Available online at: http://journal.uny.ac.id/index.php/pythagoras
PYTHAGORAS: Jurnal Matematika dan Pendidikan Matematika, 17 (1), 2022, 321-332

Aljabar Semiprima Mendasar dan Aplikasinya pada Protokol Autentikasi

Khurul Wardati [1*], Muhammad Zaki Riyanto [1]
[1] Departemen Matematika, UIN Sunan Kalijaga Yogyakarta, Indonesia
* Corresponding Author. E-mail: khurul.wardati@uin-suka.ac.id

ARTICLE INFO

Article History:
Received: 09-Apr. 2022
Revised: 13-Jun. 2022
Accepted: 08-Nov. 2022

Keywords:
Aljabar semiprima mendasar, *annihilator*, ideal dasar nilpotent, protokol autentikasi.

ABSTRACT

Library research dengan pendekatan deduksi-induksi ini bertujuan untuk mengkaji kesemiprimaan mendasar aljabar tak bebas yang dibangun secara hingga atas ring komutatif unital. Aljabar semiprima mendasar lebih umum dari aljabar semiprima, ditunjukkan dengan suatu contoh penyangkal. Secara teori, Teorema 12. merupakan hasil utama dari penelitian ini. Aljabar dibangun secara hingga bersifat semiprima mendasar jika dan hanya jika ideal dasar nol merupakan irisan dari semua ideal dasar prima, jika dan hanya jika ideal dasar nol merupakan satu-satunya ideal dasar nilpoten. Syarat perlu dan cukup ini serupa dengan sifat aljabar semiprima, dan pembuktian sifat-sifat ini pada keduanya memerlukan konsep *annihilator*. Tujuan secara praktis penelitian ini adalah mengaplikasikan suatu contoh aljabar semiprima mendasar yang non-komutatif pada protokol autentikasi berdasarkan masalah dekomposisi.

This library research is conducted with a deductive-inductive approach. The aim of this study is to explore the basically semiprimeness of the finitely generated non-free algebra over a commutative unital ring. The basically semiprime algebra is more general than a semiprime algebra, which is proven by a counterexample. In theory, Theorem 12 is the main result of the study. The finitely generated algebra over a commutative unital ring is basically semiprime, if and only if, the zero basic ideal is the intersection of all prime basic ideals, if and only if, the zero basic ideal is the only nilpotent basic ideal. These necessary and sufficient conditions are analogous to the properties of a semiprime algebra, and proving these properties in both requires a concept of annihilator. The practical aim of this research is to apply an example of non-commutative basically semiprime algebra in an authentication protocol based on the decomposition problem.

How to Cite:
Wardati, K., & Riyanto, M. Z. (2022). Aplikasi aljabar semiprima mendasar pada protokol autentikasi. *Pythagoras: Jurnal Matematika dan Pendidikan Matematika*, *17*(1), 322-332. https://doi.org/10.21831/pythagoras.v17i1.48982

https://doi.org/10.21831/pythagoras.v17i1.48982

PENDAHULUAN

Secara etimologis, kriptografi (*cryptography*) berarti tulisan atau pesan rahasia. Pengertian kriptografi adalah ilmu tentang berbagai teknik matematika yang berhubungan dengan keamanan informasi (autentikasi dan kerahasiaan). Kriptografi tidak hanya menyelesaikan masalah kerahasian, tetapi juga pada keutuhan data, autentikasi, tanda tangan, sertifikat data, dan aspek-aspek keamanan informasi lainnya (Stinson & Paterson, 2019). Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga seandainya data tersebut dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut (Pabokory et al., 2015). Aljabar memiliki manfaat besar dalam aplikasinya pada kriptografi, khususnya di bidang keamanan jaringan komputer.

Masalah utama saat pengiriman data melalui internet adalah terjadinya pemalsuan atau penipuan identitas, seperti pengiriman pesan menggunakan identitas palsu dan pemalsuan surat digital. Penyelesaian masalah tersebut memerlukan kriptografi yang dikenal dengan protokol autentikasi. Saat ini, protokol autentikasi Diffie-Hellman diaplikasikan secara luas di internet. Autentikasi adalah salah satu cara membuktikan keaslian, yaitu melalui proses pembuktian terhadap identitas pengguna ketika akan memasuki sebuah system (Ranjan & Om, 2015). Skema autentikasi ini, tingkat keamanannya bergantung pada kesulitan menyelesaikan masalah logaritma

diskrit atas grup komutatif (Klima, dkk, 2018). Masa depan komputer kuantum dalam skala besar mampu menyelesaikan masalah logaritma diskrit secara cepat dan mudah (Shor, 1997). Hal ini menunjukkan bahwa titik lemah dari skema autentikasi Diffie Hellman terhadap serangan komputer kuantum adalah penggunaan struktur aljabar komutatif. Salah satu usaha untuk menyangkal serangan komputer kuantum ini adalah dengan menerapkan masalah sulit dari struktur aljabar non-komutatif pada kriptografi, yakni masalah konjugasi dan dekomposisi (Knospe, 2019).

Sebenarnya sudah cukup banyak penelitian penerapan struktur aljabar non komutatif pada protokol pertukaran kunci. Diawali Anshel, dkk (1999) mempublikasikan sebuah protocol pertukaran kunci berdasarkan masalah konjugasi atas grup non-komutatif. Publikasi sistem kriptografi berdasarkan masalah konjugasi atas grup anyaman (*braid group*) yang bersifat non-komutatif dilakukan oleh Ko Lee, dkk (2000) dan atas grup polisiklik (*polycyclic group*) oleh Gryak dan Kahrobaei (Gryak dan Kahrobaei, 2016). Selain itu, Protokol autentikasi dapat dikonstruksi berdasarkan protokol pertukaran kunci masalah konjugasi atas grup endomorfisma (Riyanto, 2017). Konstruksi protokol pertukaran kunci dapat dilakukan berdasarkan masalah dekomposisi atas grup non-komutatif (Stickel, 2005). Telah dikembangkan pula sebuah protokol autentikasi berdasarkan masalah dekomposisi atas grup non-komutatif (Lal dan Chaturwedi, 2005). Masalah konjugasi ditemukan pada grup non-komutatif, sedangkan masalah dekomposisi ditemukan pada struktur aljabar non-komutatif, tidak terbatas pada grup saja (Myasnikov, dkk., 2008).

Secara umum, aljabar (ring) bersifat semiprima jika ideal nol dari aljabar tersebut merupakan ideal semiprima, yaitu kuadrat dari sebarang ideal tak nol juga merupakan ideal tak nol (Abrams, dkk, 2017). Pengertian aljabar semiprima mendasar dikarakterisasi oleh ideal dasar (*basic ideal*). Istilah ideal dasar pertama kali didefinisikan dalam Aljabar Lintasan Leavitt atas ring komutatif unital (Tomforde, 2011). Selanjutnya, Tomforde mengkarakterisasi aljabar $L_R(E)$ sederhana mendasar (*basically simple*) jika aljabar lintasan Leavitt ini hanya mempunyai ideal dasar trivial, yakni ideal nol dan $L_R(E)$.

