**Prosiding Seminar Nasional Integrasi Matematika dan Nilai Islami**
Vol.2, No.1, Desember 2018, pp. 25~30
p-ISSN: 2580-4596 **; e-ISSN:** 2580-460X


# Implementasi Kriptografi pada Teks Menggunakan Metode *Block Chiper*

**Mif'atul Mahmudah*, Aris Fanani*, Moh. Hafiyusholeh***

* Program Studi Matematika, UIN Sunan Ampel Surabaya

Email:Atulmahmudah08@gmail.com, arisfa@uinsby.ac.id, hafiyusholeh@uinsby.com

**Info Artikel**

**Riwayat Artikel:**

Diterima: 1 Oktober 2018
Direvisi: 1 November 2018
Diterbitkan: 1 Desember 2018

**Kata Kunci:**

*Plaintext*
Kunci
Kriptografi
Tanam padi dan Bajak sawah
*Block cipher*

**ABSTRAK**

Berkembangnya teknologi dan komunikasi memudahkan kriptanalis untuk melakukan penyadapan, untuk menghindari hal tersebut perlu dilakukan pengamanan terhadap informasi yang dikirim, salah satu ilmu yang digunakan dalam mengamankan data adalah kriptografi dengan metode *block cipher*, dimana algoritma *block cipher* yang digunakan dalam penelitian ini adalah algoritma tanam padi dan bajak sawah, algoritma tersebut dipilih karena memiliki kecepatan enkripsi dan dekripsi lebih cepat dibandingkan dengan metode AES (*Advanced Encryption Standard*). Proses pembangkitan kunci dimulai dengan merubah kunci yang telah ditentukan yaitu "muslimah" kedalam bentuk biner, selanjutnya pemasukan dan pengambilan bit dengan pola bajak sawah. Proses enkripsi dimulai dengan merubah *plaintext* "mahmudah" kedalam bentuk biner, selanjutnya pemasukan dan pengambilan bit dilakukan dengan pola tanam padi, hasil dari pengambilan *plaintext* dan pembangkitan kunci kemudian di XOR-kan, diproses sampai delapan putaran, sehingga dihasilkan enkripsi *"úEOTèZüüb*ư". Proses dekripsi yaitu ciphertext di XOR-kan dengan kunci yang telah dibangkitkan. Hasil XOR dimasukan kedalam bit menggunakan pola pengambilan *plaintext* dan diambil dengan pola pemasukan *plaintext*, setelah itu hasilnya di XOR-kan dengan kunci yang telah dibangkitkan. Proses tersebut diulang sampai delapan kali putaran, menghasilkan dekripsi yaitu "mahmudah".



**Korespondensi:**

Mif'atul Mahmudah, Aris Fanani, M.Kom, Dr. Moh. Hafiyusholeh, M.Si
Prodi Matematika
UIN Sunan Ampel Surabaya
Jln. Jl. A. Yani 117 Surabaya, Jawa Timur, Indonesia, 60237
Email:Atulmahmudah08@gmail.com

## 1. PENDAHULUAN

Berkembangnya teknologi dan komunikasi memudahkan manusia dalam bertukar informasi dengan dunia luar, sehingga keamanan data yang dikirim rawan terhadap penyadapan. Untuk menghindari penyadapan data ataupun informasi yang akan dikirim perlu dilakukan pengamanan, salah satu ilmu yang dapat digunakan dalam mengamankan data adalah kriptografi. Ada beberapa penelitian terdahulu mengenai pengamanan teks, seperti penelitian yang telah dilakukan oleh Ana Kurniawati dan Muhammad Dwiky Darmawan pada tahun 2016 yang berjudul "Implementasi Algoritma Advanced Encryption Standard (AES) untuk Enkripsi dan Dekripsi pada dokumen teks". Penelitian ini membahas tentang cara mengamankan file dokumen dengan menggunakan algoritma kriptografi Advanced Encryption Standard (AES) yang dibuat di perangkat lunak yaitu Windows 7 Ultimate 32-bit dan Netbeans 8.1.

