

$$E(F) = \{(x, y) \in F \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

Pada penggunaan kriptografi, digunakan medan F_p, yakni medan yang dibentuk dari bilangan prima p, dengan anggota $\{0,1,2,3,\dots,p-1\}$.

3) Operasi pada Kurva Eliptik

Untuk suatu kurva eliptik E, terdefinisi operasi $+$ pada himpunan titik $E(F)$ yang didefinisikan sebagai berikut:

Diberikan dua buah titik $P_1(x_1, y_1)$ dan $P_2(x_2, y_2)$, $P_1, P_2 \in E(F)$, maka titik $R(x_r, y_r)$, $R = P_1 + P_2$ dapat dihitung dengan:

- Jika $P_1 = O$ maka $R = P_2$; jika $P_2 = O$ maka $R = P_1$
- Jika $x_1 = x_2$ dan $y_1 = -y_2$, maka $R = O$
- $x_r = m^2 - x_1 - x_2$
  $y_r = m(x_1 - x_r) - y_1$,
  di mana nilai m ditentukan sebagai berikut:
  - Jika $P_1 = P_2$ dan $y_1 \neq 0$,
    maka $m = \frac{3x_1^2 + a}{2y_1}$
  - Jika $P_1 \neq P_2$, maka $m = \frac{y_1 - y_2}{x_1 - x_2}$

4) Elliptic Curve Discrete Logarithm Problem (ECDLP)

Elliptic Curve Discrete Logarithm Problem (ECDLP) merupakan hal yang mendasari penggunaan kurva eliptik pada kriptografi. ECDLP dapat dinyatakan sebagai berikut:

Untuk dua buah titik $P, Q \in E(F_p)$ sedemikian sehingga $Q = kP$, tentukan nilai k.

Pada konteks kriptografi, umumnya digunakan nilai k yang sangat besar sebagai kunci privat, sementara P merupakan titik yang merepresentasikan suatu cipherteks dan Q merupakan titik yang merepresentasikan hasil dekripsi cipherteks.

Proses komputasi Q jika diketahui P dan k dapat dengan mudah dilakukan karena komputasi dapat disederhanakan dengan mengubah operasi perkalian terhadap P menjadi sejumlah operasi penggandaan titik yang ekuivalen. Dengan begitu, kP dapat ditentukan dalam kompleksitas $O(\log_2 k)$.

Sementara itu, sangat sulit untuk menentukan nilai k jika diketahui titik P dan Q. Hal inilah yang menjadi dasar kriptografi kurva eliptik.

E. Pohlig-Hellman Attack

Pohlig-Hellman Attack/Serangan Pohlig-Hellman merupakan salah satu algoritma yang dikembangkan untuk menyerang kriptografi kurva eliptik. Algoritma ini mengincar celah medan F_p yang tidak aman berdasarkan bilangan prima p yang digunakan. Algoritma Pohlig-Hellman efektif padajika bilangan prima yang digunakan untuk mendefinsikan titik-titik pada kurva eliptik adalah *smooth prime*, yaitu bilangan prima di mana faktorisasi prima dari nilai $p-1$ terdiri dari bilangan-bilangan prima yang relatif kecil. Algoritma ini pertama kali dikembangkan oleh S. Pohlig dan M. Hellman pada tahun 1977.

Pohlig-Hellman Attack menyederhanakan pemecahan masalah ECDLP untuk titik P dan Q pada $E(F_p)$ menjadi pemecahan masalah ECDLP pada subgrup $\langle P \rangle$, yakni subgrup dari $E(F_p)$ yang dibangkitkan oleh P.

Algoritma Pohlig-Hellman adalah sebagai berikut:

