Jurnal Teknovasi
Volume 03, Nomor 2, 2016, 23 – 31
ISSN : 2355-701X

# APLIKASI KRIPTOGRAFI DATA SEDERHANA DENGAN METODE *EXLUSIVE-OR (XOR)*

Suhardi*
Program Studi Teknik Komputer, Politeknik LP3I Medan
Telp. 061-7322634 Fax: 061-7322649
*Email : ardie06200141@gmail.com

## ABSTRAK

Perkembangan teknologi informasi mengharuskan aspek keamanan data menjadi penting untuk diketahui. Aspek-aspek keamanan data yaitu : *Confidentiality, Authentication, Data integrity* dan *Nonrepudiation*. Pengetahuan terhadap aspek keamanan data bertujuan untuk mengetahui sejauh mana usaha yang telah kita lakukan untuk mengamankan data, serta upaya-upaya lanjut yang harus kita lakukan untuk menjamin bahwa data tersebut benar-benar aman. Salah satu upaya pengamanan data yang dilakukan adalah dengan menggunakan kriptografi. Kriptografi sendiri dapat didefenisikan sebagai seni dan ilmu dalam mengamankan pesan. Kriptografi bertujuan mengamankan data, sehingga data yang bersifat rahasia dan penting tidak dapat diakses oleh pihak-pihak yang tidak mempunyai izin untuk data tersebut. Penelitian ini akan menjelaskan langkah - langkah dalam kriptografi dengan metode XOR beserta implementasi salah satu teknik kriptografi modern menggunakan kunci simetris dengan metode XOR untuk enkripsi dan deskripsi data.

**Kata Kunci : Kriptografi, enkripsi, deskripsi, XOR**

## PENDAHULUAN

Data menjadi sesuatu yang amat berharga di dalam abad teknologi informasi dewasa ini. Apalagi jika data tersebut sangat rahasia dan tidak sembarang orang yang boleh mengaksesnya. Bentuk data yang diamankan dalam hal ini adalah berbentuk digital atau elektronik. Perlakuan khusus terhadap data akan diperlukan apabila data ditujukan hanya untuk kalangan terbatas dan jika data tersebut dikirimkan melalui Internet, sementara itu isi data tidak boleh berubah dari pengirim ke penerima. Berbagai upaya pengamanan data telah di upayakan untuk memastikan data hanya dapat diakses oleh orang yang benar, salah satunya adalah dengan cara kriptografi (penyandian) data.

Kriptografi didefinisikan sebagai ilmu untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.

Dalam upaya menjaga kerahasiaan data, kriptografi mentransformasikan data awal (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali. Dengan menggunakan kriptografi ini diharapkan hanya orang yang berkepentingan dan punya kunci yang bisa mengakses data yang dikirimkan.

Kekuatan suatu teknik kriptografi adalah pada kerumitan kunci dan algoritmanya, sehingga pesan yang dikirimkan tidak mudah ditebak oleh orang lain sehingga data yang dikirimkan terjaga kerahasiaannya. Ada berbagai macam jenis algoritma kriptografi yang sekarang ini telah ada dan sedang dikembangkan, namun yang akan dibahas pada penelitian ini adalah algoritma *Exlusive-OR (XOR).* Algoritma XOR adalah salah satu algoritma kriptografi modern dengan meng-XOR kan plainteks (P) dengan kunci (K) menghasilkan cipherteks. Pada penelitian ini akan diuraikan bagaimana mengimplementasikan algoritma *Excusive-OR* menggunakan pesan teks atau data

sederhana ke dalam pemrograman dan menjelaskan bagaimana langkah – langkah proses enkripsi dan dekripsi data sederhana menggunakan algoritma *Exclusive-OR*. Penelitian ini diharapkan dapat digunakan sebagai salah satu rujukan dan panduan dalam memahami proses pengamanan data sederhana menggunakan algoritma *Exclusive-OR,* sehingga dapat meningkatkan keamanan data para pengguna agar tidak mudah untuk diketahui oleh orang lain.

