J. Sains Dasar 2014 3(1) 25 - 33

Metode perjanjian *password* berdasarkan operasi matriks atas aljabar Min-Plus untuk keamanan pengiriman informasi rahasia

(The password agreement method based on matrix operation over Min-Plus algebra for safety of secret information sending)

Musthofa dan Dwi Lestari

Jurdik Matematika, FMIPA, Universitas Negeri Yogyakarta (UNY),
Kampus Karangmalang, Sleman, DI Yogyakarta 55281
tel. 08175456213, faks. (0274) 548203 dan e-mail: musthofa@uny.ac.id

diterima 2 Desember 2013, disetujui 3 Februari 2014

Abstrak

Protokol perjanjian kunci merupakan suatu metode dalam kriptografi. Protokol perjanjian kunci digunakan untuk mengatasi masalah pengiriman informasi rahasia melalui jalur komunikasi.Untuk mengamankan informasi tersebut dibutuhkan suatu kunci rahasia yang disebut dengan *password*. Kedua belah pihak yang melakukan pertukaran informasi rahasia harus menyepakati kunci yang sama. Pada metode ini, kedua belah pihak saling menukarkan parameter yang dapat diketahui umum, akan tetapi dari parameter umum tersebut dapat dibentuk satu password rahasia yang sama dan tidak diketahui oleh umum. Salah satu metode yang telah digunakan adalah menggunakan serangkaian operasi perkalian matriks yang didefinisikan atas suatu lapangan hingga. Pada penelitian ini dikonstruksi algoritma yang digunakan dalam metode perjanjian password, yaitu berupa protokol perjanjian kunci yang tingkat keamanannya didasarkan pada suatu masalah aljabar pada operasi matriks atas Aljabar Min Plus atas Z. Aljabar min-plus atas Z, yaitu $Z \cup \{+\infty\}$ dengan Z adalah himpunan semua bilangan bulat yang dilengkapi dengan operasi minimum dan operasi penjumlahan membentuk sruktur aljabar yang dinamakan semiring idempotent. Hasil penelitian menunjukkan bahwa penerapan operasi matriks atas aljabar min plus dapat digunakan sebagai protokol perjanjian password untuk mengamankan informasi rahasia.

Kata kunci: informasi rahasia, password, aljabar Min-Plus

Abstract

Key agreement protocol is a method in cryptography. Key agreement protocol is used to overcome the problem of sending secret information over communication lines. A secret key, called password, is needed to secure t he information. Both parties who exchange confidential information must agree on the same key. In this method, both parties exchange mutual general parameters that everyone can see, however from the general parameters the same passwords can be formed and not publicly known. One method that has been used is applying a series of matrix multiplication operation defined over a finite field. In this study, we constructed an algorithm in the form of a key agreement protocol that can be used in the password agreement method which the level of security based on algebraic problem of matrix operation over Z- min plus algebra. Min Plus algebra over Z, that is $Z \cup \{ + \infty \}$ with Z is the set of all integers equipped with the minimum and addition operation, is called idempotent semiring. The results showed that the application of matrix operation over min plus algebra can be used as key agreement protocol in securing secret information.

Key words: secret information, password, Min-Plus algebra

Pendahuluan

Perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya teknologi informasi seperti internet, komunikasi jarak jauh dapat dilakukan dengan cepat dan murah. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan jalur komunikasi umum yang dapat digunakan oleh siapapun, sehingga sangat rawan terhadap penyadapan. Apabila informasi yang dikirimkan bersifat rahasia, maka jaminan keamanan informasi menjadi sangat mutlak untuk dipenuhi.

Salah satu solusi untuk mengatasi masalah tersebut adalah menggunakan kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain. Enkripsi adalah suatu proses penyandian yang melakukan perubahan suatu pesan, dari yang dapat dimengerti, disebut dengan plainteks, menjadi suatu kode yang sulit dimengerti, disebut dengan cipherteks. Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi [1,2] .

Proses enkripsi-dekripsi tersebut membutuhkan suatu kunci rahasia yang disebut dengan *password*. Kedua belah pihak yang melakukan pertukaran informasi rahasia harus menyepakati kunci yang sama. Akan menjadi masalah apabila keduanya tidak dapat menyepakati *password* yang sama, sebab keduanya menggunakan jalur komunikasi yang tidak aman. Protokol perjanjian kunci merupakan suatu metode dalam kriptografi yang digunakan untuk mengatasi masalah tersebut. Pada metode ini, kedua belah pihak saling menukarkan parameter yang dapat diketahui umum, akan tetapi dari parameter umum tersebut dapat dibentuk satu *password* rahasia yang sama dan tidak diketahui oleh umum.

