Konstruksi Suatu Algoritma Kriptografi Menggunakan Transformasi Max Plus Wavelet

Joko Cahyono, Subiono

Jurusan Matematika
Institut Teknologi Sepuluh Nopember
j0k0_cahy0n0@yahoo.com
subiono2008@matematika.its.ac.id

Abstrak

Kriptografi berperan menjaga keamanan suatu informasi. Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi. Dalam tesis ini dikontruksi suatu algoritma kriptografi berdasarkan transformasi max plus wavelet. Enkripsi disusun berdasarkan proses analisis dari transformasi max plus wavelet, sedangkan dekripsi disusun berdasarkan proses sintesis. Kunci kriptografi terdiri dari tiga bagian yaitu kode untuk tipe max plus wavelet yang digunakan, banyak kanal yang digunakan dan kode untuk sinyal detail. Proses kriptografi ini hanya melibatkan operasi maksimum dan tambah sebagai operasi utama. Berdasarkan hasil uji coba dan analisis didapat bahwa algoritma kriptografi ini adalah baik berdasarkan korelasi antara *plaintext* dan *ciphertext* serta kualitas enkripsinya. Algoritma ini juga efisien dari segi waktu karena memiliki kompleksitas O(n) atau kompleksitas linier.

Kata Kunci: Kriptografi, Kunci, Transformasi Max Plus Wavelet.

1 Pendahuluan

Kriptografi adalah salah satu alat yang berperan dalam menjaga keamanan suatu informasi. Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi. Goswami dkk dalam penelitiannya [5] mengusulkan penggunaan transformasi wavelet diskrit Daubechies dalam kriptografi, yaitu untuk proses enkripsi, dekripsi dan penyusunan kunci. Grigoriev dan Shpilrain [6], serta Durcheva [3] dalam penelitiannya membahas tentang penggunaan aljabar max plus dan aljabar min plus dalam kriptografi, yaitu untuk penyusunan kunci. Fahim dalam tesisnya [4] membahas tentang transformasi max plus wavelet, yaitu transformasi wavelet menggunakan aljabar max plus. Kelebihan dari transformasi max plus wavelet ini adalah tidak melibatkan *floating point* sehingga menjadi lebih sederhana dan efisien.

Berdasarkan uraian tersebut, pada tesis ini dibahas mengenai konstruksi suatu algoritma kriptografi menggunakan transformasi max plus wavelet. Transformasi max plus wavelet ini digunakan untuk proses enkripsi, dekripsi dan penyusunan kunci. Untuk implementasi dari algoritma kriptografi ini dibuat suatu program kriptografi menggunakan software Scilab 5.5.2. Data yang dienkripsi berupa teks yang disimpan dalam file dengan format txt. Selanjutnya dianalisis kelayakan dari algoritma kriptografi max plus wavelet yang dihasilkan. Analisis dilakukan dengan cara menentukan korelasi linier antara *plaintext* dan *ciphertext*, kualitas enkripsi, *running time* program dan analisis kompleksitas algoritma. Pada tesis ini tidak dibahas masalah keamanan dari algoritma kriptografi yang dikonstruksi.

2 Konstruksi Algoritma Kriptografi

2.1 Transformasi Max Plus Wavelet

Transformasi wavelet sangat berperan dalam proses pengolahan sinyal. Pada sinyal utama yang beresolusi tinggi dilakukan operasi analisis sehingga didapatkan sinyal hampiran dan sinyal detail. Sinyal hampiran mampu merepresentasikan sinyal utama namun memiliki resolusi yang lebih rendah. Sinyal detail menjamin bahwa sinyal utama dapat diperoleh kembali dengan proses sintesis.

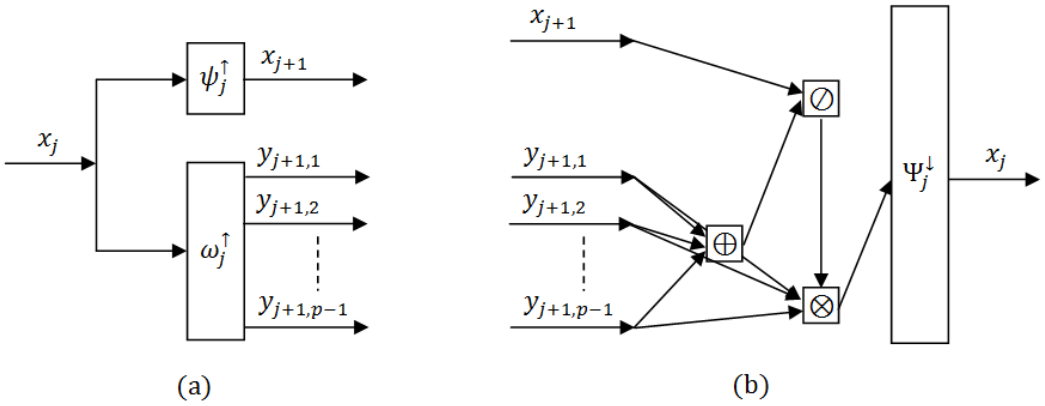
Transformasi wavelet dapat dibagi menjadi transformasi wavelet diskrit dan transformasi wavelet kontinu. Transformasi wavelet Haar adalah bentuk transformasi wavelet diskrit yang paling sederhana [2]. Berdasarkan transformasi wavelet Haar ini, Fahim [4] mengkontruksi transformasi wavelet menggunakan aljabar max plus. Aljabar max plus adalah struktur aljabar yang mempunyai dua operator yaitu maksimum dan tambah [9]. Transformasi max plus wavelet yang dikontruksi adalah tipe A, tipe B, tipe C, tipe D dan tipe E.