Penelitian pada $L_R(E)$ dengan memodifikasi ideal dasar (Tomforde, 2011), ditemukan syarat perlu dan cukup keprimaan dan sifat primitive dari aljabar lintasan Leavitt (Larki, 2015). Selain itu, pada graf asiklis berlaku aljabar lintasan Leaviit $L_R(E)$ merupakan hasil tambah langsung dari semua ideal dasar minimal (Kanwar, dkk., 2019). Karena aljabar lintasan Leavitt selalu merupakan aljabar bebas baik atas lapangan (Abrams, dkk, 2017) maupun atas ring komutatif unital (Larki, 2015) maka ideal dasar dapat diperumum dalam aljabar bebas atas ring komutatif unital (Wardati, dkk. 2014). Perumumam definisi ideal dasar pada aljabar bebas dikarenakan titik-titik pada graf sebagai pembangun aljabar lintasan Leavitt bersesuaian dengan basisnya. Jika diberikan aljabar bebas A atas ring komutatif unital R maka ideal $I \subseteq A$ disebut ideal dasar jika dan hanya jika setiap basis $X \subset A$ berlaku:

$$\text{untuk setiap elemen tak nol } r \in R, x \in X \text{ jika } rx \in I \text{ maka } x \in I \qquad (1)$$

Karena $rx \neq 0$ untuk setiap $r \neq 0$ maka ideal nol dalam aljabar bebas selalu merupakan ideal dasar. Selain itu, sebarang ideal dalam aljabar atas lapangan pasti merupakan ideal dasar. Ideal dasar definisi (1) ini telah diimplementasikan untuk mengkarakterisasi aljabar lintasan atas ring komutatif R pada graf hingga E dengan notasi RE yang prima mendasar (Wardati, dkk., 2014). Aljabar lintasan RE juga merupakan aljabar bebas dan lebih general dari $L_R(E)$. Berdasar (1) juga, dapat ditemukan syarat perlu dan cukup sifat semisederhana mendasar (*basically semisimple*) dari aljabar bebas (Wardati, dkk. 2015). Ideal dasar pada aljabar bebas atas ring komutatif unital dapat diperumum pada aljabar yang dibangun secara hingga (belum tentu aljabar bebas). Jika diberikan aljabar $A = \langle X \rangle$ atas ring komutatif unital R dengan X tidak harus bebas linear maka memungkinkan $rx = 0$ untuk suatu elemen tak nol $r \in R, x \in X$. Ideal $I \subseteq A = \langle X \rangle$ disebut ideal dasar jika dan hanya jika,

$$\text{untuk setiap elemen tak nol } r \in R, x \in X \text{ jika } 0 \neq rx \in I \text{ maka } x \in I \qquad (2)$$

Konstruksi generalisasi (2) dalam (Wardati, 2021) untuk menentukan syarat perlu dan cukup ideal dasar prima dan membahas sifat prima mendasar aljabar tak bebas dibangun secara hingga atas ring komutatif unital.

Analog dengan aljabar (ring) semiprima yang lebih umum dari aljabar prima, mudah ditunjukkan bahwa sebarang aljabar dibangun secara hingga bersifat prima mendasar pastilah semiprima mendasar, tetapi tidak sebaliknya. Secara analog pula, aljabar ini dikatakan semiprima mendasar jika ideal nol merupakan ideal dasar semiprima, yakni kuadrat dari sebarang ideal dasar bukanlah ideal nol. Hal ini berakibat bahwa aljabar semiprima merupakan aljabar semiprima mendasar, namun belum tentu sebaliknya. Kesemiprimaan aljabar didefinisikan sebagai aljabar yang *nondegenerate* (Pino dkk., 2008). Aljabar *A* bersifat *nondegenerate* jika dan hanya jika $aAa = \{0\}$ berakibat $a = 0$. Pernyataan ini ekuivalen dengan kontraposisinya, setiap $0 \neq a \in A$ maka $aAa \neq \{0\}$. Sifat *nondegenerate* ini bukanlah syarat perlu dan cukup kesemiprimaan mendasar suatu aljabar, dapat ditunjukkan

dengan contoh kontra. Secara teoritis, syarat perlu dan cukup aljabar dibangun secara hingga bersifat semiprima mendasar merupakan focus utama penelitian ini.

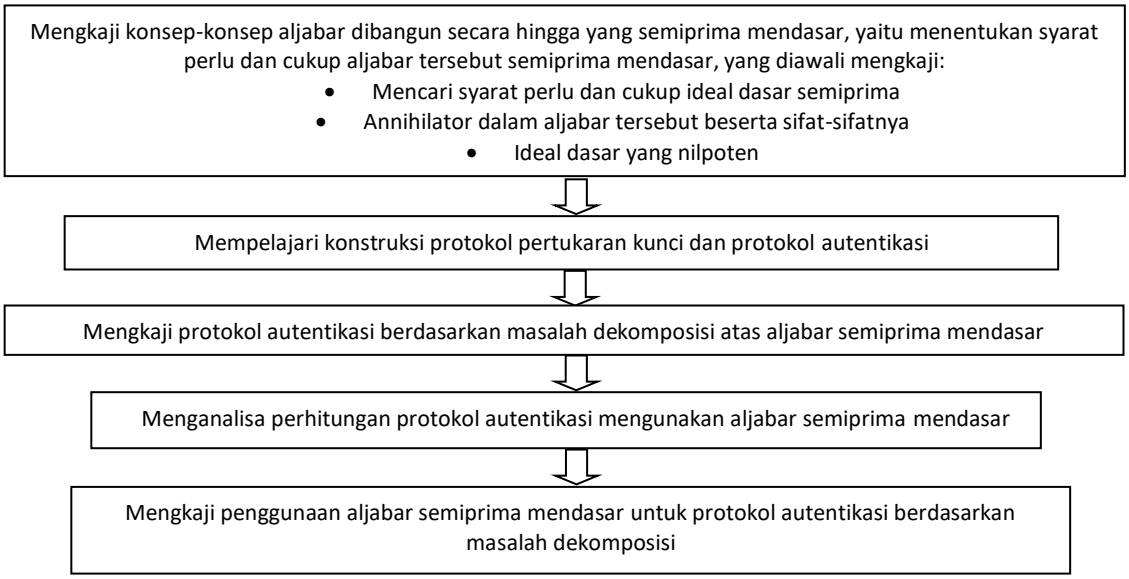
Aljabar unital A bersifat semiprima jika dan hanya jika irisan semua ideal prima merupakan ideal nol (Wisbauer, 2017), jika dan hanya jika ideal nol merupakan satu-satunya ideal nilpoten di A (Hazewinkel dan Gubareni, 2016). Muncullah konjektur atau hipotesis pertama bahwa irisan ideal-ideal dasar prima yang sama dengan ideal nol merupakan syarat perlu dan cukup suatu aljabar (tak bebas) dibangun secara hingga bersifat semiprima mendasar. Pembuktian bahwa irisan semua ideal prima merupakan syarat perlu dan cukup aljabar semiprima, memerlukan pengenol (*annihilator*) dari aljabar. Pengenol ini selalu merupakan ideal (Birkenmeier & Heider, 2019), maka perlu kajian syarat-syarat agar annihilator merupakan ideal dasar sebagai alat bantu menjawab konjektur pertama. Jika ideal nol merupakan satu-satunya ideal nilpoten maka sebarang ideal tak nol bukanlah ideal nilpoten, yaitu ideal dipangkatkan bilangan bulat positif hasilnya bukan ideal nol. Ideal nol pasti merupakan ideal dasar dari sebarang aljabar, maka konjektur kedua bahwa suatu aljabar semiprima mendasar jika dan hanya jika sebarang ideal dasar taknol bukan merupakan ideal nilpoten. Artinya aljabar semiprima mendasar tidak memuat ideal dasar nilpotent tak nol (*non-zero nilpotent basic ideal*). Istilah ini mengacu pada temuan bahwa aljabar lintasan Leavitt $L_R(E)$ tidak memuat ideal dasar nilpotent tak nol jika dan hanya jika graf E memenuhi kondisi L (Kanwar dkk., 2019).

