

# Konstruksi Suatu Algoritma Kriptografi Menggunakan Transformasi Max Plus Wavelet

Joko Cahyono  
Subiono

PROGRAM MAGISTER JURUSAN MATEMATIKA  
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM  
**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

May 5, 2016



## Abstrak

Kriptografi berperan menjaga keamanan suatu informasi. Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi. Dalam tesis ini dikonstruksi 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.



## Abstrak

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.



## Pendahuluan

- Kriptografi adalah salah satu alat yang berperan dalam menjaga keamanan suatu informasi.
- Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi.
- Goswami dkk mengusulkan penggunaan transformasi wavelet diskrit Daubechies dalam kriptografi, yaitu untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Grigoriev dan Shpilrain, serta Durcheva mengusulkan penggunaan aljabar max plus dan aljabar min plus dalam kriptografi, yaitu untuk penyusunan kunci.



## Pendahuluan

- Kriptografi adalah salah satu alat yang berperan dalam menjaga keamanan suatu informasi.
- Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi.
- Goswami dkk mengusulkan penggunaan transformasi wavelet diskrit Daubechies dalam kriptografi, yaitu untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Grigoriev dan Shpilrain, serta Durcheva mengusulkan penggunaan aljabar max plus dan aljabar min plus dalam kriptografi, yaitu untuk penyusunan kunci.



## Pendahuluan

- Kriptografi adalah salah satu alat yang berperan dalam menjaga keamanan suatu informasi.
- Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi.
- Goswami dkk mengusulkan penggunaan transformasi wavelet diskrit Daubechies dalam kriptografi, yaitu untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Grigoriev dan Shpilrain, serta Durcheva mengusulkan penggunaan aljabar max plus dan aljabar min plus dalam kriptografi, yaitu untuk penyusunan kunci.



## Pendahuluan

- Kriptografi adalah salah satu alat yang berperan dalam menjaga keamanan suatu informasi.
- Sampai saat ini sudah banyak dibuat berbagai algoritma kriptografi.
- Goswami dkk mengusulkan penggunaan transformasi wavelet diskrit Daubechies dalam kriptografi, yaitu untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Grigoriev dan Shpilrain, serta Durcheva mengusulkan penggunaan aljabar max plus dan aljabar min plus dalam kriptografi, yaitu untuk penyusunan kunci.



## Pendahuluan

- Fahim dalam tesisnya mengkonstruksi transformasi wavelet menggunakan aljabar max plus. Kelebihan dari transformasi ini adalah tidak melibatkan *floating point* sehingga menjadi lebih sederhana dan efisien.
- Pada tesis ini dikonstruksi suatu algoritma kriptografi menggunakan transformasi max plus wavelet. Transformasi max plus wavelet digunakan untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Selanjutnya dianalisis kelayakan dari algoritma yang dihasilkan dengan cara menentukan korelasi linier antara *plaintext* dan *ciphertext*, kualitas enkripsi, *running time* program dan melakukan analisis kompleksitas algoritma.



## Pendahuluan

- Fahim dalam tesisnya mengkonstruksi transformasi wavelet menggunakan aljabar max plus. Kelebihan dari transformasi ini adalah tidak melibatkan *floating point* sehingga menjadi lebih sederhana dan efisien.
- Pada tesis ini dikonstruksi suatu algoritma kriptografi menggunakan transformasi max plus wavelet. Transformasi max plus wavelet digunakan untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Selanjutnya dianalisis kelayakan dari algoritma yang dihasilkan dengan cara menentukan korelasi linier antara *plaintext* dan *ciphertext*, kualitas enkripsi, *running time* program dan melakukan analisis kompleksitas algoritma.



## Pendahuluan

- Fahim dalam tesisnya mengkonstruksi transformasi wavelet menggunakan aljabar max plus. Kelebihan dari transformasi ini adalah tidak melibatkan *floating point* sehingga menjadi lebih sederhana dan efisien.
- Pada tesis ini dikonstruksi suatu algoritma kriptografi menggunakan transformasi max plus wavelet. Transformasi max plus wavelet digunakan untuk proses enkripsi, dekripsi dan penyusunan kunci.
- Selanjutnya dianalisis kelayakan dari algoritma yang dihasilkan dengan cara menentukan korelasi linier antara *plaintext* dan *ciphertext*, kualitas enkripsi, *running time* program dan melakukan analisis kompleksitas algoritma.



## Pendahuluan

Permasalahan yang dibahas dalam tesis ini dibatasi sebagai berikut:

- Transformasi max plus wavelet yang digunakan adalah transformasi max plus wavelet tipe A, B, C, D dan E pada penelitian Kistosil Fahim [4].
- Data yang dienkripsi berupa teks yang disimpan dalam file dengan format txt.
- Analisis kelayakan algoritma kriptografi max plus wavelet 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.



## Pendahuluan

Permasalahan yang dibahas dalam tesis ini dibatasi sebagai berikut:

- Transformasi max plus wavelet yang digunakan adalah transformasi max plus wavelet tipe A, B, C, D dan E pada penelitian Kistosil Fahim [4].
- Data yang dienkripsi berupa teks yang disimpan dalam file dengan format txt.
- Analisis kelayakan algoritma kriptografi max plus wavelet 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.



