IMPLEMENTASI KRIPTOGRAFI ALGORITMA EXCLUSIVE OR KOMBINASI ALGORITMA RC4 SEBAGAI PENGAMANAN DOKUMEN DENGAN MEMANFAATKAN QR-CODE

Nanang Muzaqqi(1210651119)[1], Yeni Dwi Rahayu, S.ST,M.Kom[2].
Fakultas Teknik, Jurusan Teknik Informatika.
Universitas Muhammadiyah Jember
Jln. Karimata No. 49 Telp(0331) 336728, Jember
Email : zaqimz@gmail.com

ABSTRAK

Kriptografi dapat dimanfaatkan untuk mengamankan sebuah dokumen. Pada penelitian ini penulis mengkombinasikan kriptografi klasik dan kriptografi modern dalam bentuk *QR-Code* dengan tujuan untuk memperkuat keamanan informasi. Untuk kriptografi klasik, penulis memilih algoritma *XOR* dikarenakan mudah diimplementasikan dan tidak sulit secara komputasional. Untuk kriptografi modern penulis memilih algoritma *RC4* dikarenakan proses algoritma ini cepat dan kuat. Proses pengamanan diawali dengan proses enkripsi *plaintext* menggunakan algoritma *XOR* untuk menghasilkan *cipherteks XOR*, kemudian *ciphertext XOR* dienkripsi dengan menggunakan algoritma *RC4* yang akan menghasilkan *ciphertext* akhir dan selanjutnya diimplementasikan dalam bentuk *QR-Code*. Untuk proses dekripsi tahap awal ialah menggunakan aplikasi berbasis *mobile Android* dengan cara memindai *QR-Code* pada dokumen dan mengubah informasi *QR-Code* kedalam teks yang isinya berupa *cipherteks* yang selanjutnya didekripsikan dengan menggunakan algoritma *RC4* untuk menghasilkan *ciphertext XOR*. Kemudian *ciphertext XOR* didekripsi lagi menggunakan algoritma *XOR* untuk menghasilkan *plainteks* kembali. *Plaintext* pada penelitian ini adalah nomor surat pada sertifikat. Berdasarkan pengujian beberapa data, aplikasi *mobile* akan menampilkan *report* pada data yang sesuai/ tidak sesuai sehingga kerahasiaan sangat terjaga serta dapat menampilkan otentikasi data dengan cepat dan mudah.

Kata kunci : Kriptografi, Dokumen, Informasi, *QR-Code*, *XOR*, *RC4*, *Plaintext*, *Ciphertext*, Andorid, *Mobile*

I. PENDAHULUAN

Latar Belakang

Seiring perkembangan teknologi dan informasi, manipulasi terhadap gambar, teks, atau berkas-berkas termasuk dokumen atau sertifikat hasil tes, sangat mudah dilakukan. Sehingga dapat memberikan celah untuk melaksanakan praktik pemalsuan dokumen sertifikat. Pemalsuan dokumen umumnya dilakukan dengan cara memanipulasi isi dari dokumen setelah melalui proses *scan* atau membuat dokumen baru dengan desain dan tampilan yang serupa dengan aslinya.

Alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang bermakna. Hal tersebut dapat dilakukan dalam kriptografi dan diimplementasikan dalam bentuk *QR-Code* (*Quick Response Code*)

Kriptografi *Exclusive OR* merupakan algoritma kriptografi klasik, algoritma *Exclusive OR* adalah algoritma enkripsi sederhana dengan menggunakan prinsip operator logika *Exclusive OR*. Cara enkripsinya adalah dengan meng*XOR*-kan *plaintext* dengan kunci sehingga didapatkan *ciphertext*-nya. Keutamaan dari teknik ini adalah mudah diimplementasikan dan operasi *Exclusive OR* tidak sulit secara komputasional namun *Chiper Exclusive OR* benar-benar lemah terhadap serangan plainteks umum. Kelemahan dari algoritma *Exclusive OR* adalah pada saat dienkripsi untuk kedua kalinya, maka pesan awal akan tertayang kembali (Ilyas, 2009). Oleh karena itu perlu dilengkapi dengan mekanisme keamanan tambahan lainnya.

Algoritma *RC4* adalah algoritma kriptografi modern simetris yang termasuk *cipher* aliran (*stream cipher*) karena operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi (Ariyus, 2008). Inti dari enkripsi *RC4* adalah pembangkitan kunci aliran (*keystream*) yang bersifat acak semu (*pseudo random*) (Kromodimoeljo, 2010). Untuk kriptografi modern, penulis memilih algoritma ini dikarenakan proses algoritma ini cepat dan juga kuat.