## METODE PENELITIAN

### Pengertian kriptografi

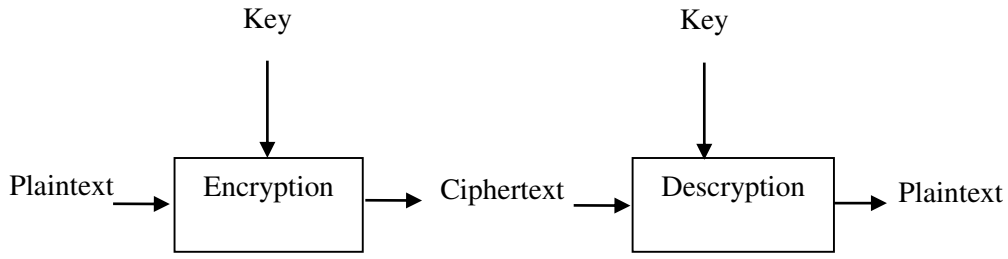
Kriptografi adalah bidang ilmu pengetahuan yang mempelajari pemakaian persamaan matematika untuk melakukan proses penyandian data (Onno, 2000). Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (*encrypt*), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya. Orang yang berhak menerima data akan mengetahui algoritma dan memiliki kunci untuk mengembalikan data sandi menjadi bentuk data aslinya, proses ini disebut dekripsi (*decrypt*). Bentuk data sandi diperlukan pada saat proses penyimpanan atau proses pengiriman data.

Untuk dapat melakukan proses enkripsi dan dekripsi maka pihak pengirim dan penerima harus mengetahui algoritma kriptografi yang digunakan serta memiliki kunci yang sesuai. Tingkat keamanan dari data sandi terhadap upaya proses dekripsi secara paksa oleh orang yang tidak berhak ditentukan oleh kekuatan algoritma yang digunakan dan kerahasiaan kunci. Kekuatan algoritma yang digunakan untuk proses enkripsi dan dekripsi berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit perhitungan dari persamaan matematika yang digunakan maka data sandi semakin aman (Alfred, 1997).

Pemanfaatan kecepatan dan ketelitian dari kerja komputer sangat membantu untuk proses ini. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistribusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapi kunci disimpan dan didistribusikan maka data sandi semakin aman.

Berikut ini adalah istilah-istilah yang berhubungan erat dengan kriptografi :

1. Plaintext
   Pesan yang hendak dikirimkan (berisi data asli).
2. Ciphertext
   Pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi
   Proses pengubahan plaintext menjadi ciphertext.
4. Dekripsi
   Merupakan kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.
5. Kunci
   Suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.




**Gambar 1.** Proses Enkripsi dan Deskripsi Data

**Jurnal Teknovasi**
**Volume 03, Nomor 2, 2016, 23 – 31**
**ISSN : 2355-701X**

**Aspek Keamanan Data**

Kriptografi merupakan salah satu upaya pengamanan data yang dilakukan sehingga data yang bersifat rahasia dan penting tidak dapat diakses oleh pihak-pihak yang tidak mempunyai izin untuk data tersebut. Menurut Stalling, ada beberapa tuntutan yang terkait dengan isu keamanan data yaitu:

1. Kerahasiaan (Confidentiality)
   Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.
2. Otentikasi (Authentication)
   Otentikasi merupakan layanan yang terkait dengan identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (entity authentication) maupun keaslian data dari sistem informasi itu sendiri (data origin authentication). Pada saat mengirim atau menerima informasi kedua belah pihak perlu mengetahui bahwa pengirim dari pesan tersebut adalah orang yang sebenarnya seperti yang diklaim.
3. Integritas data (Data integrity)
   Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data. Tuntutan ini berhubungan dengan jaminan setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian
   dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan.
4. *Nonrepudiation*
   *Nonrepudiation* mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan/informasi. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.

**Perkembangan Kriptografi**

Dalam perkembangannya teknik kriptografi dapat dibagi menjadi 2, yaitu :

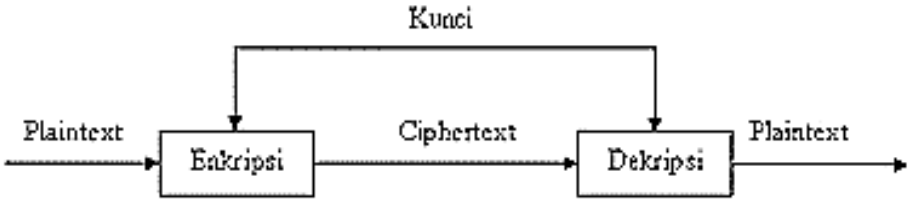
1. Kriptografi klasik
   Merupakan kriptografi yang sudah digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi klasik ini hanya melakukan pengacakan pada huruf A - Z, kriptografi semacam ini sangatlah tidak disarankan untuk mengamankan informasi informasi penting karena akan mudah dipecahkan.
2. Kriptografi modern
   Merupakan teknik kriptografi yang beroperasi dalam mode bit ketimbang mode karakter. Pengoprasi kriptografi ini dalam mode bit berarti semua data dan informasi (kunci, plainteks, maupun cipherteks) semua dinyatakan dalam rangkaian string ataupun bit biner 0 dan 1. Teknik enkripsi dan dekripsinya pun memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plainteks dienkripsi menjadi cipherteks dalam bentuk rangkaian bit, demikian sebaliknya.