## Pendahuluan

Permasalahan yang dibahas dalam tesis ini dibatasi sebagai berikut:

- Transformasi max plus wavelet yang digunakan adalah transformasi max plus wavelet tipe A, B, C, D dan E pada penelitian Kistosil Fahim [4].
- Data yang dienkripsi berupa teks yang disimpan dalam file dengan format txt.
- Analisis kelayakan algoritma kriptografi max plus wavelet 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.



## Pendahuluan

Permasalahan yang dibahas dalam tesis ini dibatasi sebagai berikut:

- Transformasi max plus wavelet yang digunakan adalah transformasi max plus wavelet tipe A, B, C, D dan E pada penelitian Kistosil Fahim [4].
- Data yang dienkripsi berupa teks yang disimpan dalam file dengan format txt.
- Analisis kelayakan algoritma kriptografi max plus wavelet 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.



## 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.



## 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.



## 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.



## 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.



## 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.



## Transformasi Max Plus Wavelet

- Berdasarkan transformasi wavelet Haar ini, Fahim mengkontruksi transformasi wavelet menggunakan aljabar max plus.
- Aljabar max plus adalah struktur aljabar yang mempunyai dua operator yaitu maksimum dan tambah.
- Transformasi max plus wavelet yang dikonstruksi 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  $\Psi_j^\downarrow$ .



## Transformasi Max Plus Wavelet

- Berdasarkan transformasi wavelet Haar ini, Fahim mengkontruksi transformasi wavelet menggunakan aljabar max plus.
- Aljabar max plus adalah struktur aljabar yang mempunyai dua operator yaitu maksimum dan tambah.
- Transformasi max plus wavelet yang dikonstruksi 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  $\Psi_j^\downarrow$ .



## Transformasi Max Plus Wavelet

- Berdasarkan transformasi wavelet Haar ini, Fahim mengkontruksi transformasi wavelet menggunakan aljabar max plus.
- Aljabar max plus adalah struktur aljabar yang mempunyai dua operator yaitu maksimum dan tambah.
- Transformasi max plus wavelet yang dikonstruksi 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  $\Psi_j^\downarrow$ .



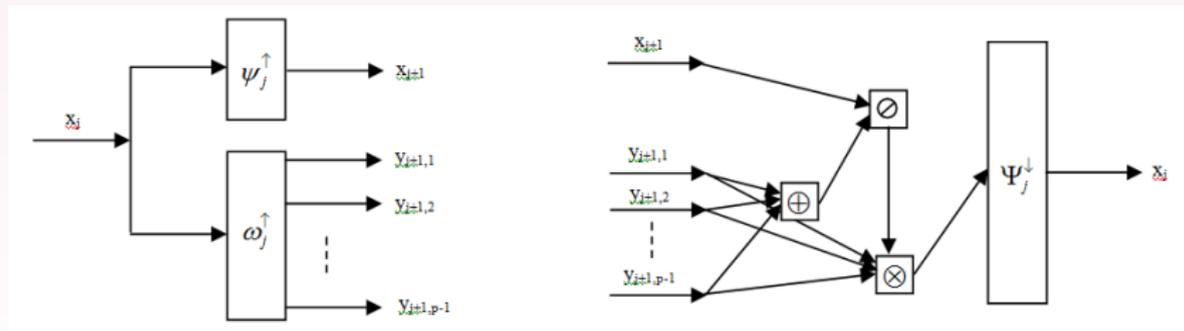
## Transformasi Max Plus Wavelet

- Berdasarkan transformasi wavelet Haar ini, Fahim mengkontruksi transformasi wavelet menggunakan aljabar max plus.
- Aljabar max plus adalah struktur aljabar yang mempunyai dua operator yaitu maksimum dan tambah.
- Transformasi max plus wavelet yang dikonstruksi 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  $\Psi_j^\downarrow$ .



# Transformasi Max Plus Wavelet

## Skema Transformasi Max Plus Wavelet Tipe A Proses Analisis dan Proses Sintesis



# Transformasi Max Plus Wavelet

Berdasarkan skema tersebut disusun operator analisis sebagai berikut :

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

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

dengan

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



# Transformasi Max Plus Wavelet

Sedangkan operasi sintesis disusun sebagai berikut:

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

$$\Psi_j^\downarrow(x_{j+1}, y_{j+1})[pn + r] = \Psi_j^\downarrow(x_{j+1}, y_{j+1})[pn] \otimes y_{j+1,r}[n],$$

with  $r = 1, 2, \dots, p - 1$



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.  
Kunci bagian pertama adalah kode max plus wavelet sedangkan kunci bagian kedua adalah banyak kanal.
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:



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.  
Kunci bagian pertama adalah kode max plus wavelet sedangkan kunci bagian kedua adalah banyak kanal.
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:



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.  
Kunci bagian pertama adalah kode max plus wavelet sedangkan kunci bagian kedua adalah banyak kanal.
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:



