APLIKASI *QUASIGROUP* DALAM PEMBENTUKAN KUNCI RAHASIA PADA ALGORITMA HIBRIDA (*RSA-QUASIGROUP CIPHER)*

Muhammad Khudzaifah

Jurusan Matematika, F.MIPA, Universitas Brawijaya, Malang, Indonesia
Email : m_khudzaifah@yahoo.com

ABSTRAK

Pada artikel ini dibahas penerapan quasigrup di bidang kriptografi. Didefinisikan Suatu operasi *quasigroup* order $p-1$ sehingga bisa membentuk suatu algoritma kriptografi yang disebut sebagai quasigrup cipher, quasigrup cipher merupakan algoritma kriptografi simetris. Algoritma kriptografi simetris memiliki sistem keamanan lemah karena kunci yang digunakan untuk proses *enciphering* sama dengan kunci yang digunakan untuk proses *deciphering*. Sehingga pada artikel ini algoritma *quasigroup cipher* dimodifikasi dengan menggabungkannya dengan algoritma RSA menjadi suatu algoritma hibrida yang memiki dua tingkatan kunci.

Kata kunci : quasigrup, kriptografi, algoritma hibrida.

ABSTRACT

In this article discusses application of quasigroup in the field of cryptography, a quasigroup order $p-1$ *operation is defined so that it can form a cryptographic algorithm called a cipher quasigrup, quasigrup cipher is a symmetric cryptographic algorithms, symmetric cryptographic algorithms have weak security systems which are used as the key for enciphering process same as the key used for deciphering process. So at this article quasigroup cipher algorithm is modified by combining the RSA algorithm into a hybrid algorithm that is thinking about the two key levels.*

Keywords: *quasigrup, cryptography, hybrid algorithm*

PENDAHULUAN

Kriptografi memegang peranan penting seiring dengan perkembangan teknologi informasi dan komunikasi. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data, ataupun informasi adalah enkripsi. Disini enkripsi dapat diartikan sebagai kode atau *cipher*.

Di sisi lain, beberapa teori dalam aljabar abstrak khususnya teori mengenai quasigroup telah dikembangkan secara luas mulai dari bentuk integrasinya dengan disiplin ilmu lain hingga aplikasinya dalam berbagai bidang. Banyak teori quasigroup yang telah diterapkan dalam steganografi, teori pengkodean, dan kriptografi. Penggunaan quasigroup pada kriptografi adalah quasigroup cipher, yang merupakan kriptografi kunci simetri yang keamanannya kurang baik. Hal ini dikarenakan proses dekripsinya dan enkripsinya menggunakan kunci yang sama. Oleh karena itu akan dikombinasikan dengan algoritma kunci asimetris, yang proses enkripsi dan dekripsinya menggunakan kunci yang berbeda.

Pada tahun 2004 Gligoroski mengembangkan quasigroup cipher dengan mendefinisikan quasigroup order $p-1$, dan dikombinasikan dengan algoritma Elgamal. Dalam tesis ini dibahas penggunaan quasigroup pada kriptografi yang dikombinasikan dengan algoritma RSA. Alasan pemilihan algoritma RSA ini adalah karena proses enkripsi dan dekripsi RSA lebih cepat daripada Algoritma Elgamal.

TEORI DASAR

1. Mengkontruksi Kunci Rahasia dalam Bentuk *Quasigroup Cipher*

Pada sub-bab ini akan diperkenalkan definisi dan teori *quasigroup* yang dikutip dari (Markovski, et al., 1997)

Teorema 1.1

Misalkan $(A,*)$ adalah *quasigroup* yang menetapkan sebuah operasi biner \ pada A sedemikian sehingga untuk semua $x, y \in A$ berlaku,

$$x \backslash y = z \leftrightarrow x * z = y,$$

Maka groupoid $(A,\backslash)$ adalah quasigroup.

