Prototipe Skema Pembagian Rahasia Asmuth-Bloom

Nur Alam Hasabie
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13517096@std.stei.itb.ac.id

***Abstrak*— Pada makalah ini akan dibahas mengenai skema pembagian rahasia Asmuth-Bloom. Selain itu, akan dibahas juga mengenai implementasi dari skema tersebut , beserta analisis skema dari berbagai dimensi.**

Kata kunci — Skema pembagian rahasia, skema Asmuth Bloom, teori sisa China.

I. Pengantar

Skema kriptografi memiliki satu keterbatasan , yaitu bahwa rahasia dipegang oleh satu-dua pihak saja. Akibatnya, rahasia dapat hilang bilamana pihak-pihak tersebut tidak dapat melakukan pemulihan rahasia. Padahal, ketersediaan rahasia sangat penting pada beberapa aplikasi, apalagi mengingat bahwa banyak sistem pada masa ini merupakan sistem yang tersebar..

Salah satu solusi atas masalah ketersediaan informasi tersebut adalah skema pembagian rahasia. Suatu informasi rahasia dibagikan kepada beberapa pihak, dan informasi rahasia dapat diambil asalkan terdapat sejumlah minimal pihak yang masih menyimpan bagian informasinya. Salah satu skema rahasia yang pernah diusulkan adalah skema pembagian rahasia Asmuth-Bloom.

Pada makalah ini , akan diimplementasikan prototipe dari skema Asmuth-Bloom. Karena skema Asmuth-Bloom menggunakan teori sisa China (*Chinese Remainder Theorem*, selanjutnya disebut CRT), maka CRT akan sedikit dijelaskan pada makalah ini.

II. Teori Pendukung

1. Skema Pembagian Rahasia

Skema pembagian rahasia merupakan skema yang memungkinkan suatu rahasia *K* dibagi ke *D* pihak , sehingga informasi rahasia dapat dipulihkan dari minimal satu set *N*. Definisi minimal berarti rahasia tidak dapat diketahui bahkan oleh *N-1* pihak yang memiliki bagian rahasia[1].

Skema Asmuth-Bloom sendiri bukanlah satu-satunya skema pembagian rahasia. Shamir [1] , sebagai contoh, mengusulkan skema berbasis interpolasi polinomial sebagai salah satu skema pembagian rahasia.

2. *Teorema Sisa China (Chinese Remainder Theorem)*

Landasan bagi skema pembagian rahasia Asmuth-Bloom adalah CRT. Permasalahan CRT pertama kali diungkap oleh Sun Tzu dalam Suan Ching.

Dalam aritmatika modular , CRT dirumuskan sebagai berikut : Diberikan m_1, m_2, m_3, …. m_n bilangan yang saling relatif prima, maka sistem persamaan $x \equiv a_1 \bmod(m_1)$, $x \equiv a_2 \bmod(m_2)$, $x \equiv a_3 \bmod(m_3)$, … $x \equiv a_n \bmod(m_n)$ mempunyai solusi unik dalam mod $(m_1 . m_2 . m_3 . \ldots . m_n)$.

Selain Asmuth-Bloom, skema pembagian rahasia Mignotte juga menggunakan CRT, namun skema Mignotte tidak akan dibahas dalam makalah ini.

3. *Skema Pembagian Rahasia Asmuth-Bloom*

Misalkan rahasia akan dibagi kepada n pihak dengan minimum t pihak sepakat agar rahasia dapat dipulihkan. Skema pembagian rahasia sebagai berikut [2][3] :

1. Pilih angka $m_0 < m_1 < m_2 < m_3 \ldots < m_n$, kesemuanya saling prima, dengan m_0 prima dan :

$$M = \prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1} \qquad [1]$$

2. Ambilah sebuah rahasia $d \in \mathbf{Z}/m_0\mathbf{Z}$ dan sebuah bilangan bulat sembarang α sehingga $0 \leq y = (d + \alpha m_0) < M$.
3. Tiap bagian i dari n mendapat bagian rahasia : $y_i = y \bmod (m_i)$.

Pemulihan rahasia dilakukan sebagai berikut :

1. Misalkan **S** adalah himpunan pihak yang hendak berkoalisi untuk memulihkan rahasia. Hitung :

$$M' = \prod_{i \in S} m_i \qquad [2]$$

2. Selanjutnya, selesaikan persamaan CRT $y \equiv y_i \bmod (m_i)$.
3. Setelah itu , hitung kembali rahasia $d \equiv y \bmod (M')$

III. PROTOTIPE IMPLEMENTASI ALGORITMA

1. *Membangkitkan Sekuens*

Diberikan sebuah rahasia **d** yang akan dibagikan ke **n** pihak, dan minimal **k** pihak dapat berkoalisi untuk melakukan konstruksi ulang rahasia. Untuk mendapatkan sebuah sekuens, suatu pendekatan heuristik sederhana dapat dibuat.

Ambil sebuah prima $m_0 > c\mathbf{d}$, c sebuah bilangan bulat. Maka, sekuens yang mungkin adalah bilangan-bilangan prima selanjutnya dari m_0. Dapat diduga bahwa c ~ **d**. Nilai ditentukan secara heuristik, misal dengan memperhatikan distribusi bilangan prima pada ambang tertentu. Bilamana sekuens yang dihasilkan tidak memenuhi syarat pada persamaan (1), maka dapat dibangkitkan sekuens untuk nilai c yang lebih besar.

Pada implementasi, diambil nilai c awal 1/10 dari **d**. Nilai ini kurang baik untuk nilai c yang besar.

2. *Menghasilkan Bilangan Random*

Bilangan random **α** dapat diambil dari rentang 0 sampai nilai lantai dari $(M-m_0)/\mathbf{d}$.