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.  
Kunci bagian pertama adalah kode max plus wavelet sedangkan kunci bagian kedua adalah banyak kanal.
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:



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

1. Pesan diubah menjadi kode ASCII dan disimpan dalam array **PlainASCII**.
2. Masukkan kunci enkripsi yaitu kunci kriptografi bagian pertama dan bagian kedua.  
Kunci bagian pertama adalah kode max plus wavelet sedangkan kunci bagian kedua adalah banyak kanal.
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:



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

- 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

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

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**.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

- 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

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

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**.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

- 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

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

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**.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Enkripsi

- 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

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

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**.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Penyusunan Kunci

Kunci kriptografi terdiri dari tiga bagian. Bagian pertama adalah tipe max plus wavelet, bagian kedua adalah besarnya kanal, 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 dimutlakan 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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Penyusunan Kunci

Kunci kriptografi terdiri dari tiga bagian. Bagian pertama adalah tipe max plus wavelet, bagian kedua adalah besarnya kanal, 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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Penyusunan Kunci

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Penyusunan Kunci

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Penyusunan Kunci

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

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.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. Sedangkan sisa **CipherASCII** bersama dengan kode biner akan digunakan untuk mendapatkan sinyal detail dengan rumus sebagai berikut:

• Untuk max plus wavelet tipe A, G, D dan E:

$$\text{Sinyal detail} = \text{CipherASCII} \times (-1)^{\text{kode biner}}$$

• Untuk max plus wavelet tipe B, C, F dan H:

$$\text{Sinyal detail} = -\text{CipherASCII} \times \text{kode biner}$$

7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.

8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.

9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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 =  $\text{CipherASCII} \times (-1)^{\text{kode biner}}$
  - Untuk max plus wavelet tipe B:  
Sinyal detail =  $-(\text{CipherASCII} + 95 \times \text{kode biner})$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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:  
$$\text{Sinyal detail} = \text{CipherASCII} \times (-1)^{\text{kode biner}}$$
  - Untuk max plus wavelet tipe B:  
$$\text{Sinyal detail} = -(\text{CipherASCII} + 95 \times \text{kode biner})$$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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 =  $\text{CipherASCII} \times (-1)^{\text{kode biner}}$
  - Untuk max plus wavelet tipe B:  
Sinyal detail =  $-(\text{CipherASCII} + 95 \times \text{kode biner})$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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:  
$$\text{Sinyal detail} = \text{CipherASCII} \times (-1)^{\text{kode biner}}$$
  - Untuk max plus wavelet tipe B:  
$$\text{Sinyal detail} = -(\text{CipherASCII} + 95 \times \text{kode biner})$$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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:  
$$\text{Sinyal detail} = \text{CipherASCII} \times (-1)^{\text{kode biner}}$$
  - Untuk max plus wavelet tipe B:  
$$\text{Sinyal detail} = -(\text{CipherASCII} + 95 \times \text{kode biner})$$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Konstruksi Algoritma Kriptografi Max Plus Wavelet

## Proses Dekripsi

6. 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:  
$$\text{Sinyal detail} = \text{CipherASCII} \times (-1)^{\text{kode biner}}$$
  - Untuk max plus wavelet tipe B:  
$$\text{Sinyal detail} = -(\text{CipherASCII} + 95 \times \text{kode biner})$$
7. Sinyal hampiran dan sinyal detail dimasukkan kedalam operasi sintesis.
8. Didapatkan sinyal utama yang disimpan dalam variable **PlainASCII**.
9. **PlainASCII** diubah menjadi pesan awal.



# Implementasi

- 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.
- 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.



# Implementasi

- 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.
- 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.



# Implementasi

- 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.
- 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.



# Implementasi

- 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.
- 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.



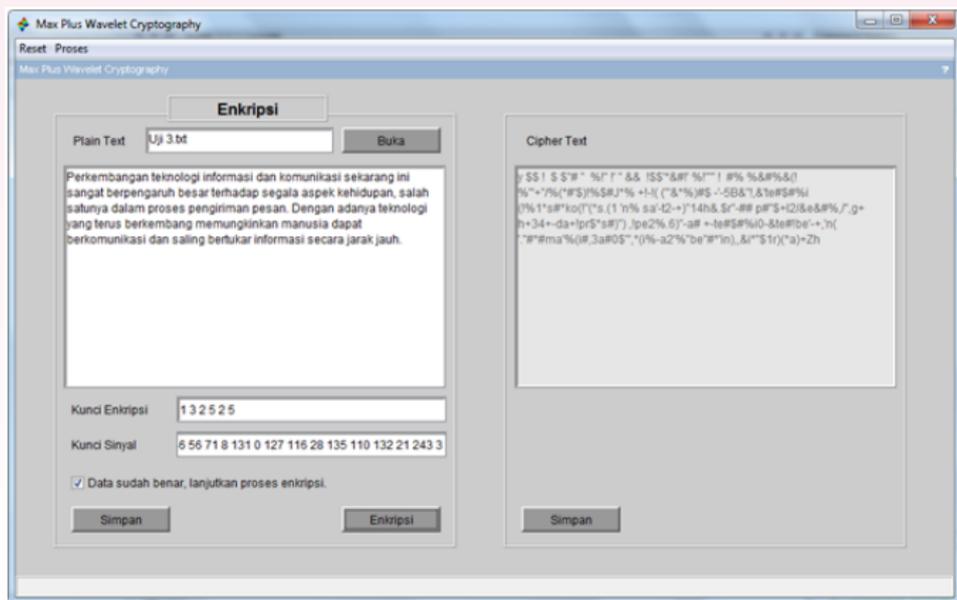
# Implementasi

- 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.
- 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.