Pada transformasi max plus wavelet tipe A terdapat operator analisis ($\psi_j^{\uparrow}$ dan $\omega_j^{\uparrow}$) dan operator sintesis $\Psi_j^{\downarrow}$. Skema operator analisis dan operator sintesis dapat dilihat pada Gambar 1 [4].

Pada operator analisis terlihat bahwa output terdiri dari satu sinyal hampiran dan $p-1$ sinyal detail. Berdasarkan hal tersebut disusun operator analisis sebagai berikut:

$$\psi_j^{\uparrow}(x_j)[n] = \bigoplus_{k=0}^{p-1} x_j[pn+k] = x_{j+1}[n] \tag{1}$$

$$\begin{aligned} \omega_j^{\uparrow}(x_j)[n] &= y_{j+1}[n] \\ &= (y_{j+1,1}[n], y_{j+1,2}[n], ..., y_{j+1,p-1}[n]) \\ &= (\omega_{j,1}^{\uparrow}(x_j)[n], \omega_{j,2}^{\uparrow}(x_j)[n], ..., \omega_{j,p-1}^{\uparrow}(x_j)[n]) \end{aligned} \tag{2}$$



Gambar 1: Skema Transformasi MP-Wavelet Tipe A dengan p Kanal (a) Operator Analisis (b) Operator Sintesis

dengan

$$\omega_{j,r}^{\uparrow}(x_j)[n] = x_j[pn+r] \oslash x_j[pn] = y_{j+1,r}[n].$$

Pada operator sintesis terlihat bahwa input terdiri dari satu sinyal hampiran dan $p-1$ sinyal detail. Berdasarkan hal tersebut disusun operator sintesis sebagai berikut:

$$\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] = x_{j+1}[n] \oslash [(\bigoplus_{k=1}^{p-1} y_{j+1,k}[n]) \oplus 0] \quad (3)$$

$$\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn+r] = \Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] \otimes y_{j+1,r}[n], \quad (4)$$
dengan $r = 1, 2, ..., p-1$.

Skema dan operator transformasi max plus wavelet secara lengkap terdapat di [4].

2.2 Konstruksi Algoritma Kriptografi Max Plus Wavelet

2.2.1 Proses Enkripsi

Langkah-langkah enkripsi dilakukan sebagai berikut:

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.
3. **PlainASCII** kemudian dimasukkan ke dalam proses analisis. Dari proses analisis didapatkan sinyal hampiran, sinyal detail dan kunci bagian ketiga yaitu kode sinyal detail yang dihasilkan.

4. Dapatkan **CipherASCII** yaitu kode ASCII dari ciphertext, yang dihasilkan dengan cara sebagai berikut.

   - Untuk max plus wavelet tipe A, C, D dan E:
     CipherASCII terdiri dari sinyal hampiran dan nilai absolut sinyal detail + 32.
   - Untuk max plus wavelet tipe B:
     Pada sinyal detail terlebih dahulu dilakukan operasi

     $$S_b = ((|S_d| \text{ - } 32) \bmod 95) + 32$$

     dimana S_b adalah sinyal detail baru dan S_d adalah sinyal detail lama. Kemudian sinyal hampiran dan sinyal detail baru akan menjadi **CipherASCII**.

5. **CipherASCII** diubah menjadi text dan disimpan dalam variable **Ciphertext**.

Selanjutnya Ciphertext dan kunci kriptografi akan dikirimkan kepada penerima pesan. Algoritma proses analisis disusun berdasarkan operator analisis pada transformasi max plus wavelet yang dikonstruksi oleh Fahim [4].

2.2.2 Penyusunan Kunci

Kunci kriptografi terdiri dari tiga bagian. Kunci bagian pertama adalah kode transformasi max plus wavelet yang digunakan. Kunci bagian kedua adalah besarnya kanal yang digunakan. Kunci bagian ketiga adalah kode sinyal detail yang didapatkan dengan langkah-langkah berikut:

1.
   - Untuk max plus wavelet tipe A, C, D dan E: Sinyal detail yang bernilai negatif diberi kode 1 dan yang bertanda positif diberi kode 0.
   - Untuk max plus wavelet tipe B: Sinyal detail terlebih dahulu dimutlakkan dan dikurangi 32. Kemudian sinyal yang bernilai lebih dari atau sama dengan 95 diberi kode 1 dan yang bernilai kurang dari 95 diberi kode 0.

2. Setiap 8 angka dari kode sinyal detail ini akan dibaca menjadi sebuah kode biner suatu bilangan. Begitu juga dengan angka sisanya.