Penelitian kedua tentang pengamanan file dokumen adalah penelitian yang dilakukan oleh Fresly Nandar Pabokory, Indah Fitri Astuti, dan Awang Harsa pada tahun 2015 yang berjudul "Implementasi

Kriptografi Pengamanan Data pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advance Encryption Standard". Penelitian ini membahas tentang sistem keamanan data dengan mengimplementasikan kriptografi dengan algoritma Advance Encryption Standard (AES) pada pesan teks, isi file dokumen, dan file dokumen dengan menggunakan program Fres-CAESAS.

Mayoritas pengamanan file dokumen pada penelitian terdahulu menggunakan metode AES karena metode AES lebih cepat. Namun ada pengembangan penelitian yang membandingkan metode AES dengan metode tanam padi dan bajak sawah yaitu Ahmad Widodo, Alz Danny Wowor, Evangs Mailoa, dan Magdalena A.Ineke Pakereng pada tahun 2015 dengan judul "Perancangan Kriptografi Block Cipher Berbasis Pada Teknik Tanam Padi dan Bajak Sawah". Dimana tanam padi sebagai plaintext dan bajak sawah sebagai kunci. Setelah algoritma tersebut sudah selesai, untuk mengetahui kecepatan dari algoritma tanam padi dan bajak sawah tersebut dibandingkan dengan metode AES. Setelah dibandingkan, menunjukan bahwa metode tanam padi dan bajak sawah lebih cepat dalam mengamankan teks dibandingkan dengan metode AES-128.

Pada penelitian ini dikaji penyandian dan penguraian sandi menggunakan metode block chiper dengan algoritma tanam padi dan bajak sawah. Algoritma Tanam padi digunakan untuk mengubah plaintext dalam bentuk ciphertext, sedangkan bajak sawah digunakan untuk membangkitkan kunci.

## 2. TINJAUAN PUSTAKA

### 2.1 Kriptografi

Kata Kriptografi berasal dari bahasa Yunani yaitu *crypto* yang berarti rahasia dan *graphia* yang berarti tulisan. Berarti kata kriptografi adalah tulisan rahasia.

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan sebuah pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dipahami lagi maknanya. Menurut Menezes, kriptografi adalah sebuah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, misalnya kerahasiaan, integritas data, serta otentikasinya.

Enkripsi merupakan proses penyandian plaintext menjadi ciphertext (Rosnawan, 2011). Sedangkan dekripsi merupakan proses mengembalikan ciphertext menjadi plaintext-nya.

### 2.2 *Cipher block*

Cipher block merupakan suatu algoritma yang membagi rangkaian bit menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Plaintext akan diproses dengan panjang blok yang tetap. Pada umumnya, setiap cipher block memproses teks dengan blok yang relatif panjangnya lebih dari 64-bit, untuk mempersulit teknik kriptanalisis dalam membongkar kunci. Dalam cipher block menggunakan kunci simetris untuk proses enkripsi dan dekripsinya karena kunci merupakan parameter yang digunakan untuk transformasi plaintext ke ciphertext.

Misalkan blok plaintext (P) yang berukuran n bit dinyatakan sebagai vektor

$P = (P_1, P_2, \ldots, P_n)$ (1)

Dalam hal ini $p_i$ adalah 0 atau 1 untuk $i = 1,2,\ldots,n$ dan blok ciphertext (C) adalah :

$C = (c_1, c_2, \ldots, c_n)$ (2)

Dalam hal ini $c_i$ adalah 0 atau 1 untuk $i = 1,2,\ldots,n$ bila plaintext dibagi menjadi m buah blok, barisan blok-blok plaintext dinyatakan sebagai $(P_1, P_2, \ldots, P_m)$ untuk setiap blok plaintext $p_i$, bit-bit penyusunannya dapat dinyatakan sebagai vektor

$p_i = (P_1, P_2, \ldots, p_m)$ (3)

Enkripsi dan dekripsi dengan kunci K dinyatakan berturut-turut $E_k(p) = C$ adalah enkripsi dan $D_k(C) = P$. Fungsi E harus berkorespondensi satu satu. $E^1 = D$.