# Implementasi

## Tampilan GUI Program Kriptografi Max Plus Wavelet



## 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 mempunyai korelasi positif. Akan tetapi jika keduanya mengikuti garis lurus dengan arah kemiringan yang berlawanan, maka mempunyai korelasi negatif.
- Jika korelasi bernilai 1 atau -1 maka *ciphertext* mempunyai hubungan linier yang kuat dengan *plaintext*, 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.



## 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 mempunyai korelasi positif. Akan tetapi jika keduanya mengikuti garis lurus dengan arah kemiringan yang berlawanan, maka mempunyai korelasi negatif.
- Jika korelasi bernilai 1 atau -1 maka *ciphertext* mempunyai hubungan linier yang kuat dengan *plaintext*, 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.



## 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 mempunyai korelasi positif. Akan tetapi jika keduanya mengikuti garis lurus dengan arah kemiringan yang berlawanan, maka mempunyai korelasi negatif.
- Jika korelasi bernilai 1 atau -1 maka *ciphertext* mempunyai hubungan linier yang kuat dengan *plaintext*, 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.



## Korelasi *plaintext* dan *ciphertext*

- Penghitungan nilai korelasi dilakukan dengan menggunakan rumus :

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

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



# Korelasi *plaintext* dan *ciphertext*

## Korelasi *plaintext* dan *ciphertext*

Nama File	Nilai Korelasi				
	Type A	Type B	Type C	Type D	Type 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



## Korelasi *plaintext* dan *ciphertext*

- Tanda negatif 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*.
- Dari Tabel tersebut terlihat bahwa nilai korelasi sebagian besar berada pada selang -0.2 sampai 0.2. 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.



## Korelasi *plaintext* dan *ciphertext*

- Tanda negatif 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*.
- Dari Tabel tersebut terlihat bahwa nilai korelasi sebagian besar berada pada selang -0.2 sampai 0.2. 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.



# Kualitas Enkripsi

- 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.
- Nilai kualitas enkripsi maksimal muncul jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*.
- Penghitungan nilai kualitas enkripsi dilakukan dengan menggunakan rumus :

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

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



# Kualitas Enkripsi

- 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.
- Nilai kualitas enkripsi maksimal muncul jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*.
- Penghitungan nilai kualitas enkripsi dilakukan dengan menggunakan rumus :

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

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



# Kualitas Enkripsi

- 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.
- Nilai kualitas enkripsi maksimal muncul jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*.
- Penghitungan nilai kualitas enkripsi dilakukan dengan menggunakan rumus :

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

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



## Kualitas Enkripsi

- 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.
- Nilai kualitas enkripsi maksimal muncul jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*.
- Penghitungan nilai kualitas enkripsi dilakukan dengan menggunakan rumus :

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

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



# Kualitas Enkripsi

## 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



## Kualitas Enkripsi

- 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*, dan dapat dihitung dengan rumus  $2n/95$ , dimana  $n$  adalah panjang *plaintext*.
- Dari hasil penghitungan 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. Sedangkan max plus wavelet tipe C dan D adalah yang terbaik.



## Kualitas Enkripsi

- 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*, dan dapat dihitung dengan rumus  $2n/95$ , dimana  $n$  adalah panjang *plaintext*.
- Dari hasil penghitungan 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. Sedangkan max plus wavelet tipe C dan D adalah yang terbaik.



## Kualitas Enkripsi

- 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*, dan dapat dihitung dengan rumus  $2n/95$ , dimana  $n$  adalah panjang *plaintext*.
- Dari hasil penghitungan 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. Sedangkan max plus wavelet tipe C dan D adalah yang terbaik.



## Kualitas Enkripsi

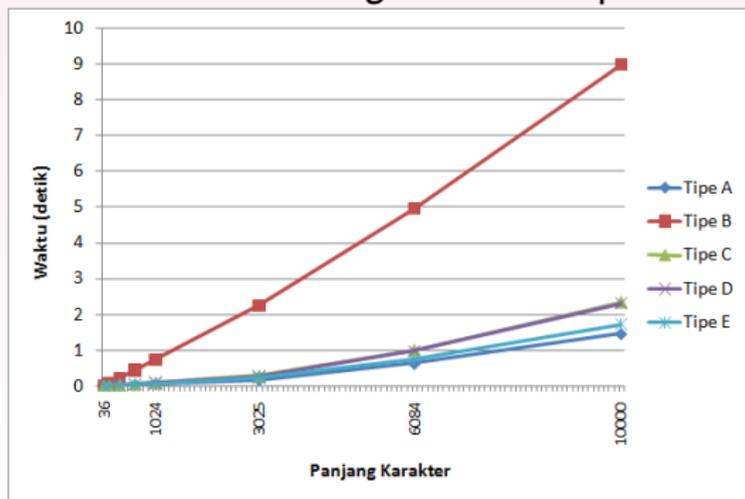
- Dari tabel tersebut terlihat bahwa semakin banyak *plaintext* maka nilai kualitas enkripsi juga semakin besar.
- Nilai kualitas enkripsi maksimal muncul jika semua karakter di *plaintext* berbeda dengan karakter di *ciphertext*, dan dapat dihitung dengan rumus  $2n/95$ , dimana  $n$  adalah panjang *plaintext*.
- Dari hasil penghitungan 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. Sedangkan max plus wavelet tipe C dan D adalah yang terbaik.