Protokol perjanjian kunci yang didasarkan pada grup perkalian matriks yang merupakan salah satu contoh grup non-komutatif telah dibahas dalam beberapa literature, seperti dalam [3]. Selain itu, operasi matriks pada struktur aljabar yang merupakan semiring telah dibahas dalam [4] dan [5]. Dalam penelitian ini, peneliti ingin mengembangkan protokol perjanjian kunci yang didasarkan pada operasi matriks atas Aljabar Min-Plus.

Berdasarkan latar belakang di atas diidentifikasi masalah pentingnya menjaga keamanan informasi yang dikirim. Hal tersebut dapat dilakukan dengan menyepakati perjanjian antara kedua belah pihak dalam pengiriman misal kunci atau *password* pengiriman. Berbagai metode ditempuh untuk mengkonstruksi kunci dalam perjanjian pengiriman informasi. Salah satu metode yang dibahas dalam penelitian ini adalah penggunaan operasi matriks atas aljabar Min-Plus yang akan diaplikasikan dalam pengkontruksian kunci rahasia atau password.

Metode Penelitian

Dalam penelitian ini digunakan metode penelitian studi literatur berupa jurnal-jurnal ilmiah yang terkait dengan topik penelitian, dan buku-buku referensi yang mendukung. Pada tahap awal dipelajari konsep-konsep dasar tentang Aljabar Min-Plus dan Operasi Matriks atas Aljabar Min-Plus beserta sifat-sifatnya yang dinyatakan dalam beberapa definisi dan teorema. Konsep-konsep ini nantinya digunakan sebagai dasar dalam memahami perkalian matriks atas Aljabar Min-Plus yang akan digunakan dalam perhitungan protokol perjanjian kunci. Setelah itu, dipelajari konsep-konsep dalam kriptografi yang digunakan pada protokol perjanjian kunci.

Selanjutnya, dipelajari metode protokol perjanjian kunci Stickel (2005) yang telah dibahas dalam [3] dan menganalisa perkalian matriks atas Aljabar Min-Plus [4] yang akan digunakan sebagai dasar perhitungan protokol perjanjian kunci yang akan dibuat algoritma-algoritmanya. Hal-hal yang dianalisa adalah sifat-sifat Aljabar Min-Plus dan cara menghitung perkalian matriks atas Aljabar Min-Plus dengan mengkaji pembahasan dalam [6] .

Langkah terakhir adalah menerapkan hasil-hasil yang diperoleh untuk membuat rancangan algoritma-algoritma yang mendukung berjalannya protokol perjanjian kunci yang didasarkan pada operasi matriks atas Aljabar Min-Plus.

Hasil dan Diskusi

Sistem Kriptografi Kunci Rahasia

Sistem kriptografi atau sering disebut dengan cipher merupakan suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Sistem kriptografi simetris adalah sistem kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi cipherteks [2]. Sistem kriptografi ini sering disebut dengan sistem kriptografi kunci rahasia, seperti dijelaskan pada gambar berikut ini.

Sistem kriptografi atau sering disebut dengan cipher merupakan suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Sistem kriptografi simetris adalah sistem kriptografi yang menggunakan kunci enkripsi dan dekripsi yang sama. Sistem ini mengharuskan dua pihak yang berkomunikasi menyepakati suatu kunci rahasia yang sama sebelum keduanya saling berkomunikasi. Keamanan dari sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain yang berhasil mendapatkan kunci dapat mendekripsi cipherteks [2].

Beberapa sistem kriptografi kunci rahasia yang saat ini telah dikenal secara luas adalah DES, 3DES, Blowfish, RC4, A5 dan AES. Sistem-sistem kriptografi yang banyak digunakan di internet adalah RC4, 3DES dan AES, sedangkan pada pengamanan telepon seluler digunakan sistem kriptografi A5. Sistem kriptografi AES saat ini telah menjadi standar enkripsi file digital, seperti untuk dokumen-dokumen rahasia.

Aljabar Min Plus atas Z

Pada penelitian ini digunakan konsep-konsep mengenai matriks Aljabar Min-Plus. Berikut ini diberikan pengertian-pengertian dan sifat-sifatnya. Berbeda dengan Aljabar Min-Plus yang dikenal selama ini yaitu didefinisikan atas himpunan semua bilangan real R, pada penelitian ini Aljabar Min-Plus yang digunakan didefinisikan atas himpunan Z.