3. Kode biner bilangan ini kemudian diubah menjadi bilangan desimal dan akan menjadi kunci bagian ketiga.

2.2.3 Proses Dekripsi

Langkah-langkah dekripsi dilakukan sebagai berikut:

1. Ciphertext diubah menjadi kode ASCII dan disimpan dalam array **CipherASCII**.
2. Masukkan kunci dekripsi (kunci kriptografi).
3. Kunci kriptografi dipisah menjadi tiga bagian.
4. Kunci bagian ketiga diubah menjadi kode biner.
5. Angka pertama dari **CipherASCII** akan menjadi sinyal hampiran. Sedangkan sisa **CipherASCII** bersama dengan kode biner akan digunakan untuk mendapatkan sinyal detail dengan rumus sebagai berikut:
   - Untuk max plus wavelet tipe A, C, D dan E:
     Sinyal detail = CipherASCII $\times(-1)^{\text{kode biner}}$
   - Untuk max plus wavelet tipe B:
     Sinyal detail = -(CipherASCII + 95 $\times$ kode biner)
6. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
7. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
8. **PlainASCII** diubah menjadi pesan awal.

Algoritma proses sintesis disusun berdasarkan operator sintesis pada transformasi max plus wavelet yang dikonstruksi oleh Fahim [4].

3 Analisis Kelayakan Algoritma Kriptografi

Algoritma kriptografi max plus wavelet ini diimplementasikan dalam suatu program kriptografi yang disusun menggunakan software Scilab 5.5.2. Input program adalah teks atau file dengan format .txt. Output program adalah teks yang dapat disimpan dalam file dengan format .txt. Uji coba program dilakukan pada komputer dengan prosesor Pentium Dual Core 2,2 GHz dan memory 1 GB. Secara keseluruhan uji coba dilakukan menggunakan delapan file input yang berisi pesan awal (*plaintext*) dengan panjang karakter yang berbeda-beda. Berdasarkan hasil dari uji coba ini kemudian dilakukan analisis kelayakan algoritma.

Analisis kelayakan algoritma ini bertujuan untuk mengetahui kualitas dan performa algoritma kriptografi yang dikonstruksi. Untuk mengetahui kualitas algoritma kriptografi dilakukan penghitungan nilai korelasi antara *plaintext*

dan *ciphertext* serta penghitungan nilai kualitas enkripsi. Untuk mengetahui performa algoritma kriptografi dilakukan penghitungan *running time* serta analisis kompleksitas algoritma.

Untuk mengetahui perbedaan antara kelima tipe max plus wavelet, maka data yang digunakan untuk analisis korelasi, kualitas enkripsi dan *running time* berikut ini merupakan hasil uji coba program dengan menggunakan kunci kanal yang sama untuk semua tipe max plus wavelet.

3.1 Korelasi *plaintext* dan *ciphertext*

Penghitungan korelasi *plaintext* dan *ciphertext* bertujuan untuk mengetahui hubungan linier antara *plaintext* dan *ciphertext*. Jika *plaintext* dan *ciphertext* cenderung mengikuti garis lurus dengan kemiringan yang sama, maka ada korelasi positif yang tinggi antara keduanya. Akan tetapi jika keduanya mengikuti garis lurus dengan arah kemiringan yang berlawanan, maka terdapat nilai korelasi yang negatif. Jika korelasi bernilai 1 atau -1 maka *ciphertext* mempunyai hubungan linier yang kuat dengan *plaintext*. Di dalam kriptografi hal ini merupakan enkripsi yang tidak baik. Jika korelasi bernilai 0 maka *plaintext* dan *ciphertext* tidak mempunyai hubungan linier. Hal ini menunjukkan bahwa algoritma tersebut mempunyai proses enkripsi yang baik.

Penghitungan nilai korelasi dilakukan dengan menggunakan rumus [1]:

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{(n\sum(x^2) - (\sum x)^2)(n\sum(y^2) - (\sum y)^2)}} \tag{5}$$

dimana x adalah kode ASCII *plaintext*, y adalah kode ASCII *ciphertext* dan n adalah panjang *plaintext*.

Tabel 1: Korelasi *plaintext* dan *ciphertext*

Nama File	Nilai Korelasi				
	Tipe A	Tipe B	Tipe C	Tipe D	Tipe E
uji 1.txt	0.1251757	0.471351	0.2503786	0.0664618	0.1080021
uji 2.txt	-0.0353653	-0.0339805	-0.1235486	-0.6244079	-0.1520281
uji 3.txt	0.1050945	0.2148343	0.0885354	0.0472774	0.0672378
uji 4.txt	0.01741	0.1450937	0.1141744	0.08814	-0.0558546
uji 5.txt	0.006129	0.0661493	-0.0061864	0.0328503	0.0344253
uji 6.txt	-0.0205778	0.0261839	0.0048731	0.0009255	-0.0061328
uji 7.txt	0.0181245	0.0235925	0.0196891	0.0283679	0.0338908
uji 8.txt	-0.0137571	0.0103303	-0.0119865	0.0026814	0.0063104

Dari Tabel 1 terlihat bahwa nilai korelasi sebagian besar berada pada selang -0.2 sampai 0.2. Hanya ada empat data yang berada diluar selang tersebut. Nilai mutlak korelasi dibawah 0.2 menunjukkan bahwa hampir tidak ada korelasi linier antara *plaintext* dan *ciphertext*. Data tersebut menunjukkan semua tipe max plus wavelet mempunyai nilai korelasi yang kecil. Tidak ada tipe max plus wavelet yang selalu lebih baik daripada tipe yang lain. Tanda negatif pada tabel tersebut hanya menunjukkan bahwa arah kemiringan *ciphertext* berlawanan dengan kemiringan *plaintext*. Sedangkan tanda positif menunjukkan bahwa arah kemiringan *ciphertext* sama dengan kemiringan *plaintext*. Sebagai contoh korelasi 0.3 dan -0.3 mempunyai kekuatan korelasi yang sama, perbedaannya hanya ada pada arah kemiringan *ciphertext*.