## Running Time Enkripsi

Penghitungan waktu enkripsi dimulai dari proses mengubah *plaintext* menjadi kode ASCII, proses analisis, proses penyusunan kunci hingga proses mendapatkan *ciphertext*.

Grafik *Running Time* Enkripsi



## Running Time Enkripsi

- Pada Grafik terlihat bahwa *running time* enkripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext*.
- Nilai taksiran gradien garis dapat dihitung dengan menggunakan rumus regresi :

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

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

- Nilai tipe A adalah 0.000139073, tipe B 0.000883765, tipe C 0.00022221, tipe D 0.000219091 dan tipe E 0.000162504.
- Max plus wavelet tipe A adalah tipe yang paling cepat, sedangkan tipe B adalah yang paling lambat.



## Running Time Enkripsi

- Pada Grafik terlihat bahwa *running time* enkripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext*.
- Nilai taksiran gradien garis dapat dihitung dengan menggunakan rumus regresi :

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

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

- Nilai tipe A adalah 0.000139073, tipe B 0.000883765, tipe C 0.00022221, tipe D 0.000219091 dan tipe E 0.000162504.
- Max plus wavelet tipe A adalah tipe yang paling cepat, sedangkan tipe B adalah yang paling lambat.



## Running Time Enkripsi

- Pada Grafik terlihat bahwa *running time* enkripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext*.
- Nilai taksiran gradien garis dapat dihitung dengan menggunakan rumus regresi :

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

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

- Nilai tipe A adalah 0.000139073, tipe B 0.000883765, tipe C 0.00022221, tipe D 0.000219091 dan tipe E 0.000162504.
- Max plus wavelet tipe A adalah tipe yang paling cepat, sedangkan tipe B adalah yang paling lambat.



## Running Time Enkripsi

- Pada Grafik terlihat bahwa *running time* enkripsi bertambah secara linier seiring dengan bertambahnya panjang karakter *plaintext*.
- Nilai taksiran gradien garis dapat dihitung dengan menggunakan rumus regresi :

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

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

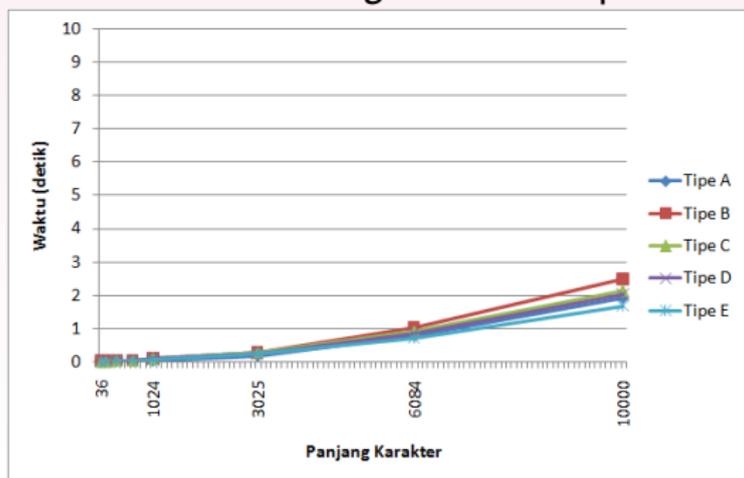
- Nilai tipe A adalah 0.000139073, tipe B 0.000883765, tipe C 0.00022221, tipe D 0.000219091 dan tipe E 0.000162504.
- Max plus wavelet tipe A adalah tipe yang paling cepat, sedangkan tipe B adalah yang paling lambat.



## 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*.

Grafik *Running Time* Dekripsi



## Running Time Dekripsi

- Pada Grafik tersebut 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.



## Running Time Dekripsi

- Pada Grafik tersebut 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.



## Running Time Dekripsi

- Pada Grafik tersebut 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.



## Running Time Dekripsi

- Pada Grafik tersebut 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.