Menindaklanjuti temuan Myasnikov dkk. (2008), dapat dikembangkan suatu protokol autentikasi didasarkan pada masalah dekomposisi atas suatu aljabar semiprima mendasar yang non-komutatif. Secara tegas, tujuan utama secara teoritis artikel ini akan mengkaji kesemiprimaan mendasar aljabar tak bebas yang dibangun secara hingga atas ring komutatif unital. Kajian tersebut bertumpu pada syarat perlu dan cukup aljabar tersebut semiprima mendasar. Terdapat tiga pernyataan yang ekuivalen dengan aljabar semiprima mendasar yang seluruhnya memerlukan bukti formal. Temuan teori matematik ini akan diterapkan pada kriptografi khususnya protokol autentikasi, sehingga riset ini juga merupakan penelitian terapan. Struktur aljabar semiprima mendasar secara umum merupakan aljabar non-komutatif. Diambil suatu contoh aljabar semiprima mendasar yang akan diterapkan pada protokol autentikasi sebagai tujuan praktis dari penelitian ini.

METODE

Penelitian teoritis matematis ini merupakan riset pustaka (*library research*), karena semua referensi sebagai sumber data utama penelitian (Zed, 2014). Proses perumuman atau generalisasi merupakan metode yang lazim digunakan dalam penelitian di bidang Matematika (khususnya aljabar). Pendekatan penelitiannya merupakan penelitian kualitatif dengan metode deduktif-induktif. Deduksi adalah proses ilmiah dalam pengambilan simpulan yang bertumpu pada premis-premis tertentu, sementara induksi merupakan pola berpikir berdasarkan pada realitas atau fenomena untuk membuat simpulan dan keduanya memerlukan keabsahan dengan bukti logis matematis (Sari, 2016).

Riset ini juga merupakan penelitian terapan karena temuan teori matematik ini akan diterapkan pada kriptografi. Aljabar dibangun secara hingga atas ring komutatif unital dan bersifat semiprima mendasar ini akan diaplikasikan sebagai sebuah struktur aljabar non-komutatif untuk mendukung proses autentikasi berdasarkan masalah dekomposisi. Prosedur penelitian secara utuh disajikan dalam bagan alir, pada Gambar 1. Proses autentikasi berdasarkan masalah dekomposisi dimulai dari penentuan parameter publik dan rahasia yang dimiliki oleh kedua belah pihak yang akan berkomunikasi, yaitu pihak verifikator dan pihak yang akan membuktikan kebenaran identitasnya. Selanjutnya, kedua belah pihak melakukan serangkaian perhitungan-perhitungan tertentu yang melibatkan parameter publik dan rahasia. Langkah terakhir adalah pihak verifikator yang memutuskan apakah identitasnya benar atau salah. Keamanan dari proses autentikasi diletakkan pada masalah sulit dalam matematika, dalam hal ini adalah masalah dekomposisi atas aljabar semiprimam mendasar.



Gambar 1. *Flowchart* penelitian

HASIL PENELITIAN DAN PEMBAHASAN

Aljabar semiprima mendasar atas ring komutatif unital

Penelitian teoritis matematis ini, dibatasi pada aljabar unital dibangun secara hingga atas ring komutatif unital dan secara umum bukan aljabar bebas. Selanjutnya, secara ringkas hanya dikatakan aljabar dibangun secara hingga. Pembangun berhingga ini merupakan pembangun minimal, artinya jika elemen pembangun dikeluarkan paling sedikit satu elemen maka tidak merentang aljabar tersebut. Selain itu, pembangun minimal ini secara umum tidak bebas linear.

Aljabar bebas atas ring komutatif unital selalu berlaku berlaku $rx \neq 0$ untuk setiap elemen tak nol r dalam ringnya dan setiap elemen x dalam basis. Sifat ini berpengaruh dalam perumuman ideal dasar dalam aljabar tak bebas.

Definisi 1. (Wardati, 2018*)* Diberikan R-aljabar *unital* A dengan R ring komutatif *unital.* Himpunan *A* disebut *R*-aljabar dibangun secara hingga jika *R*-aljabar $A = \langle X \rangle$, dengan X berhingga dan X adalah pembangun minimal yang belum tentu bebas linear. Ideal I di A dikatakan ideal dasar, jika dan hanya jika untuk setiap elemen tak nol $r \in R$, dan setiap $x \in X$, berlaku jika $0 \neq rx \in I$ maka $x \in I$. Ideal dasar P di A disebut ideal dasar prima jika dan hanya jika, setiap ideal dasar $X, Y \subseteq A$ berlaku jika $XY \subseteq P$ maka $X \subseteq P$ atau $Y \subseteq P$.

Jika $A = \langle X \rangle$ adalah *R*-aljabar bebas maka definisi ideal dasar J, yakni untuk setiap elemen tak nol $r \in R$ dan $x \in X$ dengan $rx \in J$ berakibat $x \in J$, merupakan kasus khusus jika pembangunnya bebas linear. Perlu dipertegas bahwa *R*-aljabar dibangun secara hingga dalam Definisi 1 adalah

$$A = \langle X \rangle = \{\textstyle\sum_{i=1}^{m} r_i x_i : r_i \in R, x_i \in X, m \in \mathbb{N}\}$$

dengan X tidak harus bebas linear. Sifat penting ideal dasar dalam aljabar dibangun secara hingga di bawah ini akan sering digunakan untuk pembuktian sifat-sifat aljabarnya.

Lemma 2. (Wardati, 2018) Jika diberikan $A = \langle X \rangle$ adalah *R*-aljabar dibangun secara hingga maka :

1. Setiap $x \in X$ berlaku $x \in I$ jika dan hanya jika x merupakan suatu elemen pembangun dari *I* sebagai *R*-submodul dari *A*;
2. Untuk setiap elemen tak nol $r_i \in R$ dan setiap $x_i \in X$, dengan $i = 1, 2, \ldots, n$ untuk suatu $n \in \mathbb{N}$, jika $0 \neq \sum_{i=1}^{n} r_i x_i \in I$ maka $x_i \in I$ untuk setiap i;
3. Ideal dasar $I = \langle X_I \rangle$ dengan $X_I = X \cap I$.

Jika diperhatikan Definisi 1, definisi ideal dasar prima dalam aljabar dibangun secara hingga analog dengan ideal prima dalam (Wisbauer, 2017). Analogi tersebut juga digunakan dalam mendefinisikan ideal dasar semiprima. Terminologi ideal dasar semiprima merupakan perumuman dari ideal dasar prima, sebagaimana ideal prima pasti merupakan ideal semiprima dan tidak sebaliknya.

Definisi 3. (Wardati, 2021) Diberikan *R*-aljabar dibangun secara hingga *A*. Ideal dasar S di A disebut ideal dasar semiprima jika dan hanya jika, setiap ideal dasar $I \subseteq A$ berlaku jika $I^2 \subseteq S$ maka $I \subseteq S$.

Analogi terminologi ideal semiprima dan ideal dasar semiprima ini tidak menjadikan keduanya saling berkaitan. Contoh 4 di bawah ini akan memberikan penyangkal kondisi tersebut. Contoh penyangkal ideal dasar semprima tetapi bukan ideal dasar prima juga diberikan, selain sebagai penguatan ideal dasar Definisi 1.