### 2.3 Teknik tanam padi dan bajak sawah

Pengembangan dari metode *Cipher block* sangat banyak sekali. Salah satu yang digunakan dalam penelitian ini yaitu algoritma tanam padi dan bajak sawah yang terinspirasi dari kearifan lokal sehingga diberi nama tanam padi dan bajak sawah. Algoritma tanam padi digunakan untuk mengubah plaintext kedalam bentuk *ciphertext*, sedangkan bajak sawah digunakan membangkitkan kunci.

**1. Tanam Padi**

Algoritma tanam padi digunakan untuk sebuah *plaintext*. Proses tanam padi biasanya dilakukan dengan menyesuaikan dengan panjang petakan sawah. Penanaman dilakukan secara horisontal yang berkesinambungan. Rancangan ini menggunakan cara yang sama dengan menempatkan bit seperti proses penanaman padi, dengan menggunakan kotak berukuran 8×8 yang

secara keseluruhan terdapat 64 kotak. Setiap kotak ditempatkan satu bit, sehingga untuk melakukan satu kali proses dibutuhkan 8 karakter. Misal *plaintext*

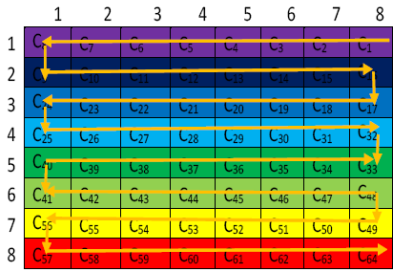
$$Y = \{Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7, Y_8\}$$
$$Y_1 = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$$
$$Y_2 = \{C_9, C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}\} \quad (4)$$
$$\vdots$$
$$Y_n = \{C_{8-7}, C_{8-6}, C_{8-5}, \dots, C_8\}$$

Diubah dalam bentuk bit yang akan menghasilkan 64 bit, dimana bit-bit tersebut diubah kedalam biner berdasarkan karakternya yaitu :

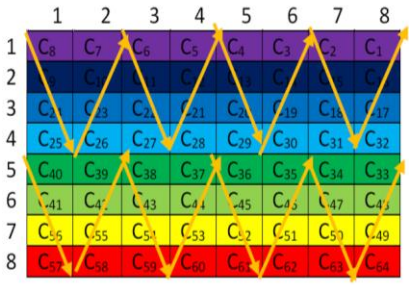
$Kar\ 1 \rightarrow \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$
$Kar\ 2 \rightarrow \{C_9, C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}\}$
$Kar\ 3 \rightarrow \{C_{17}, C_{18}, C_{19}, C_{20}, C_{21}, C_{22}, C_{23}, C_{24}\}$
$Kar\ 4 \rightarrow \{C_{25}, C_{26}, C_{27}, C_{28}, C_{29}, C_{30}, C_{31}, C_{32}\}$
$Kar\ 5 \rightarrow \{C_{33}, C_{34}, C_{35}, C_{36}, C_{37}, C_{38}, C_{39}, C_{40}\}$
$Kar\ 6 \rightarrow \{C_{41}, C_{42}, C_{43}, C_{44}, C_{45}, C_{46}, C_{47}, C_{48}\}$
$Kar\ 7 \rightarrow \{C_{49}, C_{50}, C_{51}, C_{52}, C_{53}, C_{54}, C_{55}, C_{56}\}$
$Kar\ 8 \rightarrow \{C_{57}, C_{58}, C_{59}, C_{60}, C_{61}, C_{62}, C_{63}, C_{64}\}$