**Kriptografi Modern**

Berdasarkan kuncinya algoritma kriptografi modern terbagi 2, yaitu :

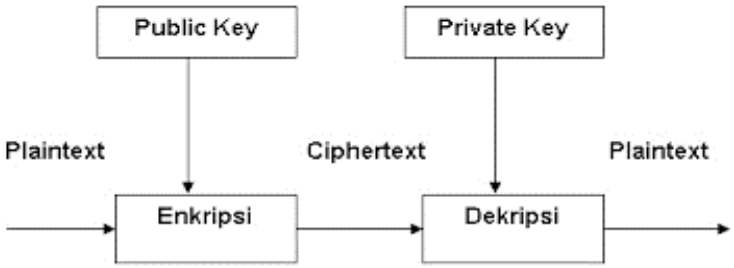
1. Algoritma Simetris
   Algoritma yang menggunakan kunci yang sama untuk melakukan proses enkripsi dan deskripsi.

Jurnal Teknovasi
Volume 03, Nomor 2, 2016, 23 – 31
ISSN : 2355-701X




**Gambar 2.** Proses Enkripsi dan Deskripsi Data pada Algoritma Simetris

2. Algoritma asimetris
   Algoritma yang menggunakan dua buah kunci yang berbeda untuk melakukan proses enkripsi dan deskripsi. Kunci *public* digunakan untuk proses enkripsi data dan kunci *private* digunakan untuk proses dekripsi data.




**Gambar 3.** Proses Enkripsi dan Deskripsi Data pada Algoritma Asimetris

**Operasi Logika *Exclusive OR* (*XOR*)**

Operator biner yang sering digunakan dalam *cipher* yang yang beroperasi dalam mode bit adalah *XO.* Notasi matematis untuk operator *XOR* adalah " ⊕ " . Operator *XOR* diperasikan pada dua bit dengan aturan sebagai berikut:

**Tabel 1.** Aturan Operasi XOR

| A | B | A ⊕ B |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Contoh: 10011 ⊕ 11001 = 01010
hasilnya diperoleh sebagai berikut:

$$\begin{array}{ccccccccccc} 1 & & 0 & & 0 & & 1 & & 1 & & \\ 1 & & 1 & & 0 & & 0 & & 1 & \oplus & \\ \hline 1 \oplus 1 & & 0 \oplus 1 & & 0 \oplus 0 & & 1 \oplus 0 & & 1 \oplus 1 & & \\ 0 & & 1 & & 0 & & 1 & & 0 & & \end{array}$$

**Kriptografi metode *Exclusive OR* (*XOR*)**

Sesuai dengan namanya kriptografi dengan metode *XOR* adalah suatu teknik kriptografi (penyandian) data yang menggunakan prinsip operasi logika XOR dalam proses enkripsi dan deskripsinya.

**Jurnal Teknovasi**
**Volume 03, Nomor 2, 2016, 23 – 31**
**ISSN : 2355-701X**

**Analisis Proses Enkripsi dan Deskripsi metode *XOR***

Algoritma enkripsi menggunakan *XOR* adalah dengan meng-*XOR*-kan plainteks (P) dengan kunci (K) menghasilkan cipherteks (C):

$C = P \oplus K$

Algoritma dekripsi menggunakan *XOR* adalah dengan meng-*XOR*-kan ciphertext (C) dengan kunci (K) menghasilkan plainteks (P):

$P = C \oplus K$

Misalkan kita ingin mengirim pesan (plainteks) "AYO" dengan kunci "8", tahapan penghitungan manualnya adalah sebagai berikut :

1. Buka tabel ASCII, kemudian cari nilai "AYO" dan "8", sehingga kita temukan nilai A = 65, Y=89, O=79, dan 8=56
2. Ubah angka 65, 89, 79, dan 56 kedalam bilangan biner, sehingga kita dapatkan nilai 65=01000001, 89=01011001, 79=0100111, 56=00111000
3. Lakukan proses enkripsi dengan metode *XOR* ($C = P \oplus K$ ) seperti berikut :

   plainteks 01000001 (karakter 'A')
   kunci 00111000⊕ (karakter '8')
   cipherteks 01111001 (karakter 'y')

   plainteks 01011001 (karakter 'Y')
   kunci 00111000⊕ (karakter '8')
   cipherteks 01100001 (karakter 'a')