Berdasarkan uraian di atas, maka dilakukan penerapan kriptografi pengamanan informasi *QR-Code* menggunakan algoritma *Exclusive OR* yang dikombinasikan dengan algoritma *RC4* yang selanjutnya diimplementasikan dalam bentuk *QR-*

Code. Oleh karena itu penulis tertarik untuk mengambil studi kasus penelitian yang berjudul "IMPLEMENTASI KRIPTOGRAFI EXCLUSIVE OR KOMBINASI ALGORITMA RC4 SEBAGAI PENGAMANAN DOKUMEN DENGAN MEMANFAATKAN QR-CODE".

Rumusan Masalah

Berdasarkan permasalahan yang dijelaskan pada latar belakang, maka didapatkan permasalahan sebagai berikut:

1. Bagaimana mengkombinasikan enkripsi algoritma *Exclusive OR* dengan Algoritma *RC4* dan diimplementasikan dalam bentuk *QR-Code*?
2. Bagaimana melakukan dekripsi Algoritma *Exclusive OR* yang dikombinasikan dengan Algoritma *RC4* dalam bentuk *QR-Code* untuk menampilkan keterangan keaslian dokumen?

Tujuan

1. Mampu melakukan enkripsi dan meningkatkan keamanan Algoritma *Exclusive OR* yang dikombinasikan dengan Algoritma *RC4* dan diimplementasikan ke dalam bentuk *QR-Code*.
2. Menghasilkan suatu sistem pemindai untuk membaca data *QR-Code* dan didekripsi dengan menggunakan Algoritma *Exclusive OR* yang dikombinasikan dengan algoritma *RC4* serta dapat menampilkan keterangan keaslian dokumen.

Batasan Masalah

1 Melakukan enkripsi dan dekripsi terhadap beberapa teks informasi pada dokumen sertifikat yang berupa *QR-Code*.
2 Pemindaian *QR-Code* menggunakan *Android versi 4.0.1* keatas dan dilakukan pada media tercetak.
3 Data yang digunakan sebagai input dalam proses pengimplementasian adalah *alfanumerik*.
4 Data yang akan digunakan pada proses kriptografi adalah dalam bentuk teks yang dikodekan dalam *ASCII 128bit*.
5 Algoritma yang digunakan pada penelitian ini adalah Algoritma *Exclusive OR* dan Algoritma *RC4*.
6 Panjang kunci yang digunakan dibatasi sampai dengan 128 bit.
7 Pembangkitan *QR-Code* menggunakan *Library Zxing*
8 Bahasa pemrograman yang dipakai adalah *Java* dan *PHP*.

Manfaat

1. Manfaat bagi penulis sendiri ialah mampu mengkombinasikan Algoritma *Exclusive OR* dengan Algoritma *RC4* yang diimplementasikan dalam bentuk *QR-Code* untuk melakukan deteksi keaslian dokumen sertifikat.
2. Dapat mengurangi atau meminimalisir terjadinya pemalsuan dokumen sertifikat pada suatu lembaga.

II. LANDASAN TEORI

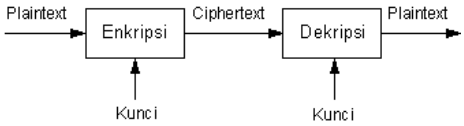
Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani "*cryptos*" artinya "*secret*"(rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti"*secret writing*" (tulisan rahasia). Definisi ini mungkin cocok pada masalalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga tujuan data *integrity*, *authentication* dan *nonrepudiation*. (Satria, 2009).

Algoritma Kriptografi

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan *dechipering*, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *dechiphering*.

Gambar dibawah memperlihatkan skema enkripsi dan dekripsi dengan menggunakan kunci.



Gambar 2.1 Proses Enkripsi dan Dekripsi
(Sumber: Irawan, 2011)

Macam-Macam Algoritma Kriptografi

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern terdiri dari dua bagian (Franindo, 2007):

1. Kriptografi Simetris
2. Kriptografi Asimetris

Algoritma Exclusive OR

Algoritma XOR adalah algoritma enkripsi sederhana dengan menggunakan prinsip operator logika XOR (*Exclusive-OR*). Cara enkripsinya adalah dengan meng-XOR-kan *plaintext* dengan kunci sehingga didapatkan *ciphertext*-nya.