3.2 Kualitas Enkripsi

Penghitungan kualitas enkripsi dilakukan dengan membandingkan frekuensi kemunculan setiap karakter di *plaintext* dan *ciphertext*. Kualitas enkripsi merepresentasikan rata-rata selisih frekuensi kemunculan setiap karakter di *plaintext* dan *ciphertext*. Proses enkripsi yang lebih baik adalah proses yang memiliki nilai kualitas enkripsi yang lebih tinggi. Penghitungan nilai kualitas enkripsi dilakukan dengan menggunakan rumus [1]:

$$EQ = \frac{\sum_{L=32}^{126} |H_L(C) - H_L(P)|}{95} \tag{6}$$

dimana $H_L(C)$ adalah frekuensi kemunculan karakter dengan kode ASCII L di *ciphertext* dan $H_L(P)$ adalah frekuensi kemunculan karakter dengan kode ASCII L di *plaintext*.

Tabel 2: Kualitas Enkripsi

Nama File	Kualitas Enkripsi				
	Tipe A	Tipe B	Tipe C	Tipe D	Tipe E
uji 1.txt	0.5473684	0.4842105	0.5578947	0.5578947	0.4631579
uji 2.txt	1.6	1.1578947	1.7368421	1.7368421	1.4736842
uji 3.txt	4.6315789	3.0526316	5.0631579	5.0631579	5.0947368
uji 4.txt	8.3368421	7.8315789	8.6105263	8.6105263	8.7789474
uji 5.txt	14.505263	9.6631579	16.189474	16.189474	15.726316
uji 6.txt	42.736842	37.431579	41.863158	41.863158	43.136842
uji 7.txt	86.315789	56.947368	95.631579	95.631579	90.863158
uji 8.txt	146.10526	103.23158	163.46316	163.46316	155.54737

Dari tabel tersebut terlihat bahwa semakin banyak *plaintext* maka nilai kualitas enkripsi juga semakin besar. Nilai kualitas enkripsi maksimal muncul

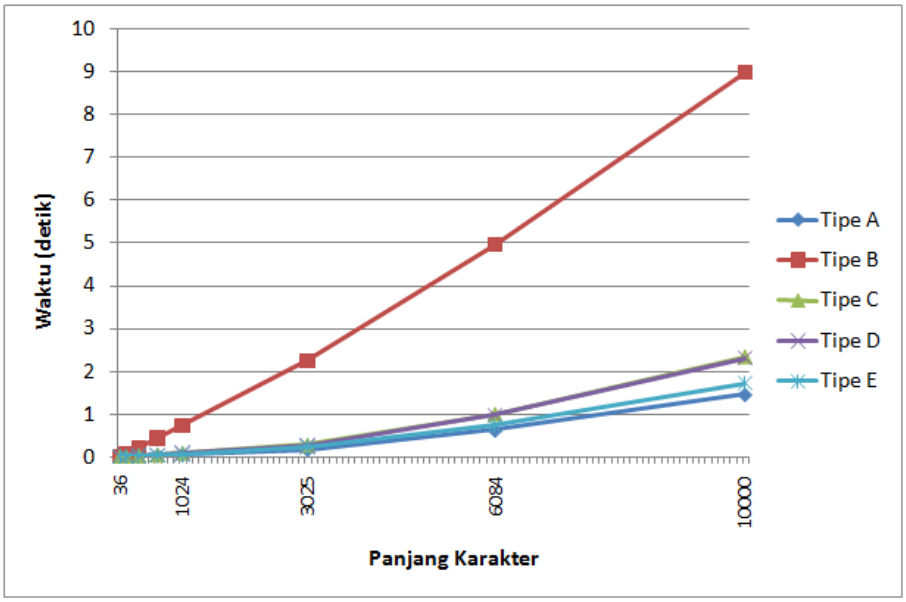
jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*. Untuk algoritma kriptografi ini nilai kualitas enkripsi maksiml dapat dihitung dengan rumus 2n/95, dimana n adalah panjang *plaintext*.

Dengan rumus ini dapat diketahui bahwa nilai kualitas enkripsi maksimal dari uji 1 adalah 0.757894737, uji 2 adalah 2.105263158, uji 3 adalah 6.821052632, uji 4 adalah 13.15789474, uji 5 adalah 21.55789474, uji 6 adalah 63.68421053, uji 7 adalah 128.0842105 dan uji 8 adalah 210.5263158. Dari Tabel 2 dapat diketahui bahwa rata-rata kualitas enkripsi dari setiap uji coba bernilai 67% dari nilai kualitas enkripsi maksimal.

Nilai kualitas enkripsi dari max plus wavelet tipe B adalah yang paling kecil dibandingkan dengan tipe yang lain. Dari data tersebut dapat diambil kesimpulan bahwa berdasarkan nilai kualitas enkripsi, max plus wavelet tipe C dan D adalah yang terbaik.