   plainteks 01001111 (karakter 'O')
   kunci 00111000⊕ (karakter '8')
   cipherteks 01110111 (karakter 'w')
4. Cipherteks dari pesan "AYO" dengan kunci "8" adalah "yaw". Karakter "yaw" didapatkan dari nilai :
   01111001(*biner*)=121(*decimal*)=karakter "y" (tabel ASCII)
   01100001(*biner*)= 97(*decimal*)=karakter "a" (tabel ASCII)
   01110111(*biner*)=117(*decimal*)=karakter "w" (tabel ASCII)
5. Untuk melakukan proses dekripsi dengan metode *XOR* ($P = C \oplus K$ ) seperti berikut :

   cipherteks 01111001 (karakter 'y')
   kunci 00111000⊕ (karakter '8')
   Plainteks 01000001 (karakter 'A')

   cipherteks 01100001 (karakter 'a')
   kunci 00111000⊕ (karakter '8')
   Plainteks 01011001 (karakter 'Y')

   cipherteks 01110111 (karakter 'w')
   kunci 00111000⊕ (karakter '8')
   Plainteks 01001111 (karakter 'O')
6. Plainteks dari pesan "yaw" dengan kunci "8" adalah "AYO". Karakter "AYO" didapatkan dari nilai seperti yang telah dijelaskan pada poin 1 dan 2 diatas.

Jurnal Teknovasi
Volume 03, Nomor 2, 2016, 23 – 31
ISSN : 2355-701X

## HASIL DAN PEMBAHASAN

### Fungsi-fungsi dalam Aplikasi

Aplikasi ini dibangun menggunakan bahasa pemrograman C++, yang dijalankan pada Dev-C++ 5.11. Adapun fungsi-fungsi yang tersedia pada aplikasi ini fungsi enkrisi dan dekripsi sebagai berikut :

1. Fungsi Enkripsi dalam program adalah :

```
void enkripsi()
{
    int ascii, ascii_kunci,i;
    char enkripsi[255];
    cout<<"\nPESAN\n";
    cout<<"-----\n";
    for (i = 0; i <= pjg_pesan-1 ; i++)
    {
        ascii = int(pesan[i]);
        cout<<"ASCII dari karakter "<<pesan[i]<<" adalah :"<<ascii<<"\n";
    }
    cout<<"\nKUNCI\n";
    cout<<"-----\n";
    for (i = 0; i <= pjg_kunci-1 ; i++)
    {
        ascii = int(kunci[i]);
        cout<<"ASCII dari karakter "<<kunci[i]<<" adalah :"<<ascii<<"\n";
    }

    int j= 0 ;
    cout<<"\n\nProses Enkripsi\n" ;
    for (i = 0; i<= pjg_pesan-1; i++)
    {
        ascii = int(pesan[i]);
        ascii_kunci = int(kunci[j]);

        enkripsi[i] = pesan[i] ^ kunci[j];
        cout<<pesan[i]<<" XOR " <<kunci[j]<< " = "<<enkripsi[i]<<"\n";
        j++;
        if (j == pjg_kunci)
        {
            j=0;
        }
    }

    cout<<"\n\nPesan Enkripsi =  ";
    for (i=0; i<=pjg_pesan-1; i++)
    {
        cout<<enkripsi[i];
    }
}
```

2. Fungsi Deskripsi dalam program adalah

```
void dekripsi(void)
{
	int ascii, ascii_kunci, i;
	char enkripsi[255];
	cout<<"\nPESAN\n";
	cout<<"-----\n";
	for (i = 0; i <= pjg_pesan-1 ; i++)
	{
		ascii = int(pesan[i]);
		cout<<"ASCII dari karakter "<<pesan[i]<<" adalah :"<<ascii<<"\n";
	}

	cout<<"\nKUNCI\n";
	cout<<"-----\n";
	for (i = 0; i <= pjg_kunci-1 ; i++)
	{
		ascii = int(kunci[i]);
		cout<<"ASCII dari karakter "<<kunci[i]<<" adalah :"<<ascii;
	}

	int j= 0 ;
	cout<<"\n\nProses Enkripsi" ;
	for (i = 0; i<= pjg_pesan-1; i++)
	{
		ascii = int(pesan[i]);
		ascii_kunci = int(kunci[j]);
		cout<< "\n"<<pesan[i]<<" XOR " <<kunci[j]<< " = ";
		enkripsi[i] = pesan[i] ^ kunci[j];
		cout<< enkripsi[i];
		j++;
		if (j == pjg_kunci)
		{
			j=0;
		}
	}

	cout<<"\n\nPesan Dekripsi =  ";
	for (i=0; i<=pjg_pesan-1; i++)
	{
		cout<<enkripsi[i];
	}
}
```