Contoh 4. Diberikan $\mathcal{M} = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ 0 & \mathbb{Z}_6 \end{pmatrix}\right]$ adalah $\mathbb{Z}$-aljabar dibangun secara hingga, dan ideal-ideal dari $\mathcal{M}$ berikut :

$I = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix}\right]; J = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix}\right]; K = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right];$
$L = \left[\begin{pmatrix} 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \\ 16\mathbb{Z}_{256} & 16\mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & 0 \end{pmatrix}\right]$ dan $M = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \mathbb{Z}_6 \\ 0 & \mathbb{Z}_6 \end{pmatrix}\right]$

Menurut Definisi 1, hanyalah ideal L yang bukan ideal dasar di $\mathcal{M}$ karena elemen pembangun standar $x = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right] \notin L$ dan $16x \in L$. Oleh karenanya, L bukan ideal dasar semiprima tetapi L merupakan ideal semiprima di $\mathcal{M}$. Perhatikan bahwa I ideal dasar semiprima di $\mathcal{M}$ berdasar Definisi 3, tetapi bukan ideal dasar prima karena ideal dasar $J, M \not\subset I$ dan $JM = I$. Selain itu, ideal I tidak semiprima di $\mathcal{M}$ karena $L^2 = \{0\} \subset I$ dan $L \not\subset I$. Ideal J adalah semiprima dan sekaligus merupakan ideal dasar semiprima, sementara ideal dasar K tidak keduanya.

Jika diberikan *R*-aljabar dibangun secara hingga $A = \langle X \rangle$ dan $x \in X$ maka A dapat dipandang sebagai ring. Selain itu, $(x) = \{\sum_i a_i x b_i : a_i, b_i \in A\}$ merupakan ideal dan dikatakan ideal dibangun oleh x (Bland, 2011). Lebih penting dari itu, berdasarkan pada Lemma 3.5 dalam (Wardati, 2018) bahwa (x) merupakan ideal dasar di A. Ideal dasar yang dibangun oleh suatu elemen dalam aljabar sebagai ring dapat digunakan untuk menyelidiki suatu ideal dasar semiprima.

Proposisi 5. (Wardati, 2021) Diberikan *R*-aljabar yang dibangun secara hingga $A = \langle X \rangle$ dan ideal dasar $S \subset A$, maka ketiga pernyataan di bawah ini ekuivalen:

1. Ideal S adalah ideal dasar semiprima
2. Untuk setiap $a \in A$ dengan (a) ideal dasar di *A*, jika $(a)^2 \subseteq S$ maka $a \in S$
3. Untuk setiap $a \in A$ dengan (a) ideal dasar di *A*, jika $aAa \subseteq S$ maka $a \in S$.

Aljabar semiprima dikarakterisasi oleh ideal nolnya sebagaimana aljabar prima. Aljabar semiprima didefinisikan sebagai aljabar yang ideal nolnya merupakan ideal semiprima (Wisbauer, 2017). Ideal nol pasti merupakan ideal dasar. Karakterisasi ideal dasar nol yang merupakan ideal dasar semiprima akan mengkarakterisasi sifat aljabar semiprima mendasar.

Definisi 6. *R*-aljabar yang dibangun secara hingga A dikatakan semiprima mendasar jika ideal nol merupakan ideal dasar semiprima.

Jika Ideal nol semiprima maka kuadrat sebarang ideal taknol juga bukan ideal nol. Akibatnya, kuadrat dari sebarang ideal dasar tak nol bukanlah ideal dasar nol. Artinya, ideal nol semiprima pastilah ideal nol tersebut merupakan ideal dasar semiprima, tetapi tidak sebaliknya. Sebagai contoh penyangkal, ideal nol di *K* sebagai $\mathbb{Z}$-aljabar pada Contoh 4. merupakan ideal dasar semiprima. Namun, ideal nol ini bukan ideal semiprima di K karena $L^2 = \{0\}$ dan ideal tak nol $L \subset K$.

Akibat 7. Aljabar dibangun secara hingga yang semiprima merupakan aljabar semiprima mendasar.

Menurut Pino dkk. (2008), suatu aljabar A bersifat semiprima jika dan hanya jika A bersifat *nondegenerate*, yaitu untuk setiap $a \in A$ jika $aAa = \{0\}$ maka $a = 0$. Jika *R*-aljabar dibangun secara hingga $A = \langle X \rangle$ bersifat *nondegerate* maka poin 3) dalam Proposisi 5. terpenuhi, yaitu untuk setiap $a \in A$ dengan (a) ideal dasar di *A, dan* $aAa = \{0\}$ maka $a = 0$. Artinya jika $A = \langle X \rangle$ bersifat *nondegerate* maka ideal nol di A merupakan ideal dasar semiprima.

Akibat 8. Jika *R*-aljabar dibangun secara hingga A semiprima atau bersifat *nondegenerate* maka aljabar A semiprima mendasar.

Akibat 8 ini tidak berlaku konversnya, maka aljabar semiprima mendasar lebih umum dari pada aljabar semiprima. Contoh 9. Di bawah ini merupakan penyangkal yang mempertegas perumuman semiprima ke semiprima mendasar aljabar dibangun secara hingga. Selain itu, contoh ini menunjukkan bahwa sifat *nondegenerate* bukan merupakan syarat perlu sifat semiprima mendasar dari aljabar dibangun secara hingga.

Contoh 9. Diberikan $\mathcal{M}' = \begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}$ adalah $\mathbb{Z}$-aljabar dibangun secara hingga, maka $\mathcal{M}'$ tidak bersifat *nondegenerate.* karena,$\begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} \mathcal{M}' \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix} = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$. Artinya, $\mathcal{M}'$ tidak semiprima. Namun, untuk setiap matriks X di $\mathcal{M}'$ dengan (X) ideal dasar, jika $X\mathcal{M}'X = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$ maka $X = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Artinya, $\mathbb{Z}$-aljabar $\mathcal{M}'$ merupakan aljabar semiprima mendasar tetapi tidak semiprima.

Selain elemen pembagi nol, dalam Aljabar dibangun secara hingga A atas ring komutatif unital R dikenal istilah pengenol (*annihilator*), karena A merupakan ring sekaligus *R*-modul. *Annihilator* (dua sisi) dari S dalam aljabar A dinotasikan dan didefinisikan sebagai

$$Ann(S) = \{a \in A : as = 0 = sa, \forall s \in S\} = Ann^l(S) \cap Ann^r(S)$$

dengan $Ann^l(S) = \{a \in A : as = 0, \forall s \in S\}$; $Ann^r(S) = \{a \in A : sa = 0, \forall s \in S\}$ adalah *annihilator* kiri dan kanan secara berurutan (Wisbauer, 2017). *Annihilator* ini berperan banyak dalam pembuktian semiprima mendasar aljabar dibangun secara hingga, sebagaimana diilustrasikan pada Contoh 10.

Contoh 10. Diberikan $\mathbb{Z}$-aljabar $\aleph = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ \mathbb{Z}_6 & \mathbb{Z}_6 \end{pmatrix} \right]$. Aljabar $\aleph$ hanya memiliki ideal dasar nontrivial $K = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right], K' = \left[\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ \mathbb{Z}_6 & \mathbb{Z}_6 \end{pmatrix} \right]$ dan $KK' = \{0\}$, sehingga ideal nol bukan ideal dasar prima tetapi merupakan ideal dasar semiprima. Jadi, Aljabar $\aleph$ bukan aljabar prima mendasar tetapi semiprima mendasar. Selain itu, K, K' ideal dasar prima dengan $K \cap K' = \{0\}$. Perhatikan bahwa $ann(K) = K'$ dan $ann(K') = K$ sehingga $K.ann(K) = ann(K').K' = \{0\}$.

Contoh 10. memberikan indikasi bahwa ideal nol merupakan ideal dasar semiprima jika dan hanya jika irisan semua ideal dasar prima merupakan ideal nol. Indikasi ini diilhami oleh sifat bahwa ideal nol semiprima jika dan hanya jika ideal nol merupakan irisan semua ideal prima (Wisbauer, 2017), yang karakterisasi ini memerlukan konsep *annihilator*. Jika dicermati, Contoh 10 juga mengindikasikan sifat bahwa *annihilator* dari ideal dasar juga merupakan ideal dasar.