Sebagai contoh Algoritma XOR sederhana diketahui *plaintext* "ILKOM" jika ditulis dalam format ASCII 8-bit menjadi 01001001 01001100 01001011 01001111 01001101 dapat dienkripsi dengan suatu kunci string "AAAAA" (01000001 01000001 01000001 01000001 01000001 dalam format ASCII 8-bit) sehingga didapat hasil sebagai berikut:

01001001 01001100 01001011 01001111 01001101
01000001 01000001 01000001 01000001 01000001 ⊕
00001000 00001101 00001010 00001110 00001100
(BSCRLFSOFF)

dan sebaliknya proses dekripsi:

00001000 00001101 00001010 00001110 00001100
01000001 01000001 01000001 01000001 01000001⊕
01001001 01001100 01001011 01001111 01001101
(ILKOM)

Algoritma RC4

RC4 termasuk ke dalam kode aliran (*stream cipher*) dengan kunci rahasia/kunci simetri (kunci yang sama digunakan untuk proses enkripsi dan dekripsi). Seperti halnya dengan *Vernam Cipher*, inti dari enkripsi RC4 adalah pembangkitan kunci aliran (*keystream*) yang bersifat acak semu (*pseudo random*). Algoritma RC4 terdiri atas 2 bagian yaitu *Key Scheduling algorithm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA) (Mooduto, 2004).

Contoh Enkripsi dengan metode RC4

Untuk menunjukkan bagaimana RC4 bekerja pada tingkat dasar, mari kita *state-array* 4 bit. Hal ini dikarenakan akan sangat sulit menggambarkan proses RC4 secara manual dengan *state-array* 256 bit. Kali ini, kita akan mengenkripsi kata HALO dengan kunci 3123. Pertama, kita menginisialisasi *array* S 4 bit sehingga terbentuk *state-array* S dan *state-array* K sebagai berikut,

Array S

0	1	2	3

Array K

2	5	7	3

Inisialisasi i dan j dengan 0 kemudian dilakukan KSA agar tercipta *state-array* yang acak. Penjelasan iterasi lebih lanjut dapat dijelaskan sebagai berikut:

Iterasi 1

```
i = 0
j = (0 + S[0] + K [0 mod 4]) mod 4
= (0 + 0 + 2) mod 4 = 2
Swap (S[0],S[2])
```

Hasil *Array* S

2	1	0	3

Iterasi 2

```
i = 1
j = (2 + S[1] + K [1 mod 4]) mod 4
= (2 + 1 + 5) mod 4 = 0
Swap (S[1],S[0])
```

Hasil *Array* S

1	2	0	3

Iterasi 3

```
i = 2
j = (0 + S[2] + K [2 mod 4]) mod 4
= (0 + 0 + 7) mod 4 = 3
Swap (S[2],S[3])
```

Hasil

1	2	3	0

Iterasi 4

```
i = 3
j = (3 + S[3] + K [3 mod 4]) mod 4
= (3 + 0 + 3) mod 4 = 2
Swap (S[3],S[2])
```

Hasil *Array* S

1	2	0	3

Setelah melakukan KSA, akan dilakukan PRGA. PRGA akan dilakukan sebanyak 4 kali dikarenakan *plaintext* yang akan dienkripsi berjumlah 4 karakter. Hal ini disebakan karena dibutuhkan 1 kunci dan 1 kali pengoperasian XOR untuk tiap-tiap karakter pada *plaintext*. Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA.

Array S

1	2	0	3

Inisialisasi

```
i = 0
j = 0
```

Iterasi 1

```
i = (0 + 1) mod 4 = 1
j = (0 + S[1]) mod 4 = (0+ 2) mod
4 = 2
swap (S[1],S[2])
```

1	0	2	3

```
K1 = S[(S[1]+S[2]) mod 4] = S[2
mod 4] = 2
K1 = 00000010
```

Iterasi 2

```
i = (1 + 1) mod 4 = 2
j = (2 + S[2]) mod 4 = (2+ 2) mod
4 = 0
swap (S[2],S[0])
```

2	0	1	3

```
K2 = S[(S[2]+S[0]) mod 4] = S[3
mod 4] = 3
K2 = 00000011
```

Iterasi 3

```
i = (2 + 1) mod 4 = 3
j = (0 + S[3]) mod 4 = (0+ 3) mod
4 = 3
swap (S[3],S[3])
```

1	0	2	3

```
K3 = S[(S[3]+S[3]) mod 4] = S[6
mod 4] = 2
K3 = 00000010
```

Iterasi 4

```
i = (3 + 1) mod 4 = 0
j = (3 + S[0]) mod 4 = (3+ 1) mod
4 = 0
swap (S[0],S[0])
```

1	0	2	3

```
K1 = S[(S[0]+S[0]) mod 4] = S[2
mod 4] = 2
K1 = 00000010
```

Setelah menemukan kunci untuk tiap karakter, maka dilakukan operasi XOR antara karakter pada *plaintext* dengan kunci yang dihasilkan. Berikut adalah tabel ASCII untuk tiap-tiap karakter pada *plaintext* yang digunakan.