3. *Menyelesaikan Persamaan CRT*

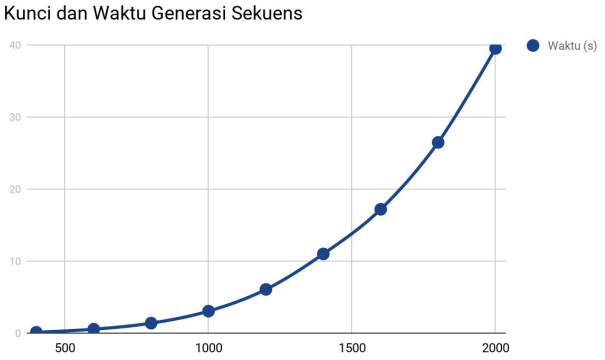
Selanjutnya, rahasia d dapat dibangun kembali dengan koalisi **k** pihak. Penyelesaian persamaan CRT dapat menggunakan Identitas Bezout dan Algoritma Euclid [4].

4. *Hasil Eksperimen dan Analisis*

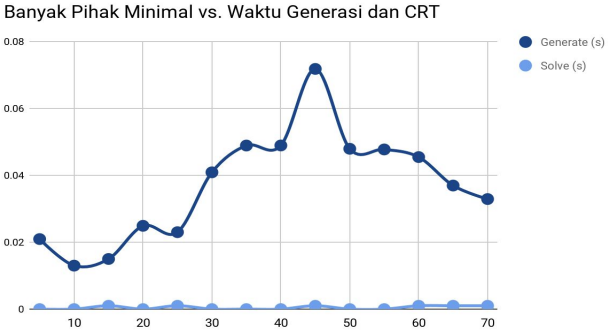
Kode prototipe dapat diakses pada link : https://github.com/AlamHasabie/simple-asmuth-bloom. Pada kode, dibuat sebuah kelas Holder. Kelas Holder merupakan abstraksi dari pihak pemegang rahasia, dengan implementasi bermacam-macam, misalkan sebuah server pada suatu sistem terdistribusi.

Secar algoritma, skema Asmuth-Bloom sempurna. Sampai pada **k-1** pihak bersepakat untuk memecahkan kunci, maka ruang pencarian kunci tetap berada dalam ruang $\mathbf{Z}/m_0\mathbf{Z}$.

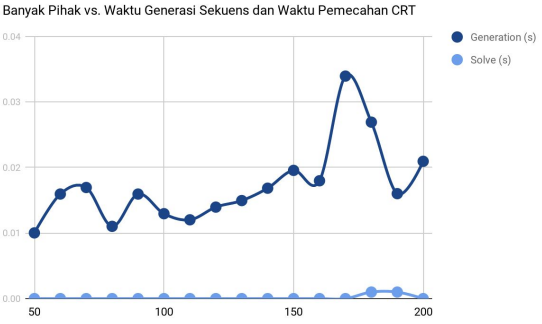
Hasil tes menunjukkan program sudah dapat mengeluarkan kunci yang benar. Selanjutnya akan ditelisik pengaruh berbagai parameter terhadap kinerja program. Perlu diperhatikan bahwa pengujian tidak bersifat menyeluruh, namun hanya akan memberikan gambaran bagaimana ketiga parameter mempengaruhi kinerja.



Grafik 3.1. Nilai kunci dan waktu generasi sekuens, untuk parameter ***n = 20*** *dan* ***k = 15***



Grafik 3.1. Perubahan waktu generasi sekuens dan pencarian solusi CRT terhadap perubahan ***k*** *, dengan n = 200 dan d = 400*



Grafik 3.1. Perubahan waktu generasi sekuens dan pencarian solusi CRT terhadap perubahan ***n >= 50*** *, dengan k = 10 dan d = 200*

Hipotesis kinerja memiliki kompleksitas eksponensial terhadap besar kunci **d**. Namun, kinerja tidak menunjukkan suatu tren tertentu dalam pengubahan variabel **n** , **k.**

IV. KESIMPULAN DAN SARAN

Telah ditunjukkan implementasi prototipe sederhana dari skema pembagian rahasia Asmuth-Bloom, dan kinerja prototipe terhadap variabilitas parameternya.

Dapat diduga bahwa skema memiliki kompleksitas eksponensial terhadap ukuran kunci, terutama dalam fungsi pembangkitan sekuens. Adapun hasil eksperimen tidak menunjukkan tren untuk variabilitas banyak pihak terlibat dan minimum pihak yang dapat berkoalisi untuk memulihkan rahasia.

Masih terdapat banyak optimasi yang dilakukan, misalkan dengan mengganti metode pencarian prima menjadi metode yang lebih optimal (karena implementasi pada prototipe ini masih sangat naif) , penulisan algoritma yang lebih optimal (misal algoritma produk suatu sekuens), ataupun optimasi numerik yang belum ditemukan oleh pengarang.

REFERENSI

[1] Shamir, Adi. "How to share a secret." Communications of the ACM 22, no. 11 (1979): 612-613.

[2] Asmuth, Charles and John Bloom. “A modular approach to key safeguarding.” IEEE Trans. Inf. Theory 29 (1983): 208-210.

[3] Kaya, Kamer, and Ali Aydın Selçuk. "Threshold cryptography based on Asmuth–Bloom secret sharing." Information sciences 177, no. 19 (2007): 4148-4160.

[4] Munir, R. 2015 “ Teori Bilangan” . Slide tersedia di : https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2015-2016/Teori%20Bilangan%20(2015).pdf

REFERENSI

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 , 6 Mei 2020

Nur Alam Hasabie