Selanjutnya bit-bit dari plaintextnya yaitu pada Persamaan 4akan dimasukkan kedalam matriks dengan menggunakan pola masukan tanam padi. Seperti pada Gambar 1dan selanjutnya akan di ambil bit baru dengan menggunakan pola pengambilan tanam padi, seperti pada Gambar 2, didapatkan bit baru yaitu:

$$P_8 = C_{40,}C_{41}, C_{56}, \dots, C_{32}, C_{17}, C_{16}, C_1$$



**Gambar 1. Pemasukan bit plaintext menggunakan pola tanam padi**



**Gambar 2.Pengambilan bit plaintext menggunakan pola tanam padi**

**2. Bajak Sawah**

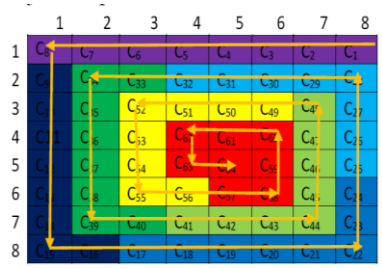
Teknik bajak sawah digunakan untuk membangkitkan sebuah kunci. Pola dalam teknik bajak sawah adalah spiral. Misal sebuah kunci

$$X = \{X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8\}$$
$$X_1 = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$$
$$X_2 = \{C_9, C_{10}, C_{11}, \dots, C_{14}, C_{15}, C_{16}\} \quad (5)$$
$$\vdots$$
$$X_n = \{C_{8-7}, C_{8-6}, C_{8-5}, \dots, C_8,\}$$

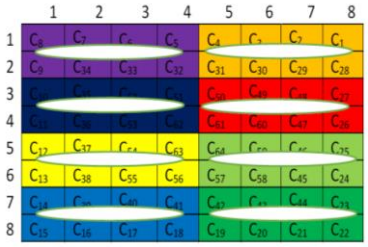
Diubah kedalam bentuk bit yang akan menghasilkan 64 bit, dimana bit-bit tersebut berdasarkan karakternya yaitu :

$kun\ 1$ ➔ $\{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$
$kun\ 2$ ➔ $\{C_9, C_{10}, C_{11}, C_{12}, C_{13}, C_{14}, C_{15}, C_{16}\}$
$kun\ 3$ ➔ $\{C_{17}, C_{18}, C_{19}, C_{20}, C_{21}, C_{22}, C_{23}, C_{24}\}$
$kun\ 4$ ➔ $\{C_{25}, C_{26}, C_{27}, C_{28}, C_{29}, C_{30}, C_{31}, C_{32}\}$
$kun\ 5$ ➔ $\{C_{33}, C_{34}, C_{35}, C_{36}, C_{37}, C_{38}, C_{39}, C_{40}\}$
$kun\ 6$ ➔ $\{C_{41}, C_{42}, C_{43}, C_{44}, C_{45}, C_{46}, C_{47}, C_{48}\}$
$kun\ 7$ ➔ $\{C_{49}, C_{50}, C_{51}, C_{52}, C_{53}, C_{54}, C_{55}, C_{56}\}$
$kun\ 8$ ➔ $\{C_{57}, C_{58}, C_{59}, C_{60}, C_{61}, C_{62}, C_{63}, C_{64}\}$

Proses masukan bit-bit kunci dilakukan dengan mengikuti pola bajak sawah yang ditunjukan pada Gambar 3. Selanjutnya akan diambil bit bit baru dengan menggunakan pola bajak sawah yang ditunjukan pada Gambar 4.



**Gambar 3. Pemasukan bit kunci menggunakan pola bajak sawah**



**Gambar 4. Pengambilan bit kunci menggunakan pola bajak sawah**

## 3. HASIL DAN PEMBAHASAN

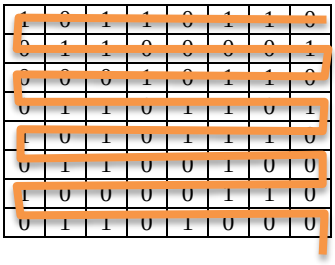
Pada pembahasan ini dilakukan penyandian plaintext “mahmudah” dengan menggunakan kata kunci “muslimah”.