Definisi 1.2

Operasi $\setminus$ adalah *dual* dari $*$ sehingga *quasigroup* $(A,\setminus)$ adalah *dual* dari *quasigroup* $(A,*).(A,*,\setminus)$ adalah *quasigroup* yang diperoleh dari hasil perluasan *quasigroup* $(A,*)$.

Teorema 2.3

Quasigroup $(A,*,\setminus)$ memenuhi persamaan identitas :

$x \setminus (x * y) = y, \quad x * (x \setminus y) = y$, Untuk semua $x, y \in A$.

Definisi 2.4

Misalkan $u_i \in A^+, k \in \mathbb{N}, k \geq 1$, dan $a_1 \in A$ maka,

$$f_*(u_1u_2 \dots u_k) = v_1v_2 \dots v_k \quad \Leftrightarrow \quad \begin{aligned} v_1 &= a_1 * u_1, \\ v_2 &= v_2 * u_2, \\ v_3 &= v_3 * u_3, \\ &\vdots \\ v_{i+1} &= v_i * u_{i+1}, \qquad i = 1,2, \dots, k-1, \end{aligned}$$

$$f_\setminus(u_1u_2 \dots u_k) = v_1v_2 \dots v_k \quad \Leftrightarrow \begin{aligned} v_1 &= a_1 \setminus u_1, \\ v_2 &= v_1 \setminus u_2, \\ v_3 &= v_2 \setminus u_2, \\ &\vdots \\ v_{i+1} &= v_i \setminus u_{i+1}, \quad i = 1,2, \dots, k-1. \end{aligned}$$

Sixtuple $(A,*,\setminus, a_1, f_*, f_\setminus)$ disebut quasigroup cipher atas alfabet A.

2. Mengkontruksi Kunci Rahasia dalam Bentuk *Quasigroup Cipher* menggunakan *quasigroup* atas *order p-1*

Misalkan himpunan huruf alfabet adalah himpunan berhingga Q dan dinotasikan Q^+ adalah himpunan semua kata tak kosong atau string berhingga yang terdiri atas anggota dari Q.

Anggota dari Q^+ akan dinotasikan sebagai $a_1a_2, \dots a_n$. $a_i \in Q$. Misalkan $*$ adalah operasi pada *quasigroup* pada himpunan Q dan $(Q,*)$ adalah *quasigroup*, untuk $a \in Q$ didefinisikan dua fungsi $e_a, d_a: Q^+ \longrightarrow Q^+$ sebagai berikut

Misal $a_i \in Q, \alpha = a_1a_2 \dots a_n$.
Maka

$$e_a(\alpha) = b_1b_2 \dots b_n \Leftrightarrow b_1 = a * a_1, b_2 = b_1 * a_2, \dots, b_n = b_{n-1} * a_n.$$

Sehingga $b_{i+1} = b_i * a_{i+1}$ untuk setiap $i = 0,1, \dots, n-1$, dimana $b_0 = a$, dan

$$d_a(\alpha) = c_1c_2 \dots c_n \Leftrightarrow c_1 = a * a_1, c_2 = a_1 * a_2, \dots, c_n = a_{n-1} * a_n.$$

Sehingga $c_{i+1} = a_i * a_{i+1}$ untuk setiap $i = 0,1, \dots, n-1$, dimana $a_0 = a$. Definisi dan teori quasigroup pada sub bab ini dikutip dari [1]

Definisi 2.1

Fungsi e_a dan d_a disebut sebagai e-transformasi string dan d-transformasi string dari Q^+ berdasarkan operasi $*$ dengan *leader* a.

Definisi 2.2

Jika dipilih sebanyak k *leaders* $a_1, a_2, \dots, a_k \in Q$ maka didefinisikan pemetaan fungsi komposisi

$$E_k = E_{a_1 \dots a_k} = e_{a_1} \circ e_{a_2} \circ \cdots \circ e_{a_k}$$

dan

$$D_k = D_{a_1 \dots a_k} = d_{a_1} \circ d_{a_2} \circ \cdots \circ d_{a_k}$$

disebut sebagai E- dan D- *quasigroup* transformasi string pada Q^+.