Lemma 11. Diberikan *R*-aljabar yang dibangun secara hingga A dan $I \subseteq A$.

1. Jika $J \subseteq I$ maka $Ann^l(I) \subseteq Ann^l(J)$, $Ann^r(I) \subseteq Ann^r(J)$ dan $Ann(I) \subseteq Ann(J)$
2. Jika I ideal dasar maka secara berurutan $Ann^l(I), Ann^r(I)$ dan $Ann(I)$ adalah ideal kiri dasar, ideal kanan dasar dan ideal dasar.

Bukti : Sangat jelas bukti poin 1. dengan menggunakan definisi *annihilator* kiri, kanan dan dua sisi. Tanpa mengurangi keumuman bukti, poin 2. hanya dibuktikan bahwa $Ann(I)$ adalah ideal dasar dari A. Karena $Ann(I)$ merupakan ideal (dua sisi) dari A (Wisbauer, 2017) maka selanjutnya ambil sebarang elemen tak nol $r \in R, x \in X$ dengan $0 \neq rx \in Ann(I)$. Akan ditunjukkan bahwa $xu = 0 = ux$ atau $x \in Ann(I)$. Karena $rx \in Ann(I)$ maka $(rx)u = 0 = u(rx)$, untuk setiap $u \in I$. Andaikan $xu \neq 0$ atau $ux \neq 0$ untuk suatu $u \in I$, maka $xu, ux \in I$. Menurut Lemma 2., ideal dasar $I = \langle H \rangle, H = X \cap I$, sehingga $0 \neq xu = \sum_{i=1}^{k} r_i h_i$ untuk suatu $r_i \in R, h_i \in H \subseteq X$. Artinya, terdapat m dengan $1 \leq m \leq k$ sedemikian sehingga $r_m h_m \neq 0$ dan $r r_m h_m \neq 0$ untuk suatu $r \in R$. Akibatnya, $r(xu) = r\sum_{i=1}^{k} r_i h_i = \sum_{i=1}^{k} r r_i h_i \neq 0$ untuk suatu $u \in I$, kontradiksi dengan $r(xu) = (rx)u = 0$ untuk setiap $u \in I$. Diperoleh, $xu = 0$ dan secara analog didapat pula $ux = 0$, maka $x \in Ann(I)$. Jadi, untuk setiap elemen tak nol $r \in R, x \in X$ dengan $0 \neq rx \in Ann(I)$ maka $x \in Ann(I)$. Dengan kata lain, $Ann(I)$ merupakan ideal dasar dari *R*-aljabar yang dibangun secara hingga A.

Karakterisasi ideal nol merupakan ideal semiprima dapat dipandang dari sifat lain, berkaitan dengan ideal nilpoten. Syarat perlu dan cukup suatu ring (aljabar) merupakan ring (aljabar) semiprima, yaitu ideal nol merupakan satu-satunya ideal nilpoten (Hazewinkel dan Gubareni, 2016). Syarat ini ekuivalen dengan setiap ideal tak nol bukan ideal nilpotent. Ideal nol merupakan ideal dasar semiprima jika dan hanya jika kuadrat setiap ideal dasar tak nol pasti tak nol pula. Hal ini mengindikasikan bahwa setiap ideal dasar tak nol bukan merupakan ideal nilpotent, jika ideal nol merupakan ideal dasar semiprima.

Teorema 12. Diberikan *R*-aljabar dibangun secara hingga $A = \langle X \rangle$, maka pernyataan-pernyataan berikut ekuivalen.

1. Aljabar A semiprima mendasar
2. Irisan dari semua ideal-ideal dasar prima adalah ideal nol
3. Setiap ideal dasar tak nol bukan merupakan ideal nilpoten

4. Setiap $x \in X, xAx \neq \{0\}$

Bukti :

$(1 \Rightarrow 2)$ Misalkan $\wp = \{P \subset A: P \text{ ideal dasar prima}\}$. Akan dibuktikan bahwa $\bigcap_{P\in\wp} P = \{0\}$. Artinya, untuk setiap $0 \neq a \in A$ maka $a \notin \bigcap_{P\in\wp} P$, sehingga terdapat ideal dasar prima P dan $a \notin P$. Karena A ideal dasar trivial maka menurut Lemma 11., $Ann(A)$ merupakan ideal dasar dari A. Diperoleh bahwa $(Ann(A))^2 \subseteq Ann(A).A = \{0\}$ dan $Ann(A) = \{0\}$ karena $\{0\}$ merupakan ideal dasar semiprima.

Perlu ditunjukkan bahwa untuk setiap $0 \neq a \in A$ berlaku $aAa \neq \{0\}, AaA \neq \{0\}$. Pertama, andaikan $aAa = \{0\}$ maka $(AaA)^2 = AaAAaA \subseteq AaAaA = \{0\}$. Karena $\{0\}$ ideal dasar semiprima, haruslah $AaA = \{0\}$. Aljabar A memuat elemen satuan maka $a = 1_A a 1_A \in AaA$, sehingga diperoleh $a = 0$ yang kontradiksi dengan $a \neq 0$. Jadi, $aAa \neq \{0\}$. Kedua, andaikan $AaA = \{0\}$ maka $Aa \subseteq Ann(A) = \{0\}$ sehingga $a \in Ann(A) = \{0\}$. Artinya, $a = 0$ dan kontradiksi dengan $a \neq 0$. Jadi, $AaA \neq \{0\}$.

Dibentuk suatu barisan $\{a_n\}_{n\in\mathbb{N}}$ dengan $0 \neq a_n \in A$ untuk setiap $n \in \mathbb{N}$. Ambil sebarang $0 \neq a \in A$ dan pilih $a = a_1$ maka $a_1 A a_1 \neq \{0\}$ karena $a_1 \neq 0$. Pilih a_2 sehingga $0 \neq a_2 \in a_1 A a_1$ dan $a_2 A a_2 \neq \{0\}$ maka dipilih $a_3$sehingga $a_3 \neq 0$ dan $a_3 \in a_2 A a_2$. Demikian seterusnya, diperoleh $a_n \neq 0$ untuk setiap $n \in \mathbb{N}$, sehingga dapat dipilih $0 \neq a_{n+1} \in a_n A a_n$. Jadi, diperoleh barisan elemen-elemen tak nol di A, yakni $S = \{a_n\}_{n\in\mathbb{N}} \subset A$. Selanjutnya dibentuk keluarga ideal-ideal dasar di A yang saling asing dengan S, yakni $\Im_S = \{I \subseteq A: I \text{ ideal dasar dengan } I \cap S = \{0\}\}$.