Tabel 2.5 Kode ASCII untuk setiap karakter *plaintext* yang digunakan

Huruf	Kode ASCII (Binary 8 bit)
H	01001000
A	01000001
L	01001100
O	01001111

Proses XOR dari kunci bisa dilihat pada tabel 2.5
Tabel 2.6 Proses XOR kunci enkripsi dengan *plaintext* pada enkripsi

	H	A	L	O
Plaintext	01001000	01000001	01001100	01001111
Key Cipher	00000010	00000011	00000010	00000010
Ciphertext	01001010 L	01000010 B	01001110 N	01001101 M

Setelah terkirim, pesan yang telah dienkripsi akan didekripsikan. Proses pendekripsian dilakukan dengan proses XOR antara kunci dekripsi yang sama dengan kunci dekripsi dengan *ciphertext* yang dapat dilihat di tabel 2.6 .Tabel 2.6 Proses XOR kunci dekripsi dengan *ciphertext* pada dekripsi

	L	B	N	M
Ciphertext	01001010	01000010	01001110	01001101
Key Cipher	00000010	00000011	00000010	00000010
Plaintext	01001000 H	01000001 A	01001100 L	01001111 O

QR-Code (Quick Response Code)

QR-Code (*Quick Response Code*) merupakan teknik yang mengubah data tertulis menjadi kode-kode 2-dimensi yang tercetak kedalam suatu media yang lebih ringkas. *QR-Code* adalah *barcode* 2-dimensi yang diperkenalkan pertama kali oleh perusahan Jepang *Denso-Wave* pada tahun 1994.

QR-Code dapat menampung data berupa:

1. Angka/Numeri maksimal 7.089 karakter
2. Alphanumerik maksimal 4.296 karakter
3. Bineri maksimal 2.844 byte
4. Kanji / Kana 1.817 karakter
5. Koreksi kesalahan level L = 7%,Level M = 15%,Level Q = 25%,Level H = 30%

Setiap versi simbol *QR-Code* memiliki kapasitas data yang sesuai dengan jumlah data, jenis karakter dan tingkat kesalahan koreksi. Untuk pemeriksaan data dengan kapasitas maksimum ditentukan pada setiap versinya. Untuk versi dan kapasitas data maksimum, maka jumlah data dan modul akan meningkat sehingga simbol *QR-Code* semakin besar. (Rahmawati., Rahman. 2011).

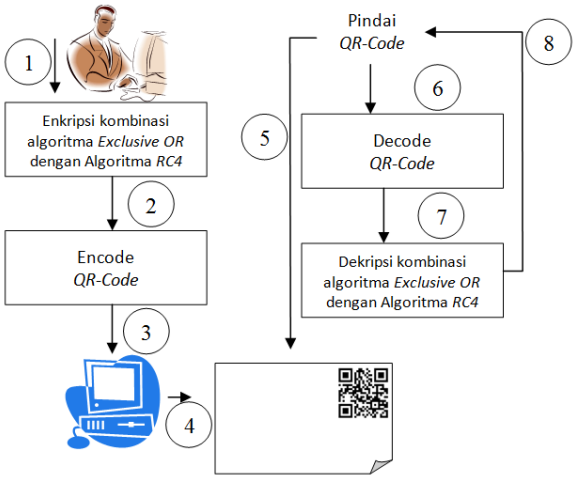
Android

Android merupakan sistem operasi *Mobile* berbasis *kernel* Linux yang dikembangkan oleh Android Inc.

Sejak April 2009, versi *Android* dikembangkan dengan nama kode yang dinamai berdasarkan makanan pencuci mulut dan penganan manis. Masing-masing versi dirilis sesuai urutan alfabet, yakni *Cupcake* (1.5), *Donut* (1.6), *Eclair* (2.0-2.1), *Froyo* (2.2-2.2.3), *Gingerbread* (2.3-2.3.7), *Honeycomb* (3.0- 3.2.6), *Ice Cream Sandwich* 4.0-4.0.4), *Jelly Bean* (4.1-4.3), *KitKat* (4.4-4.4.3), *Lollipop* (5.0) dan *Marsmallow* (6.0). (Safaat, 2016).