## Pengaruh Kunci Kanal

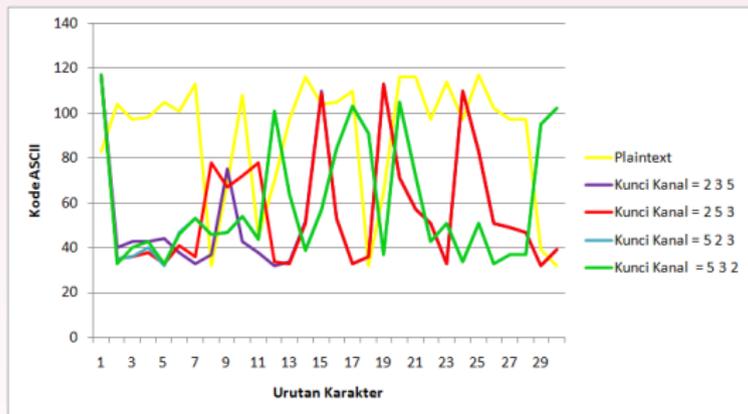
Untuk mengetahui pengaruh kunci kanal terhadap hasil enkripsi, dilakukan uji coba menggunakan file yang sama dan tipe max plus wavelet yang sama. Sedangkan kunci kanal yang digunakan berbeda. Sebagai contoh dilakukan uji coba menggunakan file uji 1.txt dengan max plus wavelet tipe A.

Kunci Kanal	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



# Pengaruh Kunci Kanal

## Perbedaan Karakter Plaintext dan Ciphertext



Hasil enkripsi menggunakan kunci 2 3 5 hampir sama dengan kunci 2 3 5. Hasil enkripsi menggunakan kunci 5 2 3 hampir sama dengan kunci 5 3 2. Perbedaan hanya terjadi di awal *ciphertext*. Hal ini disebabkan kunci kanal yang pertama adalah sama.



## Kompleksitas Algoritma

Proses yang akan dianalisa yaitu proses analisis, penyusunan kunci dan pembentukan *ciphertext* (enkripsi), serta proses sintesis dan penyusunan sinyal detail (dekripsi).

### Proses Analisis Max Plus Wavelet Tipe A

setiap  $p$  kanal terdiri dari  $p - 1$  perbandingan dan  $p - 1$  pengurangan. Jika pada enkripsi terdapat kunci kanal  $p_1, p_2, \dots, p_k$ , maka banyaknya kerja yang dilakukan adalah:

$$W_1 = \frac{n}{p_1}(p_1 - 1)(C + S)$$

$$W_2 = \frac{n}{p_1 p_2}(p_2 - 1)(C + S)$$

$$\vdots$$

$$W_k = \frac{n}{p_1 p_2 \dots p_k}(p_k - 1)(C + S).$$



# Kompleksitas Algoritma

## Proses Analisis Max Plus Wavelet Tipe A

Sehingga kerja keseluruhan

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

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

$$W < \frac{n}{p_1}(p_1) + \frac{n}{p_1 p_2}(p_2) + \dots + \frac{n}{p_1 p_2 \dots p_k}(p_k)$$



# Kompleksitas Algoritma

## Proses Analisis Max Plus Wavelet Tipe A

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

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  $O(n)$ .



# Kompleksitas Algoritma

## Proses Sintesis Max Plus Wavelet Tipe A

setiap  $p$  kanal terdiri dari  $p - 1$  perbandingan dan  $p$  penjumlahan. Jika pada dekripsi terdapat kunci kanal  $p_1, p_2, \dots, p_k$ , maka banyaknya kerja yang dilakukan adalah:

$$W_1 = \frac{n}{p_1}((p_1 - 1)C + p_1 S)$$

$$W_2 = \frac{n}{p_1 p_2}((p_2 - 1)C + p_2 S)$$

$$\vdots$$

$$W_k = \frac{n}{p_1 p_2 \dots p_k}((p_k - 1)C + p_k S).$$



# Kompleksitas Algoritma

## Proses Sintesis Max Plus Wavelet Tipe A

Sehingga kerja keseluruhan

$$W = W_1 + W_2 \dots W_k$$

$$W = \frac{n}{p_1}((p_1 - 1)C + p_1 S) + \frac{n}{p_1 p_2}((p_2 - 1)C + p_2 S) + \dots$$

$$+ \frac{n}{p_1 p_2 \dots p_k}((p_k - 1)C + p_k S).$$

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

$$W < \frac{n}{p_1}(p_1) + \frac{n}{p_1 p_2}(p_2) + \dots + \frac{n}{p_1 p_2 \dots p_k}(p_k)$$



# Kompleksitas Algoritma

## Proses Sintesis Max Plus Wavelet Tipe A

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

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  $O(n)$ .



# Kompleksitas Algoritma

## Proses Penyusunan Kode Sinyal Detail dan *Ciphertext*

Transformasi max plus wavelet tipe A, C, D dan E:

```
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)
```

Y adalah sinyal detail dengan panjang  $n-1$ . Operasi yang ada adalah perbandingan, penjumlahan dan fungsi absolut yang dilakukan sebanyak  $n - 1$ . Karena  $n - 1 < n$  maka kompleksitasnya adalah  $O(n)$  atau kompleksitas linier.



# Kompleksitas Algoritma

## Proses Penyusunan Kode Sinyal Detail dan *Ciphertext*

Transformasi max plus wavelet tipe B:

```
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)
```

Operasi yang ada yaitu perbandingan, penjumlahan, pengurangan, fungsi absolut dan modulo, yang dilakukan sebanyak  $n - 1$ . Sehingga kompleksitasnya adalah  $O(n)$ .