Menurut Lemma Zorn, terdapat elemen maksimal $P \in \Im_S$ maka P ideal dasar dan $P \cap S = \{0\}$ sehingga jika $a \in S$ maka $a \notin P$. Jadi, diperoleh bahwa setiap $0 \neq a \in A$ maka $a \notin P$ untuk suatu ideal dasar P. Selanjutnya, ditunjukkan elemen maksimal $P \in \Im_S$ adalah ideal dasar prima. Ambil sebarang ideal dasar $L, M \subseteq A$ dengan $L \not\subset P$ dan $M \not\subset P$ maka $P \subset P + L, P \sqsubset P + M$. Karena $P \in \Im_S$ maka $P \cap S = \{0\}$ sehingga $(P + L) \cap S \neq \emptyset$ dan $(P + M) \cap S \neq \emptyset$. Hal ini berarti bahwa terdapat $i, j \in \mathbb{N}$ sehingga $a_i \in P + L, a_j \in P + M$. Dapat dipilih suatu $k > maks(i, j)$ sehingga dengan pembentukan himpunan S, diperoleh : $a_{k+1} \in a_k A a_k \subseteq (P + L)(P + M) \subseteq P + LM$, dan $LM \not\subset P$ karena $a_{k+1} \notin P$. Jadi, untuk setiap ideal-ideal dasar $L, M \subseteq A$, jika $LM \subset P$ maka $L \subset P$ atau $M \subset P$ karena implikasi ini senilai dengan jika $L \not\subset P$ dan $M \not\subset P$ maka $LM \not\subset P$. Dengan kata lain, P merupakan ideal dasar prima. Hal ini membuktikan bahwa setiap $0 \neq a \in A$ terdapat ideal dasar prima P sehingga $a \notin P$. Artinya, $\bigcap_{P\in\wp} P = \{0\}$, atai ideal dasar nol merupakan irisan semua ideal dasar prima di A.

$(2 \Rightarrow 3)$ Andaikan terdapat ideal dasar nilpoten $I \neq \{0\}$, yakni $I^k = \{0\}$ untuk suatu $k \in \mathbb{N}$. Menurut hipotesis, I^k adalah irisan dari semua ideal dasar prima di A. Artinya, $I^k = I^{k-1} I \subseteq P$ maka $I \subset P$ untuk setiap ideal dasar prima P. Diperoleh, I subhimpunan dari irisan semua ideal dasar prima di A sehingga $I = \{0\}$ yang kontradiksi dengan $I \neq \{0\}$. Jadi, setiap ideal dasar tak nol bukan merupakan ideal nilpotent.

$(3 \Rightarrow 4)$ Ambil sebarang elemen pembangun $x \in X \subset A$, maka ideal (x) merupakan ideal dasar dan $(x) \neq \{0\}$ sehingga $(x)^2 \neq \{0\}$ karena setiap ideal tak nol bukan ideal nilpotent. Kita menunjukkan bahwa $xAx \neq \{0\}$, sebagai berikut.

Andaikan $xAx = \{0\}$ untuk suatu $x \in X$ maka $xax = 0$ untuk setiap $a \in A$. Ambil sebarang $y \in (x)^2$ maka $y = (pxq)(rxs)$ untuk suatu p, q, r, s di A, sehingga $y = px(qr)xs = p\{xax)s = p0s = 0$ dengan $a = qr \in A$. Jadi, setiap $y \in (x)^2$ maka $y = 0$. Dengan kata lain, $(x)^2 = \{0\}$ yang kontradiksi dengan $(x)^2 \neq \{0\}$. Jadi, $xAx \neq \{0\}$ untuk setiap $x \in X$.

$(4 \Rightarrow 1)$ Ambil sebarang ideal tak nol S di $A = \langle X \rangle$. Berdasarkan Lemma 4.1.3, poin 3), $S = \langle X_S \rangle$ sebagai R-modul dengan $X_S = X \cap S$. Ambil sebarang $s \in X_S$ maka $s \in X$ dan terdapat $a \in A$ dengan $sas \neq 0$. Selain itu, $s \in S$ sehingga $0 \neq sas = (1_A sa)(1_A s 1_A) \in S^2$. Tampak bahwa $S^2 \neq \{0\}$, artinya kuadrat dari setiap ideal dasar tak nol di A, juga tak nol. Terbukti, aljabar dibangun secara berhingga A merupakan aljabar semiprima mendasar karena $\{0\}$ merupakan ideal dasar semiprima di A.

Kajian teoritis aljabar dibangun secara hingga atas ring komutatif unital ini dapat diterapkan dalam kriptografi. Sebagaimana diuraikan dalam pendahuluan, diperlukan struktur aljabar non-komutatif dalam terapan tersebut. Salah satu contoh struktur aljabar non-komutatif adalah aljabar semiprima mendasar, dan masalah sulit yang ditemui pada aljabar semiprima mendasar adalah masalah dekomposisi. Oleh karena itu, akan dikonstruksi protokol autentikasi atas aljabar semiprima mendasar berdasarkan masalah dekomposisi.

Terapan aljabar semiprima mendasar pada protokol autentikasi

Kriptografi tidak hanya menyelesaikan masalah kerahasiaan, tetapi juga dituntut untuk mampu menyelesaikan masalah autentikasi identititas yang disebut dengan protokol autentikasi (Vasco dan Steinwandt, 2015). Tujuan dari protokol autentikasi adalah agar kedua belah pihak yang akan berkomunikasi dapat saling mempercayai kebenaran identitasnya, sebelum dilakukan komunikasi informasi. Protokol autentikasi berbasis kunci publik pertama kali dikembangkan dari protokol pertukaran kunci Diffie-Hellman, berdasarkan masalah logaritma diskrit atas grup komutatif. Hingga saat ini, protokol pertukaran kunci Diffie-Hellman masih digunakan secara luas di internet (Baumslag, dkk., 2015). Grup komutatif tersebut, di antaranya adalah grup kurva elliptik. Protokol autentikasi memiliki langkah-langkah berurutan dan dilakukan oleh dua pihak, yakni Alice dan Bob. Alice sebagai pihak pertama akan melegitimasi identitas dan Bob sebagai pihak kedua yang melakukan verifikasi identitas. Langkah pertama adalah Alice mempublikasikan parameter publiknya, kemudian Alice memilih parameter rahasia, menghitungnya dengan suatu fungsi, dan mengirimkan hasilnya kepada Bob. Selanjutnya, Bob memberi tantangan kepada Alice yang harus direspon oleh Alice dengan benar. Protokol autentikasi digunakan sebelum komunikasi utama dimulai.

Perkembangan komputer kuantum memberikan ancaman serius pada kriptografi kunci publik yang didasarkan pada struktur aljabar komutatif. Komputer kuantum dapat menyelesaikan masalah logaritma diskrit dan masalah faktorisasi dalam waktu polinomial, sehingga apabila komputer kuantum dalam skala besar dapat terwujud, maka dapat mengancam keamanan internet (Horan dan Kahrobaei, 2018). Adanya ancaman tersebut mengharuskan para peneliti di bidang kriptografi untuk mencari pengganti dari protokol autentikasi Diffie-Hellman. Salah satu titik lemah serangan komputer kuantum terhadap protokol autentikasi Diffie-Hellman adalah penggunaan struktur aljabar komutatif. Oleh karena itu, perlu dikembangkan protokol autentikasi berdasarkan struktur aljabar non-komutatif.

Penggunaan struktur aljabar non-komutatif untuk protokol autentikasi telah dilakukan oleh Lal dan Chatuwedi (2005) berdasarkan masalah dekomposisi atas grup non-komutatif, sebagai berikut. Diberikan A_1, A_2, B_1, B_2 subgrup-subgrup dari grup non-komutatif *G* sedemikian hingga elemen-elemen dari A_1 dan B_1 saling komutatif, dan elemen-elemen dari A_2 dan B_2 juga saling komutatif.

1. Alice memililih $a_1 \in A_1$, $a_2 \in A_2$ dan $w \in G$.
2. Alice menghitung $t = a_1 w a_2$.
3. Alice mengirimkan *w* dan *t* kepada Bob.
4. Bob memilih $b_1 \in B_1$ dan $b_2 \in B_2$, kemudian menghitung $w' = b_1 w b_2$.
5. Bob mengirimkan w' sebagai tantangan (challenge) untuk Alice.
6. Alice menghitung $w'' = a_1 w' a_2$.
7. Alice mengirimkan w'' sebagai respon untuk Bob.
8. Bob melakukan verifikasi apakah memenuhi kondisi $w'' = b_1 t b_2$?