III. METODE PENELITIAN

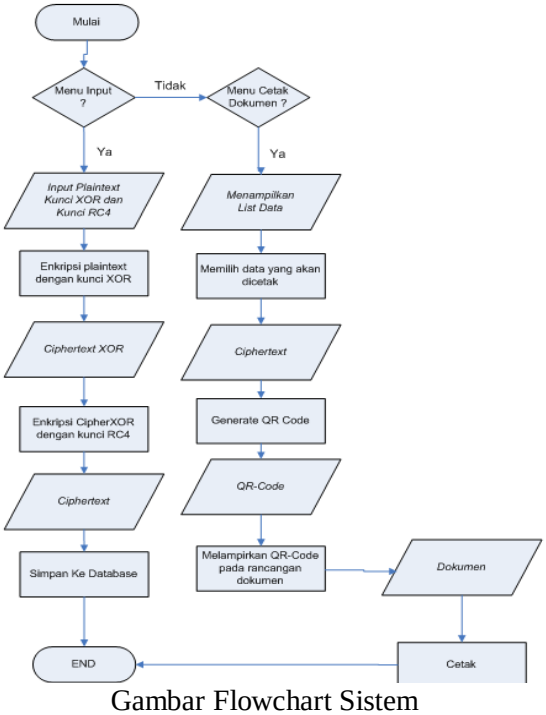
Desain Skema Sistem



Gambar 3.1 Rencana Skema Sistem

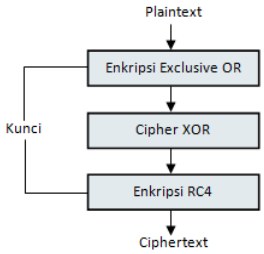
Skema di atas menjelaskan proses pengamanan sertifikat/dokumen dengan menggunakan kriptografi Algoritma *XOR* kombinasi *RC4* dengan memanfaatkan *QR-Code*. Pertama pengguna menginputkan *plaintext* lalu dienkripsi dengan menggunakan algoritma kombinasi XOR dengan RC4 dan di encode ke dalam bentuk QR-Code, setelah itu proses pencetakan dokumen yang sudah disisipi QR-Code. Proses pindai QR-Code sertifikat/dokumen dengan cara scan menggunakan aplikasi, hasil scan berupa ciphertext yang selanjutnya di dekripsi dengan menggunakan algoritma XOR kombinasi RC4 lalu hasil dari dekripsi yang berupa plaintext dan format informasinya akan ditampilkan pada laporan aplikasi.

Flowchart Sistem



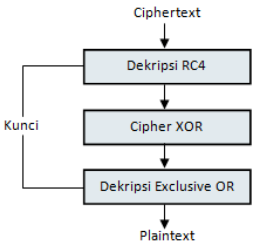
Gambar Flowchart Sistem

Flowchart Enkripsi Kombinasi Algoritma Exclusive OR dengan Algoritma RC4



Gambar Skema Enkripsi kombinasi Algoritma *Exclusive OR* dengan Algoritma *RC4*.

Flowchart Dekripsi Kombinasi Algoritma Exclusive OR dengan Algoritma RC4



Gambar Skema Dekripsi kombinasi Algoritma Exclusive OR dengan Algoritma RC4.

IV. IMPLEMENTASI

Implementasi Antarmuka

Dari Analisis yang sudah dibuat pada bab sebelumnya, kemudian diimplementasikan kedalam sebuah sistem.

Menu Utama Aplikasi

Gambar 4.1 Menu Utama Aplikasi

Form Data Sertifikat

Gambar 4.2 *Form* Data Sertifikat

Laporan Sertifikat/Dokumen

Gambar 4.3 Cetak Dokumen

Hasil Laporan

Gambar 4.4 Bentuk Laporan Sertifikat

Antarmuka Aplikasi Scanner

Gambar 4.5 Menu Utama *Scanner*

V. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan uraian permasalahan dan pembahasan pada bab sebelumnya mengenai penggunaan implementasi kriptografi algoritma *Exclusive Or* kombinasi algoritma *RC4* sebagai pengamanan dokumen dengan memanfaatkan *QR-Code*, maka dapat diambil kesimpulan bahwa :

1. Algoritma *XOR* yang dikombinasikan dengan *RC4* dapat diimplementasikan pada *QR-Code* dan dapat didekripsi.
2. Kriptografi Algoritma Exclusive OR yang dikombinasikan dengan Algoritma RC4 dan diimplementasikan ke dalam bentuk QR-Code pada dokumen dapat mengurangi kecurangan/pemalsuan terhadap dokumen.