### 3.1 Enkripsi

Proses enkripsi dimulai dari merubah plaintext dan kunci kedalam bentuk biner yaitu

$m = 109 = 01101101, a = 97 = 01100001, h = 104 = 01101000, u = 117 = 01110101,$
$d = 100 = 01100100, s = 115 = 01110011, l = 108 = 01101100, i = 105 = 01101001.$

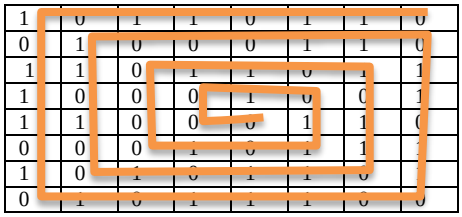
Selanjutnya dimasukan kedalam bit dan diambil bit-bitnya menggunakan teknik tanam padi, sebagaimana ilustrasi pada gambar berikut.



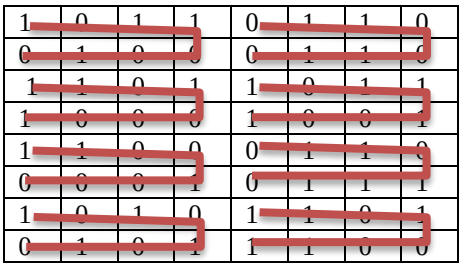
**Gambar 8. Pemasukan bit plaintext putaran 1**

**Gambar 9. Pengambilan bit plaintext putaran 1**

Dari proses pengambilan bit plaintext didapatkan hasil
$p_1$ = 10101010 11010000 10010111 10100000 10001010 11010101 00011101 10101010
Setelah itu ialah proses pembangkitan kunci dimana bit-bit kunci yang telah dirubah kedalam biner dimasukan kedalam pola pemasukan dan pengambilan bit kunci dengan menggunakan algoritma bajak sawah seperti pada Gambar 3 dan 4 yaitu.



**Gambar 10. Pemasukan bit kunci putaran 1**

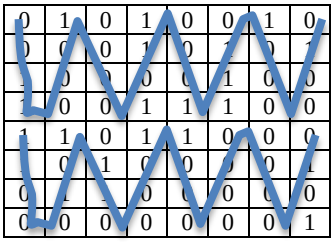


**Gambar 11. Pengambilan bit kunci putaran 1**

Dari pengambilan bit kunci pada putaran satu didapatkan hasil
$K_1$ = 10110010 11010001 11001000 10101010 11010011 01101110 10111001 01100110
selanjutnya hasil dari pengambilan *plaintext* dan pembangkitan kunci di XOR-kan yaitu :
$p_1$ = 10101010 11010000 10010111 10100000 10001010 11010101 00011101 10101010$K_1$ = 10110010 11010001 11001000 10101010 11010011 01101110 10111001 01100110
----------XOR----------
$R_1$ = 00011000 00000001 01011111 00001010 01011001 10111011 10100100 11001100
Hasil dari XOR diproses lagi dan diulang sampai dengan 8 putaran, hingga didapatkan hasil akhir atau *ciphertext "ú*EOT*è*Z*üüü*b*ɯ*"

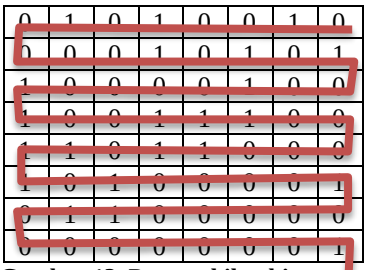
## 3.2 Dekripsi

Proses dekripsi dimulai dari ciphertext di XOR-kan dengan kunci yang telah dibangkitkan yaitu $R_8$ = 11111010 00000100 11101000 01011010 11111100 11111011 01100010 11011100
$K_8$ = 00111111 01100101 01101000 01010000 11001101 11110000 01111100 01011110
----------XOR----------
$P_8$ = 11000101 01100001 10000000 00001010 00110001 00001011 00011110 10000010
Hasil XOR dari *ciphertext* di masukan kedalam bit dengan pola pengambilan pada plaintext, yaitu sebagai berikut:



**Gambar 12. Pemasukan bit putaran 1**

lalu dilakukan pengambilan bit dengan pola masukan pada plaintext, sebagaimana ilustrasi gambar sebagai berikut.



**Gambar 13. Pengambilan bit putaran 1**

Hasil dari pengambilan bit tersebut akan di XOR-kan lagi dengan kunci yang telah dibangkitkan yang selanjutnya dilakukan pemasukan dan pengambilan bit, proses tersebut diulang sampai dengan 8 putaran hingga didapatkan hasil dari proses dekripsi yaitu “mahmudah”.

## 4. KESIMPULAN

1. Proses dekripsi dimulai dari ciphertext di XOR-kan dengan kunci yang telah dibangkitkan. Hasil XOR dari ciphertext di masukan kedalam bit dengan pola pengambilan pada plaintext, lalu pengambilan bit dengan pola masukan pada plaintext. Proses tersebut diulang sampai dengan 8 putaran hingga didapatkan hasil dari proses dekripsi yaitu “mahmudah”.
2. Proses enkripsi dimulai dari merubah plaintext kedalam bentuk biner, selanjutnya dimasukan kedalam bit dan diambil bit-bitnya menggunakan teknik tanam padi. selanjutnya hasil dari pengambilan plaintext dan pembangkitan kunci di XOR-kan. Hasil dari XOR diproses lagi dan diulang sampai dengan 8 putaran, hingga didapatkan hasil akhir atau ciphertext “úEOTèZüübu”
3. Proses dekripsi dimulai dari ciphertext di XOR-kan dengan kunci yang telah dibangkitkan. Hasil XOR dari ciphertext di masukan kedalam bit dengan pola pengambilan pada plaintext, lalu pengambilan bit dengan pola masukan pada plaintext. Proses tersebut diulang sampai dengan 8 putaran hingga didapatkan hasil dari proses dekripsi yaitu “mahmudah”.

## REFERENSI


[1] Kurniawati, A., & Darmawan, D. M. (2016). Implementasi algoritma advanced encryption standard (AES) untuk enkripsi dan dekripsi pada dokumen Halpen-Felsher BL, Morrell HE. Preventing and reducing tobacco use. In: Berlan ED, Bravender T, editors. Adolescent medicine today: a guide to caring for the adolescent patient [Internet]. Singapore: World Scientific Publishing Co.; 2012 [cited 2012 Nov 3]. Chapter 18. Available from: http://www.worldscientific.com/doi/pdf/10.1142/9789814324496_0018

[2] Lusiana, V. (2011). Implementasi kriptografi pada file dokumen. *Nitro PDF*.

[3] Munir, R. (2006). *Kriptografi*. Bandung: Departemen Teknik Informatika.

[4] Nurhardian, & Pudoli, A. (2016). Implementasi keamanan file dengan kompresi Huffman dan Kriptografi menggunakan algoritma RC4 serta Steganografi menggunakan End of File berbasis desktop pada SMK Negeri 3 Kota tangerang. *jurnal TICOM*.

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

[6] Rosnawan, D. (2011). *Aplikasi algoritma RSA untuk keamanan data pada sistem informasi berbasis web.* Semarang: Universitas Negeri Semarang.

[7] Widodo, A., Wowor, d. a., Mailoa, E., & Pakereng, M. A. (2015). Perancangan Kriptografi Block Cipher Berbasis pada teknik tanam padi dan bajak sawah. *Seminar Nasional Teknik Informatika dan Sistem Informasi (SETISI)*.