Lemma 2.3

Fungsi E_k dan D_k adalah permutasi pada Q^+.

Lemma 2.4

Pada quasigroup $(Q,*)$ dengan diberikan himpunan dari k *leaders* $\{a_1, a_2, \dots, a_k\}$ maka invers dari $E_k = E_{a_1 \dots a_k} = e_{a_1} \circ e_{a_2} \circ \cdots \circ e_{a_k}$ adalah $E_k^{-1} = D_k = D_{a_k \dots a_1} = d_{a_k} \circ \cdots \circ d_{a_1}$.

Definisi 2.5

Quasigroup $(Q,*)$ dan k-tuple $(a_1, a_2, \dots, a_k)$ dari leader $a_i \in Q$, sistem

$$((Q,*), (a_1, a_2, \dots, a_k), E_{a_1 \dots a_k}, D_{a_k \dots a_1})$$

terdefinisi sebagai *quasigroup stream cipher* atas string di Q^+.

Lemma 2.6

Untuk suatu p bilangan prima dan bilangan K yang memenuhi $1 \leq K \leq p-2$,

fungsi $f_K(j) = \frac{1}{1+(K+j) mod (p-1)} mod\ p$

adalah permutasi dari element di $\mathbb{Z}_p^*$

Lemma 2.7

Operasi biner $*$ pada himpunan $Q = \{1,2, \dots, p-1\}$ didefinisikan sebagai

$$i * j = i \times f_K(j) mod\ p$$

membentuk *quasigroup* $(Q,*)$.

Akibat 2.8

Jika didefinisikan fungsi

$$g(i,j,K) = \big((i \times j^{-1} mod\ p) - 1 - K\big)\ mod\ (p-1)$$

yang mengambil parameter i, j, K dari himpunan $Q = \{1,2, \dots, p-1\}$, yang memetakan himpunan $A = \{1,2, \dots, p-1\}^3$ ke himpunan $B = \{1,2, \dots, p-2\}$ maka pembagi kiri $(Q,\setminus)$ dari *quasigroup* $(Q,*)$

yang didefinisikan pada Lemma 3.2.7 didefinisikan sebagai

$$i \setminus j = \begin{cases} g(i,j,K), \text{jika } g(i,j,K) \neq 0 \\ p-1, \text{jika } g(i,j,K) = 0 \end{cases}$$

PEMBAHASAN

1. Mengkontruksi Algoritma Hibrida *(RSA-Quasigroup cipher)*

Ilustrasi proses *encipher* dan *decipher*

1) A membangkitkan kunci publik dan kunci privat dengan algoritma RSA yang mana kunci publik akan dikirimkan ke B.
2) B mengenkripsi pesan dengan algoritma *Quasigroup cipher*, dan mengenkripsi *session key* dari *Quasigroup cipher* dengan kunci publik yang diberikan oleh A dengan menggunakan Algoritma RSA. Pesan dan key yang telah terenkripsi dikirim ke A.
3) A mendekripsi *session key* dari B dengan menggunakan kunci privat algoritma RSA, lalu mendekripsi pesan dari B dengan menggunakan *session key* yang sudah terdekripsi dengan algoritma *Quasigroup cipher*.