Jurnal Teknovasi
Volume 03, Nomor 2, 2016, 23 – 31
ISSN : 2355-701X

**Tampilan Aplikasi**

Tampilan aplikasi yang dibuat mencakup menu-menu sebagai berikut :

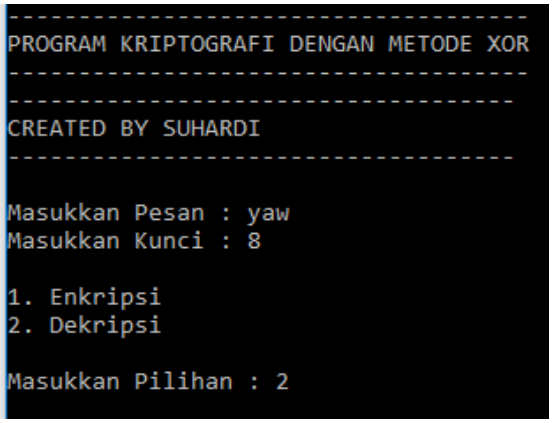
1. Input Enkripsi


**Gambar 4.** Menu Input Proses Enkripsi

2. Hasil Enkripsi

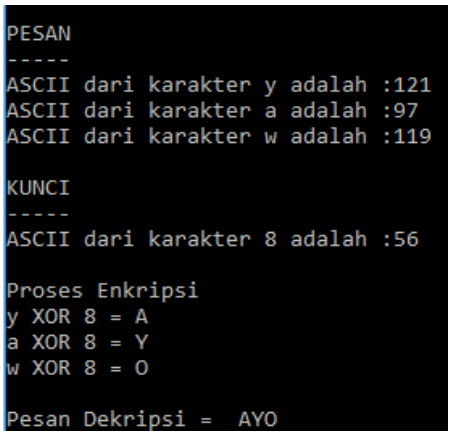

**Gambar 5.** Hasil Proses Enkripsi Dari "AYO"

3. Input Dekripsi




**Gambar 6.** Menu Input Proses Dekripsi

4. Hasil Dekripsi




**Gambar 7.** Hasil Proses Dekripsi Dari "yaw"

## KESIMPULAN

Dari aplikasi yang telah dibuat dapat disimpulkan bahwa kriprografi dengan metode *XOR* melakukan penyandian pada pesan teks dengan mengubah setiap karakter pada pesan menjadi sebuah nilai berdasarkan tabel ASCII. Nilai – nilai tersebut kemudian akan diubah menjadi bilangan biner. Untuk nilai kunci pada metode ini menggunakan kunci simetris, untuk penerapannya kunci yang digunakan sebuah kunci yang merupakan bilangan bulat yang akan diubah menjadi bilangan biner. Masing–masing nilai biner dari hasil perubahan setiap karakter pada pesan akan dioperasikan menggunakan metode XOR dengan bilangan biner dari nilai kunci yang sama. Langkah – langkah ini berlaku pada proses enkripsi dan dekripsi pesan. Metode ini diimplementasikan dengan menggunakan bahasa pemrograman C++ yang tergolong sebagai bahasa pemrograman tingkat menengah (*middle level programming language*). Meskipun tampilan aplikasi sangat sederhana, tetapi aplikasi dapat bekerja cukup baik untuk melakukan proses enkripsi dan deskripsi data. Penulis menyadari bahwa masih banyak terdapat kekurangan dalam aplikasi ini. Untuk pengembangan selanjutnya diharapkan dapat membuat aplikasi kriptografi dengan menggabungkan metode *XOR* dengan berbagai macam metode yang lain dalam proses enkripsi dan deskripsi datanya. Sehingga diperoleh aplikasi yang lebih baik dalam mengamankan data.

## DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi.* Yogyakarta: Andi.

Kromodimoeljo, S. (2009). *Teori dan Aplikasi Kriptografi.* SPK IT Consulting.

Menezes, A. J., Oorshot, P. v., & Vanstone, S. (1997). *Handbook of Applied Cryptography.* Florida, USA: CRC Press LLC.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

Onno, W., & Wahyudi, A. A. (2000). *Mengenal eCommerce.* Jakarta: Elex Media Komputindo.

Sadiki, R. (2012). *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Andi.

Stallings, W. (1999). *Cryptography and Network Security Principles and Practice second edition.* New Jersey, USA: Prentice Hall.

Wirdasari, D. (2008). *Prinsip Kerja Kriptografi dalam Mengamankan Informasi* (Vol. Vol 5). -: Jurnal Saintikom.