Aljabar Min-Plus atas Z merupakan himpunan $Z \cup \{+\infty\}$ yang dilengkapi dengan operasi minimum, dinotasikan dengan $\oplus$, dan operasi penjumlahan yang dinotasikan dengan $\otimes$. Selanjutnya $(Z \cup \{+\infty\}, \oplus, \otimes)$ dinotasikan dengan $Z_{\min}$. Jadi, dalam $Z_{\min}$: $3 \oplus 4 = \min(3, 4) = 3$ dan $3 \otimes 4 = 3 + 4 = 7$. Sifat –sifat yang berlaku dalam $Z_{\min}$ antara lain:

1) $x \oplus (y \oplus z) = \min(x, \min(y, z)) = \min(\min(x,y), z) = (x \oplus y) \oplus z$
2) $x \oplus \{+\infty\} = \min(x, +\infty) = x$
3) $x \otimes \{+\infty\} = x + \{+\infty\} = \{+\infty\}$
4) $x \otimes 0 = x + 0 = x$
5) $x \otimes (y \otimes z) = x + (y + z) = (x + y) + z = (x \otimes y) \otimes z$
6) $x \otimes y = x + y = y + x = y \otimes x$
7) $x \otimes (-x) = x + (-x) = 0$
8) $x \otimes (y \oplus z) = x + (\min(y, z)) = \min(x + y, x + z) = (x \otimes y) \oplus (x \otimes z)$

Dari sifat –sifat di atas, terlihat bahwa $+\infty$ merupakan elemen identitas (elemen netral) terhadap operasi $\oplus$ dan 0 merupakan elemen identitas (elemen satuan) terhadap operasi $\otimes$. Oleh karena itu, ditinjau dari struktur aljabar $R_{\min}$ merupakan semiring, yaitu:

1) $(Z \cup \{+\infty\}, \oplus)$ merupakan monoid komutatif dengan elemen netral $+\infty$
2) $(Z \cup \{+\infty\}, \otimes)$ merupakan monoid dengan elemen satuan 0
3) Operasi $\otimes$ terhadap $\oplus$ bersifat distributif
4) Elemen netral terhadap operasi $\oplus$, yaitu $\{+\infty\}$ bersifat menyerap terhadap operasi $\otimes$. Jadi $x \otimes +\infty = +\infty \otimes x = +\infty$, $\forall x \in Z_{\min}$

Selanjutnya karena operasi $\oplus$ bersifat idempotent, yaitu $x \oplus x = x$, untuk setiap $x \in Z_{\min}$, maka $Z_{\min}$ merupakan semiring idempoten. Sifat idempotent ini mengakibatkan tidak adanya invers terhadap operasi tersebut. Lebih lanjut karena operasi kedua , yatu “plus” memiliki

invers, maka Z_{min} merupakan semifield idempotent.

Matriks Atas Aljabar Minplus

Selanjutnya seperti pada ring pada umumnya, jika diberikan suatu semifield idempotent Z_{min}, dapat dibentuk matriks dengan entri-entrinya elemen-elemen Z_{min}. Operasi $\oplus$ dan $\otimes$ pada matriks yang telah terbentuk didefinisikan sebagai berikut:

(1) $(A \oplus B)_{ij} = A_{ij} \oplus B_{ij}$

(2) $(A \otimes B)_{ij} = \underset{k}{\oplus}(A_{ik} \otimes B_{kj})$

Contoh 1.

Jika $A = \begin{bmatrix} 0 & 2 \\ -2 & 1 \end{bmatrix}$ dan $B = \begin{bmatrix} -2 & 3 \\ 1 & 2 \end{bmatrix}$, maka

$$A \oplus B = \begin{bmatrix} 0 & 2 \\ -2 & 1 \end{bmatrix} \oplus \begin{bmatrix} -2 & 3 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 \oplus -2 & 2 \oplus 3 \\ -2 \oplus 1 & 1 \oplus 2 \end{bmatrix} = \begin{bmatrix} -2 & 2 \\ -2 & 1 \end{bmatrix}$$

dan

$$A \otimes B = \begin{bmatrix} 0 & 2 \\ -2 & 1 \end{bmatrix} \otimes \begin{bmatrix} -2 & 3 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} (0+(-2) \oplus (2+1) & (0+3) \oplus (2+2) \\ (-2+(-2)) \oplus (1+1) & (-2+3) \oplus (1+2) \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ -4 & 1 \end{bmatrix}$$