Salah satu struktur aljabar non-komutatif adalah aljabar semiprima mendasar. Protokol autentikasi yang dikembangkan oleh Lal dan Chatuwedi (2005) di atas dapat dimodifikasi sehingga dapat diterapkan pada aljabar semiprima mendasar. Hal ini dikarenakan pada protokol tersebut tidak melibatkan penggunaan invers, sedangkan subgrup diganti dengan ideal yang dibangun oleh sebuah elemen, seperti diberikan pada protokol autentikasi berikut ini:

1. Alice memilih aljabar semiprima mendasar yang dibangun secara hingga *A* atas ring komutatif dengan elemen satuan *R,* mempublikasikan suatu ideal dasar semiprima J dari *A*, dan suatu elemen $a \in A$.
2. Alice memilih $w \in J$ dan $m, n \in \mathbb{N}$, kemudian menghitung $t = a^m w a^n$.
3. Alice mengirimkan *w* dan *t* kepada Bob.
4. Bob memilih secara rahasia $u, v \in \mathbb{N}$, kemudian menghitung $w' = a^u w a^v$.
5. Bob mengirimkan w' sebagai tantangan (*challenge*) untuk Alice.
6. Alice menghitung $w'' = a^m w' a^n$.
7. Alice mengirimkan respon w'' kepada Bob.
8. Bob melakukan verifikasi apakah berlaku $w'' = a^u t a^v$?

Dapat ditunjukkan bahwa protokol ini dapat berjalan, karena terpenuhinya:

$$a^u t a^v = a^u a^m w a^n a^v = a^{u+m} w a^{n+v} = a^{m+u} w a^{n+v} = a^m a^u w a^n a^v = a^m w' a^v = w''.$$

Tingkat keamanan dari protokol autentikasi ini didasarkan pada masalah dekomposisi, yaitu menentukan nilai a^m dan a^n apabila diketahui nilai $t = a^m w a^n$ dan w, atau masalah menentukan nilai a^u dan a^v apabila diketahui nilai $w' = a^u w a^v$ dan w, yang berarti masalah menentukan $m, n \in \mathbb{N}$, atau $u, v \in \mathbb{N}$. Kajian tentang tingkat keamanan dari kriptografi berbasis struktur aljabar non-komutatif telah dikemukakan oleh Roman'kov (Roman'kov, 2017). Salah satu hal penting yang mempengaruhi tingkat kesulitan masalah dekomposisi adalah pemilihan struktur aljabar non-komutatif. Berikut ini diberikan contoh sederhana protokol autentikasi menggunakan aljabar semiprima mendasar.

Contoh 13. Berikut ini diberikan contoh sederhana protokol autentikasi menggunakan aljabar semiprima mendasar. Dalam kasus ini, sebagai pihak yang ingin membuktikan identitasnya adalah Alice, dan pihak verifikator adalah Bob.

1. Alice memilih aljabar semiprima mendasar $\aleph = \left[\begin{pmatrix} \mathbb{Z}_{256} & \mathbb{Z}_{256} \\ \mathbb{Z}_{256} & \mathbb{Z}_{256} \end{pmatrix}, \begin{pmatrix} \mathbb{Z}_6 & \mathbb{Z}_6 \\ \mathbb{Z}_6 & \mathbb{Z}_6 \end{pmatrix}\right]$ atas ring $\mathbb{Z}$ pada Contoh 10, suatu elemen $a = \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right) \in \aleph$ dan suatu ideal dasar semiprima $J = \aleph$.
2. Alice memilih $w = \left(\begin{pmatrix} 35 & 203 \\ 196 & 182 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}\right) \in J, m = 34\ dan\ n = 45$, kemudian menghitung
$$t = \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{34} \left(\begin{pmatrix} 35 & 203 \\ 196 & 182 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}\right) \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{45}$$
$$= \left(\begin{pmatrix} 90 & 196 \\ 187 & 235 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}\right)$$
3. Alice mengirimkan $w = \left(\begin{pmatrix} 35 & 203 \\ 196 & 182 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 5 & 4 \end{pmatrix}\right)$ dan $t = \left(\begin{pmatrix} 90 & 196 \\ 187 & 235 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}\right)$ kepada Bob.
4. Bob memilih $u = 47, v = 54$, kemudian menghitung
$$w' = \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{47} \left(\begin{pmatrix} 35 & 203 \\ 196 & 182 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}\right) \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{54}$$
$$= \left(\begin{pmatrix} 225 & 187 \\ 11 & 203 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 0 \end{pmatrix}\right)$$
5. Bob mengirimkan $w' = \left(\begin{pmatrix} 225 & 187 \\ 11 & 203 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 0 \end{pmatrix}\right)$ sebagai tantangan kepada Alice.
6. Alice menghitung $w'' = a^m w' a^n$
$$w'' = \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{34} \left(\begin{pmatrix} 225 & 187 \\ 11 & 203 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 0 \end{pmatrix}\right) \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}\right)^{45}$$
$$= \left(\begin{pmatrix} 105 & 207 \\ 158 & 88 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}\right)$$
7. Alice mengirimkan $w'' = \left(\begin{pmatrix} 105 & 207 \\ 158 & 88 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}\right)$ sebagai respon kepada Bob.
8. Bob melakukan verifikasi
$$a^u t a^v = \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\right)^{47} \left(\begin{pmatrix} 90 & 196 \\ 187 & 235 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 5 & 0 \end{pmatrix}\right) \left(\begin{pmatrix} 132 & 97 \\ 241 & 169 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}\right)^{54}$$
$$= \left(\begin{pmatrix} 105 & 207 \\ 158 & 88 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}\right)$$
$$= w''$$

Dapat dilihat bahwa proses verifikasi berhasil, yaitu diperoleh $w'' = a^u t a^v$. Perlu disampaikan bahwa kerumitan menghitung perpangkatan matriks dan perkalian matriks pada contoh atas menjadi mudah karena bantuan program *maple* 2019.

SIMPULAN

Sifat semiprima mendasar aljabar dibangun secara hingga merupakan perumuman dari aljabar semiprima. Sifat *nondegenerate* merupakan syarat perlu dan cukup aljabar semiprima tetapi bukan syarat perlu aljabar semiprima mendasar. Sifat *nondegenerate* ini mirip dengan syarat perlu dan cukup aljabar semiprima mendasar $A = \langle X \rangle$ yaitu bahwa $xAx \neq \{0\}$ untuk sebarang $x \in X$. Sebarang aljabar prima mendasar pasti semiprima mendasar, tetapi tidak sebaliknya. Syarat perlu dan cukup aljabar semiprima mendasar adalah bahwa irisan semua ideal dasar prima merupakan ideal nol. Pembuktian kondisi ini memerlukan sifat-sifat *annihilator,* terutama bahwa *annihilator* dari suatu ideal dasar juga merupakan ideal dasar pula. Selain itu, aljabar dikatakan semiprima mendasar jika dan hanya jika setiap ideal dasar tak nol bukan merupakan ideal nilpoten. Struktur aljabar semiprima mendasar umumnya merupakan aljabar non-komutatif.

Proses protokol autentiikasi dimulai dari penentuan parameter publik oleh pihak yang ingin membutkikan kebenaran identitasnya, yaitu berupa sebuah aljabar semiprima mendasar non-komutatif beserta sebuah elemennya dan sebuah ideal mendasar semiprima. Selanjutnya, kedua belah pihak melakukan beberapa perhitungan pada proses tantangan dan menanggapainya dengan menghitung respon, selanjutnya dilakukan verifikasi atas kebenaran dari respon yang diterima. Keseluruhan perhitungan dilakukan dalam aljabar semiprima mendasar yang non-komutatif.