2. Algoritma Hibrida (RSA-Quasigroup cipher)

Algoritma Enkripsi

1) Pilih sebarang bilangan bulat K, $1 \leq K \leq p-1$ yang mana *quasigroup* $(Q,*)$ terdefinisi untuk elemen $\{1,2,\dots,p-1\}$ dengan persamaan pada Lemma 2.7, dengan p adalah sebarang bilangan prima yang dipilih
2) Enkripsi K dengan Algoritma RSA
3) Pilih $k \geq 3$ bilangan bulat acak $a_i, i = 1,2,\dots,k, 1 \leq a_i \leq p-2$ untuk menjadi leader untuk *quasigroup cipher* dan enkripsikan dengan Algoritma RSA
4) Ubah setiap karakter pada pesan m_μ menjadi bilangan bulat pada range $\{1,2,\dots,p-1\}$, dengan μ adalah indeks setiap karakter dari pesan
5) Secara berulang hitung $m_\mu^i = a_i * m_\mu^{i-1}$, dimana $m_\mu^0 = m_\mu$, $i = 1,\dots,k$ dan $*$ adalah operasi *quasigroup* yang terdefinisi pada Lemma 2.7
6) $c_\mu = m_\mu^k$ dan update nilai leader dengan $a_i = m_\mu^i, i = 1,\dots,k-1$ dan $a_k = 1 + (\sum_{i=1}^{k} m_\mu^i \ mod\ (p-1))$.
7) Didapatkan *Session key* terenkripsi dan pesan yang terenkripsi c_μ (*ciphertext*)

Algoritma Dekripsi

1) Dekripsi *Session key* dengan Algoritma RSA, maka didapatkan K untuk membuat $(Q,\setminus)$ dan didapatkan sejumlah k leader.
2) Secara berulang hitung $c_\mu^k = a_k \setminus c_\mu$, $c_\mu^i = a_i \setminus c_\mu^{i+1}, i = k-1,\dots,1$ dan $\setminus$ adalah operasi $quasigroup$ yang terdefinisi pada Akibat 2.8
3) $m_\mu = c_\mu^1$ dan update nilai leader dengan $a_i = c_\mu^{i+1}, i = 1,\dots,k-1$ dan $a_k = 1 + (c_\mu + \sum_{i=2}^{k} c_\mu^i \ mod\ (p-1))$.
4) Didapatkan *plaintext* m_μ

KESIMPULAN

Algoritma kriptografi yang didasarkan dari quasigroup yaitu quasigroup cipher memiliki keamanan cukup baik, hal ini dibuktikan pada contoh ketika kriptanalis salah mendekripsi satu huruf saja maka pesan tidak bisa terbaca.

Kelemahan algoritma quasigroup adalah karena kuncinya adalah kunci simetris, sehingga bila kuncinya bocor kepada orang lain, maka pesan bisa dibaca orang lain. Sehingga diperkuat dengan algoritma RSA yang memiliki kunci asimetris menjadi algoritma hibrida yang tingkat keamanannya lebih tinggi karena memiliki 2 tingkatan kunci.

BIBLIOGRAPHY

[1] D. Gligoroski, "Stream Cipher Based on Quasigroup String Transformation in Zp*.," Faculty of Natural Sciences institute of Informatics, Skopje, 2004.

[2] D. Ariyus, Pengantar Ilmu Kriptografi, Yogyakarta: Andi Press, 2008.

[3] M. A. Al-Turky, "On the number and Equivalent Latin Squares," *Journal of Al-Anbar University for pure Science,* pp. 71-75, 2007.

[4] P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul, Basic Abstrack Algebra, New York: Cambridge University Press, 1990.

[5] J. Bell, "An Introduction to SDR's and Latin Squares," *More-head Electonic Journal of Applicable Mathematics,* pp. 1-8, 2005.

[6] Koscielny, "Generating Quasigroups for Cryptograpic Applications," *International*

Journal of Applied Mathematic and Computer Science, pp. 559-569, 2002.

[7] E. Ochodkova. and V. Snasel, "Using Quasigroups for Secure Encoding of File Sistem," in *Proceedings of The Confrence for Security and Protection of Information*, 2001.

[8] S. Markovski, D. Glikoroski and S. Andonova., "Using Quasigroups for One-one Secure Encoding," in *Proceeding of VII-th Confrence for Logic and Computing-LIRA'97*, 1997.