Selanjutnya didefinisikan $(Z_{min})^{n \times n}$ sebagai himpunan semua matriks berukuran $n \times n$ dengan entri-entrinya elemen $Z_{min,}$. Elemen netral terhadap operasi $\oplus$ dan elemen netral terhadap operasi $\otimes$ dalam $(Z_{min})^{n \times n}$ berturut-turut adalah matriks E

dengan $(E)_{ij} = \begin{cases} 0, \text{ jika } i = j \\ +\infty, \text{ jika } i \neq j \end{cases}$ dan matriks ε dengan $(\varepsilon)_{ij} = +\infty$,untuk setiap i dan j . Jadi ,

(1) $(E \otimes A) = (A \otimes E) = A$ untuk setiap $A \in (Z_{min})^{n \times n}$;

(2) $(\varepsilon \oplus A) = (A \oplus \varepsilon) = A$, untuk setiap $A \in (Z_{min})^{n \times n}$.

Berikut ini beberapa sifat matriks atas aljabar min-plus :

Sifat 2. *Jika A, B, C* $\in (Z_{min})^{n \times n}$ *maka berlaku :*

(1) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

(2) $A \oplus B = B \oplus A$

(3) $A \otimes (B \otimes C) = (A \otimes B) \otimes C$

(4) $A \otimes (B \oplus C) = (A \otimes B) \oplus (A \otimes C)$

(5) $(A \oplus B) \otimes C = (A \otimes C) \oplus (B \otimes C)$

(6) $A \oplus A = A$

Bukti :

1. $[A \oplus (B \oplus C)]_{ij} = A_{ij} \oplus (B_{ij} \oplus C_{ij}) = (A_{ij} \oplus B_{ij}) \oplus C_{ij} = [(A \oplus B) \oplus C]_{ij}$.

2. $[A \oplus B]_{ij} = A_{ij} \oplus B_{ij} = B_{ij} \oplus A_{ij} = [B \oplus A]_{ij}$.

3. $\left[A \otimes (B \otimes C)\right]_{ij} = \underset{k=1}{\overset{n}{\oplus}} A_{ik} \left(\underset{l=1}{\overset{n}{\oplus}} B_{kl} \otimes C_{lj} \right)$

$= \underset{k=1}{\overset{n}{\oplus}} \underset{l=1}{\overset{n}{\oplus}} A_{ik} \otimes B_{kl} \otimes C_{lj}$

$= \underset{k=1}{\overset{n}{\oplus}} \left(\underset{l=1}{\overset{n}{\oplus}} A_{ik} \otimes B_{kl} \right) \otimes C_{lj}$

$= \left[(A \otimes B) \otimes C\right]_{ij}$

4. $\left[A \otimes (B \oplus C)\right]_{ij}$

$= \underset{k=1}{\overset{n}{\oplus}} A_{ik} \left(B_{kj} \oplus C_{kj} \right)$

$= \underset{k=1}{\overset{n}{\oplus}} \left(\left(A_{ik} \otimes B_{kj} \right) \oplus \left(A_{ik} \otimes C_{kj} \right) \right)$

$= \left(\underset{k=1}{\overset{n}{\oplus}} \left(A_{ik} \otimes B_{kj} \right) \right) \oplus \left(\underset{k=1}{\overset{n}{\oplus}} A_{ik} \otimes C_{kj} \right)$

$= \left[(A \otimes B) \oplus (A \otimes C)\right]_{ij}$

5. $\left[(A \oplus B) \otimes C)\right]_{ij}$

$= \underset{k=1}{\overset{n}{\oplus}} \left(A_{ik} \oplus B_{ik} \right) C_{kj}$

$= \underset{k=1}{\overset{n}{\oplus}} \left(\left(A_{ik} \otimes C_{kj} \right) \oplus \left(B_{ik} \otimes C_{kj} \right) \right)$

$= \underset{k=1}{\overset{n}{\oplus}} \left(A_{ik} \otimes C_{kj} \right) \oplus \underset{k=1}{\overset{n}{\oplus}} \left(B_{ik} \otimes C_{kj} \right)$

$= \left[(A \otimes C) \oplus (B \otimes C)\right]_{ij}$

6. $\left[A \oplus A\right]_{ij} = A_{ij} \oplus A_{ij} = A_{ij}$.

Berdasarkan sifat-sifat di atas, $(Z_{min})^{n \times n}$ merupakan semiring idempotent.