# Kompleksitas Algoritma

## Proses Penyusunan Sinyal Detail

Proses ini dilakukan sebelum melakukan proses sintesis. Pada max plus wavelet tipe A, C, D dan E:

```
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 yang dilakukan sebanyak  $n - 1$ . Karena  $n - 1 < n$  maka kompleksitasnya adalah  $O(n)$  atau kompleksitas linier.



# Kompleksitas Algoritma

## Proses Penyusunan Sinyal Detail

Pada max plus wavelet tipe B:

```
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. Operasi penjumlahan dilakukan sebanyak  $n - 1$  dan operasi perkalian dilakukan sebanyak  $2(n - 1)$ . Karena  $n - 1 < n$  dan  $2(n - 1) < 2n$  maka kompleksitasnya adalah  $O(n)$  atau kompleksitas linier.



## Kompleksitas Algoritma

- Dari analisis kompleksitas 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 grafik *running time* enkripsi dan dekripsi.
- *Running time* dari proses analisis menggunakan max plus wavelet tipe B terlihat jauh lebih lambat daripada tipe yang lain. Berdasarkan analisis kompleksitas, hal ini terjadi karena proses penyusunan kunci dan *ciphertext* pada max plus wavelet tipe B menggunakan lebih banyak operasi daripada tipe yang lain.



## Kompleksitas Algoritma

- Dari analisis kompleksitas 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 grafik *running time* enkripsi dan dekripsi.
- *Running time* dari proses analisis menggunakan max plus wavelet tipe B terlihat jauh lebih lambat daripada tipe yang lain. Berdasarkan analisis kompleksitas, hal ini terjadi karena proses penyusunan kunci dan *ciphertext* pada max plus wavelet tipe B menggunakan lebih banyak operasi daripada tipe yang lain.



## Kompleksitas Algoritma

- Dari analisis kompleksitas 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 grafik *running time* enkripsi dan dekripsi.
- *Running time* dari proses analisis menggunakan max plus wavelet tipe B terlihat jauh lebih lambat daripada tipe yang lain. Berdasarkan analisis kompleksitas, hal ini terjadi karena proses penyusunan kunci dan *ciphertext* pada max plus wavelet tipe B menggunakan lebih banyak operasi daripada tipe yang lain.



## Kesimpulan

1. Algoritma kriptografi berdasarkan transformasi max plus wavelet ini termasuk dalam algoritma kriptografi *stream cipher*. Proses enkripsi dan dekripsi didasarkan pada proses analisis dan 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. Algoritma kriptografi 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.



## Kesimpulan

1. Algoritma kriptografi berdasarkan transformasi max plus wavelet ini termasuk dalam algoritma kriptografi *stream cipher*. Proses enkripsi dan dekripsi didasarkan pada proses analisis dan 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. Algoritma kriptografi 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.



## Kesimpulan

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.



## Kesimpulan

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.



## Kesimpulan

5. Kompleksitas algoritma kriptografi ini adalah  $O(n)$  atau kompleksitas linier. Hasil ini sesuai dengan hasil uji coba *running time*. Hasil analisis kompleksitas algoritma menunjukkan bahwa Algoritma kriptografi yang dikonstruksi ini efisien dalam hal waktu proses.
6. Pada tesis ini hanya dibahas tentang konstruksi algoritma kriptografi dan analisis kelayakannya berdasarkan korelasi *plaintext* dan *ciphertext*, kualitas enkripsi, simulasi *running time* dan analisis kompleksitas algoritma. Untuk pengembangan algoritma ini diharapkan ada penelitian lanjutan yang membahas tentang keamanannya (*cryptanalysis*). Selain itu juga bisa dikembangkan penggunaan transformasi max plus wavelet untuk algoritma kriptografi *block cipher*, kriptografi citra dan lain sebagainya.



## Kesimpulan

5. Kompleksitas algoritma kriptografi ini adalah  $O(n)$  atau kompleksitas linier. Hasil ini sesuai dengan hasil uji coba *running time*. Hasil analisis kompleksitas algoritma menunjukkan bahwa Algoritma kriptografi yang dikonstruksi ini efisien dalam hal waktu proses.
6. Pada tesis ini hanya dibahas tentang konstruksi algoritma kriptografi dan analisis kelayakannya berdasarkan korelasi *plaintext* dan *ciphertext*, kualitas enkripsi, simulasi *running time* dan analisis kompleksitas algoritma. Untuk pengembangan algoritma ini diharapkan ada penelitian lanjutan yang membahas tentang keamanannya (*cryptanalysis*). Selain itu juga bisa dikembangkan penggunaan transformasi max plus wavelet untuk algoritma kriptografi *block cipher*, kriptografi citra dan lain sebagainya.