Berdasarkan sifat non-komutatif pada aljabar semiprima mendasar, dapat dikembangkan suatu protokol autentikasi identitas yang tingkat keamaannya diletakkan pada masalah dekomposisi. Oleh karena itu, perlu kajian lebih lanjut tentang tingkat kesulitan penyelesaian masalah dekomposisi atas aljabar semiprima mendasar. Secara teori, Pengembangan aljabar dibangun secara hingga dapat dilakukan dari sifat lain yang dikarakterisasi dari ideal dasar, seperti sifat semisederhana, primitive, dan lain sebagainya. Selain itu, aljabar ini dapat dipandang sebagai modul tak bebas, yang sifat-sifatnya dapat dikaji pula.

UCAPAN TERIMA KASIH

Kami mengucapkan terimakasih kepada LPPM UIN Sunan Kalijaga Yogyakarta yang mendanai penelitian ini melalui penelitian kluster "*Research Leader*" tahun 2021. Ucapan terima kasih ditujukan kepada para reviewer atas masukan dan koreksinya.

DAFTAR PUSTAKA

Abrams, G., Ara, P., & Molina, M. S. (2017). *Leavitt path algebras, a primer and handbook* (pp. 37–54). Springer-Verlag, London Ltd.

Anshel, I., Anshel, M., & Goldfeld, D. (1999). An algebraic method for public-key cryptography. *Mathematical Research Letters, 6*, 287-291. https://doi.org/10.4310/MRL.1999.V6.N3.A3

Pino, G. A., Barquero, D. M., González, C. M., Molina, M. S. (2008). The socle of a Leavitt path algebra, *Journal of Pure and Applied Algebra*, *212*(3), 500–509. https://doi.org/10.1016/j.jpaa.2007.06.001

Baumslag, G., Fine, B., Kreuzer, M., & Rosenbeger, G. (2015). *A Course in Mathematical Cryptography*, (pp. 128), De Gruyter.

Birkenmeier, G. F., Heider, B. J. (2019). Annihilators and extensions of idempotent-generated ideals. *Communications in Algebra*, *47*(3), 1348–1375. https://doi.org/10.1080/00927872.2018.1506462

Bland, P. E. (2011). *Ring and Their Modules*, (pp. 14–20). Walter de Gruyter GmbH & Co. KG, berlin New-York.

Gryak, J., Kahrobaei, D. (2016). The status of polycyclic group-based cryptography: a survey and open problems. *Groups Complexity Cryptology, 8*(2), 171–186. https://doi.org/10.1515/gcc-2016-0013.

Hazewinkel, M., & Gubareni, N. (2016). *Algebras, Rings and Modules, Non-commutative Algebras and Rings*, (pp. 9–35). Taylor & Francis Group, LLC CRC Press.

Horan, K., Kahrobaei, D. (2018). The hidden subgroup problem and post-quantum group-based cryptography. *Mathematical Software-ICMS 2018, 10931,* 218–226. https://doi.org/10.1007/978-3-319-96418-8_26.

Kanwar, P., Khatkar, M., Sharma, R.K. (2019). On Leavitt path algebras over commutative rings. *International Electronic Journal of Algebra, 26*(26), 191–203. https://doi.org/10.24330/ieja.587053

Klima, R., Klima, R. E., Sigmon, N., Sigmon, N. P. (2018). *Cryptology: Classical and Modern*, (pp. 328) Chapman and Hall/CRC.

Knospe, H. (2019). A Course in Cryptography, *American Mathematical Society*, 40, 565–568.

Lal, S., Chaturvedi, A. (2005). Authentication schemes using braid groups. *arXiv preprint cs/0507066*. https://doi.org/10.48550/arXiv.cs/0507066

Larki, H. (2015). Ideal structure of Leavitt path algebras with coefficients in a unital commutative ring. *Communications in Algebra, 43*(12), 5031–5058. https://doi.org/10.1080/00927872.2014.946133

Myasnikov, A., Shpilrain, V. & Ushakov, A. (2008). *Group-based Cryptography*, (pp. 37–45) Basel Switzerland: Birkhauser Verlag.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi kriptografi pengamanan data pada pesan teks, isi file dokumen, dan file dokumen menggunakan algoritma advanced encryption standard. *Jurnal Informatika Mulawarman, 10*(1), 20-31.

Ranjan, P., & Om, H. (2015). Cryptanalysis of braid groups based authentication schemes. *2015 1st International Conference on Next Generation Computing Technologies (NGCT)*. https://doi.org/10.1109/ngct.2015.7375155

Riyanto, M. Z. (2017). Protokol otentikasi berdasarkan masalah konjugasi pada grup unit atas ring Endomorfisma END (Zp x Zp2). *Jurnal Fourier*, *6*(1), 1–8. https://www.neliti.com/publications/80470/protokol-otentikasi-berdasarkan-masalah-konjugasi-pada-grup-unit-atas-ring-endom

Roman'kov, V. (2017). Cryptanalysis of a combinatorial public key cryptosystem. *Groups Complexity Cryptology*, *9*(2), 125–135. https://doi.org/10.1515/gcc-2017-0013

Sari, D. P. (2016). Berpikir matematis dengan metode induktif, deduktif, analogi, integratif dan abstrak. *Delta-Pi: Jurnal Matematika dan Pendidikan Matematika, 5*(1), 79–89. http://dx.doi.org/10.33387/dpi.v5i1.235

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithm on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1277–1283. https://doi.org/10.1137/S0097539795293172

Stickel, E. (2005). A new method for exchanging secret keys. *In Third International Conference on Information Technology and Applications (ICITA'05)*, *IEEE*, 426–430. https://doi.org/10.1109/ICITA.2005.33

Stinson, D. R. & Paterson, M. B. (2019). *Cryptography Theory and Practice*, (Ed.4) (pp. 1–13). CRC Press.

Tomforde, M. (2011). Leavitt path algebras with coefficient in a commutative ring. *Journal of Pure and Applied Algebra*, *215*(4), 471–484. https://doi.org/10.1016/j.jpaa.2010.04.031

Vasco, M. I. G. & Steinwandt, R. (2015). *Group Theoretic Cryptography*, (pp. 31-32). CRC Press.

Wardati, K. (2018). Ideal dasar prima dalam aljabar atas suatu ring komutatif. *Jurnal Fourier*, *7*(2), 79–86. https://doi.org/10.14421/fourier.2018.72.79-86

Wardati, K. (2021). The application of semiprime basic ideal in authentication scheme, dipresentasikan pada The 2nd International Conference On Natural Sciences, Mathematics, Applications, Research, and Technology (ICON-SMART). https://aip.scitation.org/apc/info/forthcoming

Wardati, K., Wijayanti, I.E., Wahyuni, S. (2014). On primeness of path algebras over a unital commutative ring. *JP Journal of Algebra, Number Theory and Applications, 34*(2), 121–138. https://digilib.uin-suka.ac.id/id/eprint/37246/

Wardati, K., Wijayanti, I. E., Wahyuni, S. (2015). On free ideals in free algebras over a commutative ring, *Journal of the Indonesian Mathematical Society*, *21*(1), 59–69. https://doi.org/10.22342/jims.21.1.170.59-69

Wisbauer, R. (2017). *Foundations of Module and Ring Theory, A handbook for Study and Research* (pp. 9–24). (E-book) Routledge.

Zed, M. (2014). *Metode Penelitian Kepustakaan,* (Ed.3) (pp. 16–23). Yayasan Pustaka Obor Indonesia.