Protokol Perjanjian Kunci

Apabila Pihak 1 dan Pihak 2 menggunakan sistem kriptografi kunci rahasia, masalah utama yang muncul adalah keduanya harus menyepakati kunci yang sama, padahal keduanya tidak dapat bertemu secara langsung. Apabila Pihak 1 mengirimkan kunci kepada

Pihak 2, maka Pihak 3 dapat mengetahui kunci yang dikirimkan, hal ini dikarenakan proses pengiriman melalui jalur komunikasi yang tidak aman.

Salah satu cara yang dapat digunakan untuk mengatasi masalah ini adalah menggunakan protokol perjanjian kunci (*key establishment protocol*). Protokol perjanjian kunci bertujuan agar kedua belah pihak dapat menentukan kunci yang sama walaupun dilakukan melalui jalur komunikasi yang tidak aman. Salah satu contoh protokol perjanjian kunci yang paling sederhana dan telah dikenal secara luas adalah protokol perjanjian kunci Diffie-Hellman yang dipublikasikan pada tahun 1976.

Pihak 1 atau Pihak 2 mempublikasikan suatu grup siklik *G*dengan elemen pembangun $g \in G$.	
Pihak 1	**Pihak 2**
1. Pihak 1 memilih secara rahasia suatu bilangan bulat positif *a* 2. Pihak 1 menghitung g^a 3. Pihak 1 mengirim g^a kepada Pihak 2 4. Pihak 1 menerima g^b dari Pihak 2 5. Pihak 1 menghitung $K_1 = \left(g^b\right)^a = g^{ba}$	1. Pihak 2 memilih secara rahasia suatu bilangan bulat positif *b* 2. Pihak 2 menghitung g^b 3. Pihak 2 mengirim g^b kepada Pihak 1 4. Pihak 2 menerima g^a dari Pihak 1 5. Pihak 2 menghitung $K_2 = \left(g^a\right)^b = g^{ab}$
Pihak 1 dan Pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$	

Gambar 1. Skema Protokol Perjanjian Kunci Diffie-Hellman [3].

Diketahui grup siklik *G* merupakan grup komutatif, maka $ab = ba$, sehingga $K = K_1 = K_2$. Misalkan Pihak 1 dan Pihak 2 berhasil menyepakati kunci rahasia yang sama yaitu *K*. Selanjutnya, kunci rahasia *K* yang telah disepakati digunakan untuk melakukan proses enkripsi-dekripsi. Di lain pihak, Pihak 3 sebagai penyerang hanya dapat mengetahui nilai *g*, g^a dan g^b. Untuk mendapatkan kunci yang telah disepakati Pihak 1 dan Pihak 2, maka Pihak 3 harus menentukan nilai *a* atau *b.* Dengan kata lain, Pihak 3 harus menyelesaikan masalah logaritma diskrit pada *G*, yaitu menentukan nilai *a* apabila nilai *g* dan g^a diketahui. Tingkat kemanan dari protokol perjanjian kunci Diffie-Hellman didasarkan pada masalah logaritma diskrit [1].

Pada protokol perjanjian kunci Diffie-Hellman digunakan grup siklik yang merupakan grup komutatif. Dalam [3] telah diperkenalkan konsep mengenai protokol perjanjian kunci yang menggunakan grup non-komutatif. Untuk dapat menggunakan grup tidak komutatif, protokol perjanjian kunci harus dapat dikonstruksi menggunakan suatu permasalahan matematis yang ada pada grup non-komutatif. Skema protokol perjanjian kunci Stickel yang didasarkan atas grup non-komutatif adalah sebagai berikut.

Pihak 1 atau Pihak 2 mempublikasikan suatu grup non-komutatif *G* dan $a, b \in G,\ ab \neq ba$, dengan *N* dan *M* berturut-turut adalah order dari *a* dan *b*	
Pihak 1	**Pihak 2**
1. Pihak 1 memilih secara rahasia $n < N$ dan $m < M$ 2. Pihak 1 menghitung $u = a^n b^m$ 3. Pihak 1 mengirim *u* kepada Pihak 2 4. Pihak 1 menerima *v* dari Pihak 2 5. Pihak 1 menghitung $K_1 = a^n v b^m$	1. Pihak 2 memilih secara rahasia $r < N$ dan $s < M$ 2. Pihak 2 menghitung $v = a^r b^s$ 3. Pihak 2 mengirim *v* kepada Pihak 1 4. Pihak 2 menerima *u* dari Pihak 1 5. Pihak 2 menghitung $K_2 = a^r u b^s$
Pihak 1 dan Pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$	