3.3 *Running Time* Enkripsi

Penghitungan waktu enkripsi dimulai dari proses mengubah *plaintext* menjadi kode ASCII, proses analisis, proses penyusunan kunci hingga proses mendapatkan *ciphertext*. Beberapa data *running time* enkripsi disajikan dalam bentuk grafik pada Gambar 2.



Gambar 2: *Running Time* Enkripsi

Pada Gambar 2 terlihat bahwa *running time* enkripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext*. Nilai taksiran

gradien garis dapat dihitung dengan menggunakan rumus regresi [10]:

$$b = \frac{n\sum xy - \sum x \sum y}{n\sum x^2 - (\sum x)^2}$$

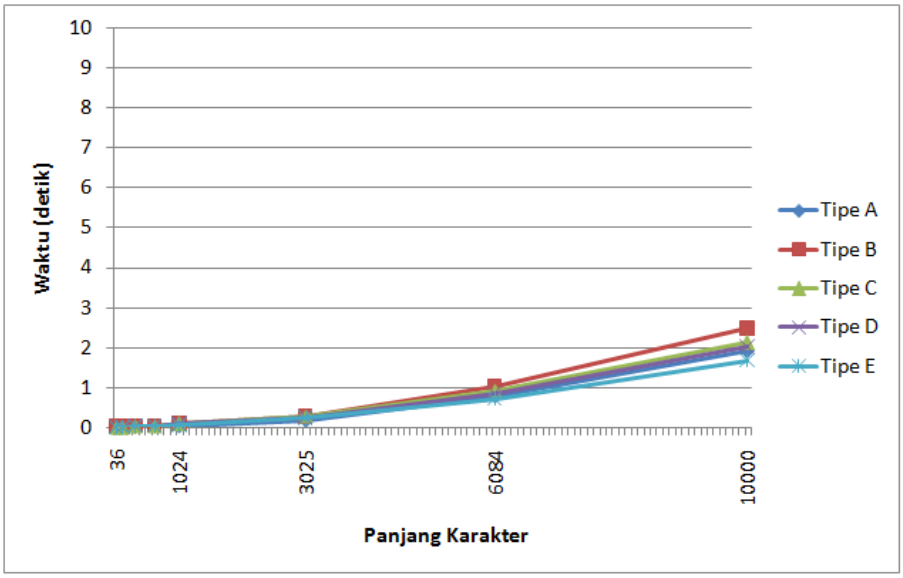
dimana x adalah panjang karakter, y adalah *running time* dan n adalah banyak data.

Nilai taksiran untuk gradien max plus wavelet tipe A adalah 0.000139073. Hal ini berarti setiap penambahan 1000 karakter, maka waktu enkripsi akan bertambah sebesar 0.139073 detik. Nilai taksiran untuk gradien tipe B adalah 0.000883765, tipe C adalah 0.00022221, tipe D adalah 0.000219091, dan gradien tipe E memiliki nilai taksiran 0.000162504.

Dari data ini terlihat bahwa max plus wavelet tipe A adalah tipe yang paling cepat. Sedangkan max plus wavelet tipe B adalah yang paling lambat dibandingkan dengan tipe yang lain dengan selisih lebih dari 0.6 detik tiap 1000 karakter.

3.4 *Running Time* Dekripsi

Penghitungan waktu dekripsi dimulai dari proses mengubah *ciphertext* menjadi kode ASCII, proses mengubah kunci menjadi kode biner, proses sintesis dan proses mendapatkan *plaintext*. Beberapa data *running time* dekripsi dari hasil uji coba disajikan dalam bentuk grafik pada Gambar 3.



Gambar 3: *Running Time* Dekripsi

Pada Gambar 3 terlihat bahwa *running time* dekripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *ciphertext*. Jika dihitung dengan menggunakan rumus regresi, nilai taksiran untuk gradien max plus wavelet tipe A adalah 0.000180097. Hal ini berarti setiap penambahan 1000 karakter, maka waktu dekripsi akan bertambah sebesar 0.180097 detik.

Nilai taksiran untuk gradien tipe B adalah 0.000235158, tipe C adalah 0.000201743, tipe D adalah 0.000190549 dan tipe E adalah 0.00015947. Dari data ini terlihat bahwa max plus wavelet tipe E adalah tipe yang paling cepat. Sedangkan tipe B adalah yang paling lambat, tetapi dengan selisih yang kecil yaitu kurang dari 0.08 detik tiap 1000 karakter.