## Daftar Pustaka

-  Arul jothi, S., Venkatesulu, M., (2012), "Encryption Quality and Performance Analysis of GK SBC Algorithm", *Journal of Information Engineering and Applications*, Vol. 2, No. 10.
-  Boggess, A., Norcowich, F. J., (2001), *A First Course In Wavelets With Fourier Analysis*, Prentice-Hall, Inc., New Jersey.
-  Durcheva, Mariana,(2015) "Some applications of idempotent semirings in Public Key Cryptography", *ACM Communication in Computer Algebra*, hal. 19.
-  Fahim, Kistosil, (2014), *Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus*, Tesis, Jurusan Matematika FMIPA Institut Teknologi Sepuluh Nopember, Surabaya.



## Daftar Pustaka

-  Arul jothi, S., Venkatesulu, M., (2012), "Encryption Quality and Performance Analysis of GK SBC Algorithm", *Journal of Information Engineering and Applications*, Vol. 2, No. 10.
-  Boggess, A., Norcowich, F. J., (2001), *A First Course In Wavelets With Fourier Analysis*, Prentice-Hall, Inc., New Jersey.
-  Durcheva, Mariana,(2015) "Some applications of idempotent semirings in Public Key Cryptography", *ACM Communication in Computer Algebra*, hal. 19.
-  Fahim, Kistosil, (2014), *Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus*, Tesis, Jurusan Matematika FMIPA Institut Teknologi Sepuluh Nopember, Surabaya.



## Daftar Pustaka

-  Arul jothi, S., Venkatesulu, M., (2012), "Encryption Quality and Performance Analysis of GK SBC Algorithm", *Journal of Information Engineering and Applications*, Vol. 2, No. 10.
-  Boggess, A., Norcowich, F. J., (2001), *A First Course In Wavelets With Fourier Analysis*, Prentice-Hall, Inc., New Jersey.
-  Durcheva, Mariana,(2015) "Some applications of idempotent semirings in Public Key Cryptography", *ACM Communication in Computer Algebra*, hal. 19.
-  Fahim, Kistosil, (2014), *Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus*, Tesis, Jurusan Matematika FMIPA Institut Teknologi Sepuluh Nopember, Surabaya.



## Daftar Pustaka

-  Arul jothi, S., Venkatesulu, M., (2012), "Encryption Quality and Performance Analysis of GKSBK Algorithm", *Journal of Information Engineering and Applications*, Vol. 2, No. 10.
-  Boggess, A., Norcowich, F. J., (2001), *A First Course In Wavelets With Fourier Analysis*, Prentice-Hall, Inc., New Jersey.
-  Durcheva, Mariana,(2015) "Some applications of idempotent semirings in Public Key Cryptography", *ACM Communication in Computer Algebra*, hal. 19.
-  Fahim, Kistosil, (2014), *Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus*, Tesis, Jurusan Matematika FMIPA Institut Teknologi Sepuluh Nopember, Surabaya.



## Daftar Pustaka

-  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.
-  Grigoriev, D., Shpilrain, V., (2013), "Tropical Cryptography", International Association for Cryptologic Research.
-  Kromodimoeljo, Sentot, (2010), *Teori Dan Aplikasi Kriptografi*, SPK IT Consulting.
-  Rosen, K. H., (2012), *Discrete Mathematics and Its Applications, Seventh Edition*, The McGraw-Hill Companies, New York.



## Daftar Pustaka

-  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.
-  Grigoriev, D., Shpilrain, V., (2013), "Tropical Cryptography", International Association for Cryptologic Research.
-  Kromodimoeljo, Sentot, (2010), *Teori Dan Aplikasi Kriptografi*, SPK IT Consulting.
-  Rosen, K. H., (2012), *Discrete Mathematics and Its Applications, Seventh Edition*, The McGraw-Hill Companies, New York.



## Daftar Pustaka

-  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.
-  Grigoriev, D., Shpilrain, V., (2013), "Tropical Cryptography", International Association for Cryptologic Research.
-  Kromodimoeljo, Sentot, (2010), *Teori Dan Aplikasi Kriptografi*, SPK IT Consulting.
-  Rosen, K. H., (2012), *Discrete Mathematics and Its Applications, Seventh Edition*, The McGraw-Hill Companies, New York.



## Daftar Pustaka

-  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.
-  Grigoriev, D., Shpilrain, V., (2013), "Tropical Cryptography", International Association for Cryptologic Research.
-  Kromodimoeljo, Sentot, (2010), *Teori Dan Aplikasi Kriptografi*, SPK IT Consulting.
-  Rosen, K. H., (2012), *Discrete Mathematics and Its Applications, Seventh Edition*, The McGraw-Hill Companies, New York.



## Daftar Pustaka

-  Subiono, (2015), *Aljabar Min Max Plus Dan Terapannya*, Institut Teknologi Sepuluh Nopember, Surabaya.
-  Walpole, R. E., (1982), *Pengantar Statistik*, PT. Gramedia Pustaka Utama, Jakarta.



## Daftar Pustaka

-  Subiono, (2015), *Aljabar Min Max Plus Dan Terapannya*, Institut Teknologi Sepuluh Nopember, Surabaya.
-  Walpole, R. E., (1982), *Pengantar Statistik*, PT. Gramedia Pustaka Utama, Jakarta.