Gambar 2. Skema Protokol Perjanjian Kunci Stickel

Dapat ditunjukkan bahwa Pihak 1 dan Pihak 2 berhasil menyepakati kunci rahasia yang sama, yaitu

$$K_1 = a^n v b^m = a^n a^r b^s b^m = a^{n+r} b^{s+m} = a^r a^n b^m b^s = a^r u b^s = K_2.$$

Salah satu contoh grup yang dapat digunakan adalah grup perkalian matriks atas suatu lapangan hingga. Penggunaan grup pada Protokol Stickel ini dapat diperumum menjadi sebarang semigrup, juga dapat diperumum menjadi sebarang semiring. Pada penelitian ini semiring yang digunakan adalah himpunan semua matriks *nxn* atas bilangan bulat dengan operasi penjumlahan dan perkaliannya didefinisikan atas suatu aljabar min-plus, yaitu $(Z_{\min})^{n\times n}$.

Operasi Perkalian Matriks atas Aljabar Min Plus

Pada pembahasan operasi perkalian matriks atas aljabar min plus telah dibuktikan bahwa operasi perkalian matriks atas aljabar min plus memenuhi sifat assosiatif. Oleh karena itu, dapat diperoleh sifat berikut:

Teorema 1.

Jika A merupakan matriks atas aljabar min plus, maka berlaku $A^m \otimes A^n = A^n \otimes A^m$.

Bukti :

Karena perkalian matriks atas aljabar min plus memenuhi sifat assosiatif, maka jelas berlaku sifat di atas .

Contoh 2.

Diberikan matriks atas aljabar min plus $A = \begin{pmatrix} 1 & 7 \\ 11 & 3 \end{pmatrix}$.

Diperoleh

$$A^2 = \begin{pmatrix} 1 & 7 \\ 11 & 3 \end{pmatrix} \otimes \begin{pmatrix} 1 & 7 \\ 11 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 8 \\ 12 & 6 \end{pmatrix};$$

$$A^3 = \begin{pmatrix} 2 & 8 \\ 12 & 6 \end{pmatrix} \otimes \begin{pmatrix} 1 & 7 \\ 11 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 9 \\ 13 & 11 \end{pmatrix};$$

$$A^2 \otimes A^3 = \begin{pmatrix} 2 & 8 \\ 12 & 6 \end{pmatrix} \otimes \begin{pmatrix} 3 & 9 \\ 13 & 11 \end{pmatrix} = \begin{pmatrix} 5 & 11 \\ 15 & 17 \end{pmatrix} = \begin{pmatrix} 3 & 9 \\ 13 & 11 \end{pmatrix} \otimes \begin{pmatrix} 2 & 8 \\ 12 & 6 \end{pmatrix} = A^3 \otimes A^2$$

Penerapan Operasi Matriks atas Aljabar Min Plus pada Protokol Perjanjian Kunci

Berdasarkan sifat operasi matriks atas aljabar min plus di atas, selanjutnya dapat disusun algoritma untuk melakukan pembentukan kunci sebagai berikut :

Pihak 1 atau Pihak 2 mempublikasikan suatu semiring $(Z_{\min})^{n\times n}$ dan $A, B \in (Z_{\min})^{n\times n}$	
Pihak 1	**Pihak 2**
1. Pihak 1 memilih secara rahasia bilangan asli *n* dan *m* 2. Pihak 1 menghitung $u = A^n B^m$ 3. Pihak 1 mengirim *u* kepada Pihak 2 4. Pihak 1 menerima *v* dari Pihak 2 5. Pihak 1 menghitung $K_1 = A^n v B^m$	1. Pihak 2 memilih secara rahasia bilangan asli *r* dan *s* 2. Pihak 2 menghitung $v = A^r B^s$ 3. Pihak 2 mengirim *v* kepada Pihak 1 4. Pihak 2 menerima *u* dari Pihak 1 5. Pihak 2 menghitung $K_1 = A^n u B^m$
Pihak 1 dan Pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$	

Menurut sifat perkalian matriks atas aljabar min plus diperoleh:

$K_1 = A^n v B^m = A^n A^r B^s B^m = A^r A^n B^m B^s = A^r u B^s = K_2$.

Oleh karena itu pihak satu dan pihak dua telah berhasil menyepakati kunci yang sama.