3.5 Pengaruh Kunci Kanal

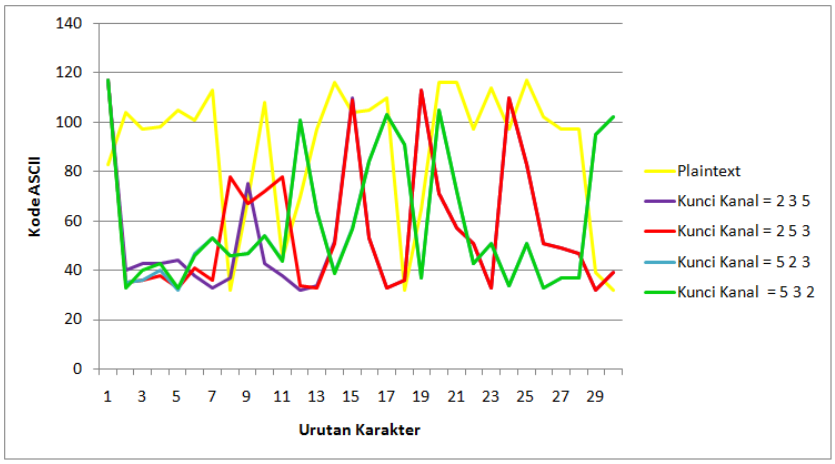
Untuk mengetahui pengaruh kunci kanal terhadap hasil enkripsi, dilakukan uji coba menggunakan file yang sama dan tipe max plus wavelet yang sama. Sedangkan kunci kanal yang digunakan berbeda. Sebagai contoh dilakukan uji coba menggunakan file uji 1.txt dengan max plus wavelet tipe A. Kunci kanal yang digunakan adalah 2 3 5, 2 5 3, 5 2 3 dan 5 3 2. Data hasil uji coba tersebut disajikan pada Tabel 3, sedangkan perbedaan antara *plaintext* dan *ciphertext* disajikan pada Gambar 4.

Tabel 3: Hasil Uji Coba Kunci Kanal

Kunci Kanal	Korelasi	Kualitas Enkripsi	Waktu Enkripsi	Waktu Dekripsi
2 3 5	0.1265434	0.4842105	0.016	0.016
2 5 3	-0.0493494	0.5052632	0.016	0.016
5 2 3	-0.2631666	0.5052632	0.016	0.016
5 3 2	-0.263015	0.5263158	0.016	0.016

Dari Tabel 3 diketahui bahwa nilai mutlak korelasi kurang dari 0.3. Perbedaan kualitas enkripsi tidak begitu besar dan *running time* menggunakan empat kunci tersebut adalah sama.

Dari Gambar 4 terlihat bahwa hasil enkripsi menggunakan kunci 2 3 5 hampir sama dengan hasil enkripsi menggunakan kunci 2 3 5. Begitu juga hasil enkripsi menggunakan kunci 5 2 3 hampir sama dengan hasil enkripsi menggunakan kunci 5 3 2. Perbedaan hanya terjadi di awal *ciphertext*. Hal ini disebabkan kunci kanal yang pertama adalah sama.



Gambar 4: Perbedaan Karakter Plaintext dan Ciphertext

3.6 Kompleksitas Algoritma

Kompleksitas algoritma dapat dianalisa menggunakan banyaknya kerja yang dilakukan oleh algoritma. Proses yang akan dianalisa banyak kerjanya yaitu proses enkripsi yang terdiri dari proses analisis, penyusunan kunci dan pembentukan *ciphertext*, serta proses dekripsi yang terdiri dari proses sintesis dan penyusunan sinyal detail.

Proses Analisis Max Plus Wavelet Tipe A

Pada tipe A ini terlihat bahwa pada operasi analisis untuk setiap p kanal terdiri dari $p-1$ perbandingan dan $p-1$ pengurangan. Jika pada enkripsi terdapat kunci kanal $p_1, p_2, \ldots p_k$, maka banyaknya kerja yang dilakukan adalah:

$$\begin{aligned} W_1 &= \frac{n}{p_1}(p_1-1)(C+S) \\ W_2 &= \frac{n}{p_1 p_2}(p_2-1)(C+S) \\ &\vdots \\ W_k &= \frac{n}{p_1 p_2 \ldots p_k}(p_k-1)(C+S). \end{aligned}$$

Sehingga kerja keseluruhan

$$\begin{aligned} W &= W_1 + W_2 \ldots W_k \\ &= \frac{n}{p_1}(p_1-1)(C+S) + \frac{n}{p_1 p_2}(p_2-1)(C+S) + \ldots \\ &\quad + \frac{n}{p_1 p_2 \ldots p_k}(p_k-1)(C+S). \end{aligned}$$

karena $p_1 - 1 < p_1, p_2 - 1 < p_2 \ldots p_k - 1 < p_k$, dan jika penulisan $(C + S)$ dihilangkan maka

$$\begin{aligned} W &< \frac{n}{p_1}(p_1) + \frac{n}{p_1 p_2}(p_2) + \ldots + \frac{n}{p_1 p_2 \ldots p_k}(p_k) \\ W &< n + \frac{n}{p_1} + \ldots + \frac{n}{p_1 p_2 \ldots p_{k-1}} \\ &< n + n + \ldots + n \\ &= kn. \end{aligned}$$

Terlihat bahwa $W < kn$, dengan demikian maka dapat dikatakan bahwa kompleksitas W = O(n) atau kompleksitas linier. Kompleksitas dari operasi analisis max plus wavelet tipe B, C, D dan E dapat dicari dengan cara yang sama, dan didapatkan bahwa kompleksitas dari operasi analisis tersebut adalah O(n).