Saran

Aplikasi kriptografi ini merupakan aplikasi mobile android yang menggunakan tambahan *library* untuk menghasilkan *QR-Code* dengan *interface* yang sangat sederhana serta algoritma *XOR* yang dikombinasikan dengan *RC4* menghasilkan *ciphertext* yang panjangnya melebihi panjang *plaintext* dan *key*. Penelitian ini masih sangat jauh dari nilai sempurna. Diharapkan akan ada aplikasi kriptografi yang lebih baik untuk pengembangan selanjutnya.

DAFTAR PUSTAKA

Ardiansyah,F. 2011. *Pengenalan Dasar Android Programming*. Universitas Gunadarma Depok

Ariyanto, Y. 2009. *Algoritma RC4 Dalam Proteksi Transmisi Dan Hasil Query Untuk Ordbms Postgresql*. Jurnal Informatika Volume 10, No.1. Hal 53-59. Institut Teknologi Adhi Tama Surabaya.

Ariyus, D. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi. ANDI: Yogyakarta.

Fiansyah, E. 2008. *Implementasi Algoritma Dasar RC4 Stream Cipher dan Pengacakan Plaintext dengan Teknik Dynamic Blocking pada Aplikasi Sistem Informasi Kegiatan Skripsi di Departemen Teknik Elektro*. Skripsi. Universitas Indonesia.

Firmansyah, Eka, R. 2012. *Makalah Sistem Keamanan Jaringan*. Universitas Islam Negri Syarif Hidayatullah Jakarta.

Franindo, A. 2007. *Chiper Blok dengan Algoritma Operasi XOR antar Pecahan Blok*. Jurnal Teknik Informatika ITB. Bandung.

Hoffstein, J., Pipher, J. & Silverman, J.H. 2008. An Intoduction to Mathematical Cryptography. Springer: New York.

Irawan, Calvin. 2011. *Enkripsi Pada QR Code Tiket dengan RSA.* Makalah IF3058 Kriptografi. Institut Teknologi Bandung.

Ilyas, Husni. Enkripsi XOR Pengenalan. Https://komputasi.wordpress.com/2009/01/16/ enkripsi-xor-sekedar-kenal. (diakses 18 Maret 2016).

Kromodimoeljo, S. 2010. Teori dan Aplikasi Kriptografi. SPK IT Consulting: Jakarta.

Mooduto, H.A. 2004. *Enkripsi Data Menggunakan Algoritma RC4.* Jurnal Ilmiah R & B *Volume* 4, Nomor 2. ISSN: 1412-5080. Hal 68.

QR Code.Com. (2010). *About 2D Code*. http://www.qrcode.com/en/index.html. (diakses 16 Februari 2016).

Rachmadi, N. D. 2013. *Kriptografi Korelasi Quick Response Code* (*QR Code*). Jurnal Ilmiah IF2120. Matematika Diskrit. Sem.I. Institut Teknologi Bandung.

Rahmawati, Anita., Rahman, Arif. 2011. *Sietem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64.* Program Studi Sistem Informasi, Universitas Ahmad Dahlan.

Ridwan, F.Z., Santoso, H., Wiseto P.A. 2010. *Mengamankan Single Identity Number (SIN) Menggunakan QR-Code dan Sidik Jari.* Internet Working Indonesia Journal. PT. Telekomunikasi Indonesia.

Safaat, N.H. 2015. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Revisi Kedua. ISBN 978-602-1514-47-4. Informatika Bandung.

Satria, Eko. 2009. *Studi Algoritma Rijndael dalam Sistem Keamanan Data.* Universitas Sumatra Utara.

Suryani, K.N. 2009 *Algoritma RC4 Sebagai Metode Kriptografi*. Jurnal Ilmiah IF2091, Struktur Diskrit. Institut Teknologi Bandung.

Tresnani, Dini Lestari., 2012. *Implementasi Sistem Absensi Menggunakan QR Code Pada Smartphone Berbasis Android.* Teknik Informatika. Institut Teknologi Bandung.

Wikipedia. *QR Code*. http://en.wikipedia.org/wiki/ QR_code. (diakses 15 Maret 2016).