- Misalkan n adalah orde dari subgrup yang dibangkitkan P
  $$n = \#\langle P \rangle$$
  Dengan kata lain, n adalah banyaknya titik berbeda yang dibangkitkan oleh P, sehingga n merupakan bilangan terkecil sehingga
  $$P^n = O$$
- Nyatakan n dalam faktorisasi primanya
  $$n = \Pi_i l_i^{e_i} = l_1^{e_1} * l_2^{e_2} * \dots * l_r^{e_r}$$
  di mana l_i merupakan bilangan prima
- Selanjutnya, untuk menyederhanakan persoalan ECDLP untuk menentukan k dari persamaan $Q = kP$, maka nilai k akan dicari melalui serangkaian persamaan ekuivalensi modulo
  $$k \equiv k_1 (mod\ l_1^{e_1})$$
  $$k \equiv k_2 (mod\ l_2^{e_2})$$
  $$\dots$$
  $$k \equiv k_r (mod\ l_r^{e_r})$$
  yang kemudian akan diselesaikan dengan Chinese Remainder Theorem
- Nyatakan k_i untuk $i \in [1, r]$ sebagai representasi dalam basis l_i, yakni
  $$k_i = z_{0,i} + z_{1,i} l_i + z_{2,i} l_i^2 + \dots + z_{e_i-1,i} l_i^{e_i-1}$$
- Misalkan sebuah list berisi kumpulan titik
  $$T_i = \{\frac{jn}{l_i} P | 0 \leq j \leq l_i - 1\}$$
  untuk $i \in [1, r]$
- Tentukan nilai
  $$\frac{n}{l_i} Q = \frac{n}{l_i}(kP)$$
  $$= \frac{n}{l_i}(z_{0,i} + z_{1,i} l_i + z_{2,i} l_i^2 + \dots + z_{e_i-1,i} l_i^{e_i-1}) P$$
  $$= z_{o,i} \frac{n}{l_i} P + \frac{n}{l_i}(z_{1,i} l_i + z_{2,i} l_i^2 + \dots + z_{e_i-1,i} l_i^{e_i-1}) P$$
  $$= \frac{z_{o,i} n}{l_i} P$$
  untuk $i \in [1, r]$
- Cari titik pada T_i yang sama dengan $\frac{n}{l_i} Q$ tersebut.
- Hasilnya adalah rangkaian persamaan ekuivalensi modulo
  $$k \equiv k_1 (mod\ l_1^{e_1})$$
  $$k \equiv k_2 (mod\ l_2^{e_2})$$
  $$\dots$$
  $$k \equiv k_r (mod\ l_r^{e_r})$$
  di mana

$$k_i = \frac{z_{0,i}n}{l_i}$$

untuk $i \in [1, r]$

- Tentukan nilai k dengan Chinese Remainder Theorem

F. Lain-lain

1) Chinese Remainder Theorem

Chinese Remainder Therome merupakan algoritma yang digunakan untuk menentukan bilangan yang memenuhi serangkaian persamaan ekuivalensi modulo.

Jika terdapat serangkaian persamaan

$$x \equiv a_1 (mod\ n_1)$$
$$x \equiv a_2 (mod\ n_2)$$
...
$$x \equiv a_k (mod\ n_k)$$

untuk bilangan bulat a_i serta bilangan n_i yang saling relatif prima, untuk $i \in [1, k]$, maka nilai x dapat ditentukan sebagai berikut:

- Misalkan N adalah hasil kali semua n_i, dan $N_i = N/n_i$, serta N_i dan n_i saling relatif prima.
- Untuk setiap n_i tentukan M_i dan m_i sedemikian sehingga
$$M_i N_i + m_i n_i = 1$$
- Nilai x adalah
$$x = \Sigma_i a_i M_i N_i$$

UCAPAN TERIMA KASIH

Penulis mengucapkan puji dan syukur yang sebesarbesarnya kepada rahmat Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga makalah ini dapat diselesaikan dengan baik. Penulis mengucapkan terima kasih kepada selaku dosen pengajar IF4020 Kriptografi, Dr. Rinaldi Munir, S.T, M.T. yang telah memberikan bimbingan dan ilmu terkait materi Kriptografi ini, khususnya pada algoritma kriptografi kunci publik dan pengaplikasiannya.

REFERENSI

[1] Musson, M. (2006). Attacking the Elliptic Curve Discrete Logarithm Problem. Acadia University.

[2] Novotney, P. (2010). Weak Curves In Elliptic Curve Cryptography. *modular. math. washington. edu/edu/2010/414/projects/novotney. pdf*.

[3] S. Pohlig, M. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, 1977. http://www.ee.stanford.edu/~hellman/publications/28.pdf

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Jakarta, 20 Desember 2021

Rexy Gamaliel Rumahorbo (13519010)