Proses Sintesis Max Plus Wavelet Tipe A

Pada tipe A ini terlihat bahwa pada operasi sintesis untuk setiap p kanal terdiri dari $p-1$ perbandingan dan p penjumlahan. Jika pada dekripsi terdapat kunci kanal $p_1, p_2, \ldots p_k$, maka banyaknya kerja yang dilakukan adalah:

$$\begin{aligned} W_1 &= \frac{n}{p_1}((p_1 - 1)C + p_1 S) \\ W_2 &= \frac{n}{p_1 p_2}((p_2 - 1)C + p_2 S) \\ &\vdots \\ W_k &= \frac{n}{p_1 p_2 \ldots p_k}((p_k - 1)C + p_k S). \end{aligned}$$

Sehingga kerja keseluruhan

$$\begin{aligned} W &= W_1 + W_2 \ldots W_k \\ W &= \frac{n}{p_1}((p_1 - 1)C + p_1 S) + \frac{n}{p_1 p_2}((p_2 - 1)C + p_2 S) + \ldots \\ &\quad + \frac{n}{p_1 p_2 \ldots p_k}((p_k - 1)C + p_k S). \end{aligned}$$

karena $(p_1 - 1)C + p_1 S < p_1(C + S), (p_2 - 1)C + p_2 S < p_2(C + S) \ldots (p_k - 1)C + p_k S < p_k(C + S)$, dan jika penulisan $(C + S)$ dihilangkan maka

$$\begin{aligned} W &< \frac{n}{p_1}(p_1) + \frac{n}{p_1 p_2}(p_2) + \ldots + \frac{n}{p_1 p_2 \ldots p_k}(p_k) \\ W &< n + \frac{n}{p_1} + \ldots + \frac{n}{p_1 p_2 \ldots p_{k-1}} \\ &< n + n + \ldots + n \\ &= kn. \end{aligned}$$

Terlihat bahwa $W < kn$, dengan demikian maka dapat dikatakan bahwa kompleksitas W = O(n) atau kompleksitas linier. Kompleksitas dari operasi sintesis max plus wavelet tipe B, C, D dan E dapat dicari dengan cara yang sama, dan didapatkan bahwa kompleksitas dari operasi sintesis tersebut adalah O(n).

Proses Penyusunan Kode Sinyal Detail dan *Ciphertext*

Proses penyusunan kode sinyal detail dan *ciphertext* pada max plus wavelet tipe A, C, D dan E dituliskan dalam bentuk pseudocode sebagai berikut:

```
for i=1:length(Y)
     if Y(i)<0 then
          Sinyal = 1
     else
          Sinyal = 0
     end if
     ChiperASCII(i+1)= abs(Y(i))+32
end for
ChiperASCII(1)= X(1)
```

Variabel Y adalah sinyal detail yang dihasilkan dari proses analisis dengan panjang n-1. Operasi yang terdapat pada proses ini adalah operasi perbandingan, penjumlahan dan fungsi absolut. Dari pseudocode diatas terlihat bahwa setiap operasi tersebut dilakukan sebanyak $n - 1$. Karena $n - 1 < n$ maka dapat dikatakan bahwa kompleksitasnya adalah O(n) atau kompleksitas linier.

Proses penyusunan kode sinyal detail dan *ciphertext* pada max plus wavelet tipe B dituliskan dalam bentuk pseudocode sebagai berikut:

```
for i=1:length(Y)
     Y(i) = abs(Y(i))-32
     if Y(i)>94 then
          Sinyal = 1
     else
          Sinyal = 0
     end if
     ChiperASCII(i+1)= Y(i) mod 95 + 32
end for
ChiperASCII(1)= X(1)
```

Variabel Y adalah sinyal detail dengan panjang n-1. Operasi yang terdapat pada proses ini adalah operasi perbandingan, penjumlahan, pengurangan, fungsi absolut dan fungsi modulo. Dari pseudocode diatas terlihat bahwa setiap operasi tersebut dilakukan sebanyak $n-1$. Karena $n-1 < n$ maka dapat dikatakan kompleksitasnya adalah O(n) atau kompleksitas linier.

Proses Penyusunan Sinyal Detail

Proses penyusunan sinyal detail ini dilakukan sebelum melakukan proses sintesis. Proses penyusunan sinyal detail pada max plus wavelet tipe A, C, D dan E dituliskan dalam bentuk pseudocode sebagai berikut:

```
for i=2:n
    Y(i-1)=(ChiperASCII(i)-32)×(−1)^s
end for
```

Operasi yang terdapat pada proses ini adalah operasi pengurangan, perkalian dan perpangkatan. Dari pseudocode diatas terlihat bahwa setiap operasi tersebut dilakukan sebanyak $n-1$. Karena $n-1 < n$ maka dapat dikatakan kompleksitasnya adalah O(n) atau kompleksitas linier.

Proses penyusunan sinyal detail pada max plus wavelet tipe B dituliskan dalam bentuk pseudocode sebagai berikut:

```
for i=2:n
    Y(i-1)=(ChiperASCII(i)+95× s)×(-1)
end for
```

Operasi yang terdapat pada proses ini adalah operasi penjumlahan dan perkalian. Dari pseudocode diatas terlihat bahwa operasi penjumlahan dilakukan sebanyak $n-1$ dan operasi perkalian dilakukan sebanyak $2(n-1)$. Karena $n-1 < n$ dan $2(n-1) < 2n$ maka dapat dikatakan kompleksitasnya adalah O(n) atau kompleksitas linier.