Pihak 1 atau pihak 2 menentukan $A = \begin{bmatrix} 1 & 7 \\ 11 & 3 \end{bmatrix}; B = \begin{bmatrix} 2 \\ 6 \end{bmatrix}$	
Pihak 1	Pihak 2
1. Memilih secara rahasia $n = 2$, $m = 5$	1. Memilih secara rahasia $r = 3$, $s = 4$

2. Menghitung $U = A^2 B^5$ $= U = \begin{bmatrix} 12 & 11 \\ 16 & 11 \end{bmatrix}$	2. Menghitung $V = A^3 B^4$ $V = \begin{bmatrix} 11 & 11 \\ 20 & 15 \end{bmatrix}$
3. Mengirim *U* ke pihak 2	3. mengirim *V* ke pihak 1
4. Pihak 1 menghitung $K_1 = A^2 V B^5$ $K_1 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix}$	4. Pihak 2 menghitung $K_2 = A^3 U B^4$ $K_2 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix}$
Pihak 1 dan pihak 2 menyepakati kunci yang sama yaitu $K = K1 = K2$	

Implementasi Algoritma untuk Pengamanan Pesan

Misal pihak 1 akan mengirim pesan **BOS AWAS DISADAP LO** kepada pihak 2 . Oleh karena itu pesan tersebut dipecah menjadi blok-blok 4 huruf yaitu **BOSA-WASD-ISAD-APLO**. Selanjutnya tiap blok di ubah ke dalam angka-angka menurut table konversi berikut:

0 ↔ A	1 ↔ B	2 ↔ C	3 ↔ D	4 ↔ E
5 ↔ F	6 ↔ G	7 ↔ H	8 ↔ I	9 ↔ J
10 ↔ K	11 ↔ L	12 ↔ M	13 ↔ N	14 ↔ O
15 ↔ P	16 ↔ Q	17 ↔ R	18 ↔ S	19 ↔ T
20 ↔ U	21 ↔ V	22 ↔ W	23 ↔ X	24 ↔ Y
25 ↔ Z				

Akhirnya diperoleh plain teks sebagai berikut :

$$P_1 = \begin{bmatrix} 1 & 14 \\ 18 & 0 \end{bmatrix}; \quad P_2 = \begin{bmatrix} 22 & 0 \\ 18 & 3 \end{bmatrix};$$

$$P_3 = \begin{bmatrix} 8 & 18 \\ 0 & 3 \end{bmatrix}; \; P_4 = \begin{bmatrix} 0 & 15 \\ 11 & 14 \end{bmatrix}.$$

Tahap selanjutnya adalah mengenkripsi pesan dengan menggunakan kunci $K = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix}$ dan melakukan perhitungan mod 26 akan diperoleh cipher teks sebagai berikut:

$$C_1 = K + P_1 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix} + \begin{bmatrix} 1 & 14 \\ 18 & 0 \end{bmatrix} = \begin{bmatrix} 19 & 27 \\ 32 & 9 \end{bmatrix} = \begin{bmatrix} 19 & 1 \\ 6 & 9 \end{bmatrix}$$ = TBGJ.

$$C_2 = K + P_2 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix} + \begin{bmatrix} 22 & 0 \\ 18 & 3 \end{bmatrix} = \begin{bmatrix} 40 & 13 \\ 32 & 12 \end{bmatrix} = \begin{bmatrix} 14 & 13 \\ 6 & 12 \end{bmatrix} =$$
ONGM.

$$C_2 = K + P_3 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix} + \begin{bmatrix} 8 & 18 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 26 & 31 \\ 14 & 12 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ 14 & 12 \end{bmatrix} =$$
AFOM.

$$C_4 = K + P_4 = \begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix} + \begin{bmatrix} 0 & 15 \\ 11 & 14 \end{bmatrix} = \begin{bmatrix} 18 & 28 \\ 25 & 23 \end{bmatrix} = \begin{bmatrix} 18 & 2 \\ 25 & 23 \end{bmatrix} =$$
SCZX.

Jadi, pihak 1 akan mengirim pesan **TBGJONGMAFOMSCZX** kepada pihak 2. Selanjutnya pihak 2 akan mendeskripsi pesan tersebut dengan kunci yang sama, yaitu $\begin{bmatrix} 18 & 13 \\ 14 & 9 \end{bmatrix}$ menurut langkah-langkah sebagai berikut :

Langkah 1. Membagi pesan menjadi blok 4 karakter: **TBGJ-ONGM-AFOM-SCZX.**

Langkah 2. Mengubah pesan menjadi matriks yaitu:

$$C_1 = \begin{bmatrix} 19 & 1 \\ 6 & 9 \end{bmatrix}; \; C_2 = \begin{bmatrix} 14 & 13 \\ 6 & 12 \end{bmatrix};$$

$$C_3 = \begin{bmatrix} 0 & 5 \\ 14 & 12 \end{bmatrix}; \; C_4 = \begin{bmatrix} 18 & 2 \\ 25 & 23 \end{bmatrix}.$$