Dari analisis kompleksitas diatas terlihat bahwa kompleksitas waktu untuk proses enkripsi dan dekripsi adalah O(n) atau kompleksitas linier. Hasil ini sesuai dengan hasil yang didapatkan pada penghitungan *running time* seperti yang disajikan pada Gambar 2 dan Gambar 3. *Running time* dari proses analisis menggunakan max plus wavelet tipe B terlihat jauh lebih lambat daripada tipe yang lain. Berdasarkan analisis kompleksitas diatas, hal ini terjadi karena proses penyusunan kunci dan *ciphertext* pada max plus wavelet tipe B menggunakan lebih banyak operasi daripada tipe yang lain.

4 Kesimpulan

Dari konstruksi dan analisis algoritma kriptografi max plus wavelet yang sudah dilakukan, dapat diambil kesimpulan serta diberikan saran untuk perbaikan dan pengembangan penelitian selanjutnya.

1. Pada tesis ini berhasil dikonstruksi algoritma kriptografi berdasarkan transformasi max plus wavelet. Algoritma ini termasuk dalam algoritma kriptografi *stream cipher*. Proses enkripsi didasarkan pada proses analisis, sedangkan proses dekripsi didasarkan pada proses sintesis. Kunci

enkripsi terdiri dari dua bagian yaitu kode untuk tipe max plus wavelet dan kanal yang digunakan. Dari proses analisis didapatkan *ciphertext* dan kode sinyal detail. Kunci dekripsi terdiri dari kunci enkripsi ditambah dengan kode sinyal detail.

2. Berdasarkan analisis hasil uji coba diketahui bahwa algoritma kriptografi yang dikonstruksi ini mempunyai nilai korelasi *plaintext* dan *ciphertext* yang kecil, artinya hampir tidak ada hubungan linier antara *plaintext* dan *ciphertext*. Hal ini menunjukkan bahwa algoritma ini mempunyai enkripsi yang baik. Semua tipe max plus wavelet mempunyai nilai korelasi yang kecil. Tidak ada tipe max plus wavelet yang selalu lebih baik daripada tipe yang lain.

3. Dari penghitungan kualitas enkripsi diketahui bahwa rata-rata nilai kualitas enkripsi dari algoritma ini adalah 67% dari nilai kualitas enkripsi maksimal. Nilai kualitas enkripsi dari max plus wavelet tipe C dan tipe D adalah yang terbaik dibandingkan dengan tipe yang lain.

4. Dari penghitungan *running time* diketahui bahwa *running time* enkripsi dan dekripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext* atau *ciphertext*. Untuk proses enkripsi, max plus wavelet tipe A mempunyai *running time* yang paling cepat, sedangkan tipe B adalah yang paling lambat. Untuk proses dekripsi, max plus wavelet tipe E mempunyai *running time* yang paling cepat, sedangkan tipe B adalah yang paling lambat.

5. Dari analisis kompleksitas algoritma diketahui bahwa kompleksitas algoritma kriptografi tersebut adalah O(n) atau kompleksitas linier. Hasil ini sesuai dengan hasil uji coba *running time*. Hasil analisis kompleksitas algoritma menunjukkan bahwa Algoritma kriptografi yang dikontruksi ini efisien dalam hal waktu proses.

6. Pada tesis ini hanya dibahas tentang kontruksi algoritma kriptografi dan analisis kelayakannya berdasarkan korelasi *plaintext* dan *ciphertext*, kualitas enkripsi, simulasi *running time* dan analisis kompleksitas algoritma. Untuk pengembangan algoritma kriptograi menggunakan max plus wavelet ini diharapkan ada penelitian lanjutan yang membahas tentang keamanan algoritma kriptografi ini dari serangan pihak lain (*cryptanalysis*). Selain itu juga bisa dikembangkan penggunaan transformasi max plus wavelet untuk algoritma kriptografi *block cipher*, kriptografi citra dan lain sebagainya.

References

[1] Arul jothi, S., Venkatesulu, M., (2012), "Encryption Quality and Performance Analysis of GKSBC Algorithm", *Journal of Information Engineering and Applications*, Vol. 2, No. 10.

[2] Boggess, A., Norcowich, F. J., (2001), *A First Course In Wavelets With Fourier Analysis*, Prentice-Hall, Inc., New Jersey.

[3] Durcheva, Mariana,(2015) "Some applications of idempotent semirings in Public Key Cryptography", ACM Communication in Computer Algebra, hal. 19.

[4] Fahim, Kistosil, (2014), *Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus*, Tesis, Jurusan Matematika FMIPA Institut Teknologi Sepuluh Nopember, Surabaya.

[5] Goswami, D., Rahman, N., Biswas, J., Koul, A., Tamang, R.L., Bhattacharjee, A.K., (2011), "A Discrete Wavelet Transform based Cryptographic algorithm", *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.

[6] Grigoriev, D., Shpilrain, V., (2013), "Tropical Cryptography", International Association for Cryptologic Research.

[7] Kromodimoeljo, Sentot, (2010), *Teori Dan Aplikasi Kriptografi*, SPK IT Consulting.

[8] Rosen, K. H., (2012), *Discrete Mathematics and Its Applications, Seventh Edition*, The McGraw-Hill Companies, New York.

[9] Subiono, (2015), *Aljabar Min Max Plus Dan Terapannya*, Institut Teknologi Sepuluh Nopember, Surabaya.

[10] Walpole, R. E., (1982), *Pengantar Statistik*, PT. Gramedia Pustaka Utama, Jakarta.