Langkah 3. Mendeskripsi pesan dengan cara sebagai berikut:

$$P_1 = C_1 - K = \begin{bmatrix}19 & 1\\ 6 & 9\end{bmatrix} - \begin{bmatrix}18 & 13\\ 14 & 9\end{bmatrix} = \begin{bmatrix}1 & 14\\ 18 & 0\end{bmatrix} = \textbf{BOSA.}$$

$$P_2 = C_2 - K = \begin{bmatrix}14 & 13\\ 6 & 12\end{bmatrix} - \begin{bmatrix}18 & 13\\ 14 & 9\end{bmatrix} = \begin{bmatrix}22 & 0\\ 18 & 3\end{bmatrix} = \textbf{WASD.}$$

$$P_3 = C_3 - K = \begin{bmatrix}0 & 5\\ 14 & 12\end{bmatrix} - \begin{bmatrix}18 & 13\\ 14 & 9\end{bmatrix} = \begin{bmatrix}8 & 18\\ 0 & 3\end{bmatrix} = \textbf{ISAD.}$$

$$P_4 = C_4 - K = \begin{bmatrix}18 & 2\\ 25 & 23\end{bmatrix} - \begin{bmatrix}18 & 13\\ 14 & 9\end{bmatrix} = \begin{bmatrix}0 & 15\\ 11 & 14\end{bmatrix} = \textbf{APLO}.$$

Pada tahap ini pihak satu telah berhasil membaca pesan tersebut, yaitu **" BOS AWAS DISADAP LO ".**

Kesimpulan

Sifat perkalian matriks atas aljabar min plus dapat diterapkan untuk menentukan kunci sebagai password pada proses pengamanan informasi rahasia. Algoritma untuk menentukan kunci tersebut adalah sebagai berikut:

Pihak 1 atau Pihak 2 mempublikasikan suatu semiring $(Z_{\min})^{n\times n}$ dan $A, B \in (Z_{\min})^{n\times n}$	
Pihak 1	**Pihak 2**
1. Pihak 1 memilih secara rahasia bilangan asli n dan m	1. Pihak 2 memilih secara rahasia bilangan asli r dan s
2. Pihak 1 menghitung $u = A^n B^m$	2. Pihak 2 menghitung $v = A^r B^s$
3. Pihak 1 mengirim u kepada Pihak 2	3. Pihak 2 mengirim v kepada Pihak 1
4. Pihak 1 menerima v dari Pihak 2	4. Pihak 2 menerima u dari Pihak 1
5. Pihak 1 menghitung $K_1 = A^n v\ B^m$	5. Pihak 2 menghitung $K_1 = A^n u\ B^m$
Pihak 1 dan Pihak 2 telah menyepakati kunci rahasia $K = K_1 = K_2$	

Untuk mengamankan informasi rahasia, pesan dapat dienkripsi dengan mengubah pesan menjadi blok-blok karakter sesuai dengan ukuran matriks, kemudian enkripsi dapat dilakukan dengan rumus $C_i = K+P_i$. Pihak penerima pesan dapat mendeskripsi pesan tersebut dengan langkah yang sama dan untuk membaca pesan dapat digunakan rumus $P_i = C_i - K$.

Ucapan Terimakasih

Tim Peneliti mengucapkan terimakasih kepada Universitas Negeri Yogyakarta, khususnya Fakultas MIPA yang telah mendanai kegiatan penelitian ini.

Pustaka

[1] A. J. Menezes, P. C. Oorschoot, dan S. A. Vanstone: Handbook of Applied Cryptography, CRC Press, Canada, 1996.

[2] M. Zaki Riyanto: Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi atas Grup Non-komutatif, dipresentasikan pada Seminar Nasional MIPA, FMIPA UNY Yogyakarta, 2011.

[3] M. Alexei, V. Shpilrain dan A. Ushakov: Group-based Cryptography, Birkhauser Verlag, Basel Switzerland, 2008.

[4] Musthofa: Sistem Persamaan Linear pada Aljabar Min-Plus, dipresentasikan pada Seminar Nasional MIPA, FMIPA UNY Yogyakarta, 2011.

[5] J. Y. Le Boudec, P. Thiran, P: Min-plus System Theory Applied to Communication

Network, Swiss. Didownload pada tanggal 5 Mei 2011.

[6] D. Grigoriev dan S. Vladimir: Tropical Crypthography. Didownload pada tanggal 28 Mei 2013.