Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume (2) No. 1 Juli 2017
ISSN: 2527-5771/EISSN: 2549-7839
http://tunasbangsa.ac.id/ejurnal/index.php/jurasik

PENGAMANAN ACAKAN BISS MENGGUNAKAN ALGORITMA RSA

Indra Gunawan
STIKOM Tunas Bangsa
Jl. Sudirman Blok A, No.1, 2 & 3 Kota Pematangsiantar, Sumatera Utara 21127
indra@amiktunasbangsa.com

Abstract

BISS scramble method is a method in which description is done before the broadcast frequency signal sent to each TV station. This is done so that the delivery system and a broadcast signal receiving premium can be gated. BISS scramble method combined with RSA (Rivest Shamir Adleman), which later on safety in the delivery and receiving radio frequency signals broadcast video files can be gated and more robust against an attack.

Keywords*: Scramble, BISS, RSA, Frequency, A Broadcast Signal*

Abstrak

Metode acakan BISS merupakan suatu metode dimana pengenskripsisan dilakukan sebelum signal frekuensi siaran dikirim ke masing-masing stasiun TV. Hal ini dilakukan agar sistem pengiriman dan penerimaan signal suatu siaran premium dapat terjaga keamanannya. Metode acakan BISS dikombinasikan dengan algoritma RSA (Rivest Shamir Adleman), yang nantinya keamanan dalam pengiriman dan penerimaan signal frekuensi radio siaran sebuah file dapat terjaga keamanannya dan lebih kuat terhaap suatu serangan.

Kata kunci: Acakan, BISS, RSA, Frekuensi, Signal Siaran

1. PENDAHULUAN

BISS (*Basic Interoperable Scrambling System*) merupakan jenis pengenkripsian yang digunakan untuk mengamankan sebuah video dari suatu sinyal tertentu. *BISS* biasanya berfungsi untuk mengunci beberapa siaran video seperti film-film terbaru yang memiliki hak siar[1].

Seiring dengan kemajuan teknologi, muncullah beberapa *provider* yang menawarkan suatu produk digital-reciever yang mampu menyajikan siaran-siaran premium dan berkualias, baik itu informasi, promosi, perfilman dan olah raga. *Provider* tersebut menawarkan siaran-siaran yang dapat menambah pengetahuan masyarakat. Disamping itu setiap siaran dari sebuah *provider* akan dienkripsi dengan beberapa jenis model acakan, sehingga siaran tersebut sangat mustahil untuk dinikmati oleh masyarakat bila menggunakan digital-reciever biasa atau selain yang ditawarkan oleh provider penyedia. Salah satu jenis acakan yang digunakan adalah acakan *BISS*.

Dengan kemajuan media dapat dijadikan sebagai pendorong untuk kemajuan teknologi yang dapat dikombinasikan untuk memberikan suatu informasi kepada

masyarakat yang memiliki latar belakang yang beragam, sehingga muncullah beberapa produk dari *digital-reciever* yang mampu untuk membuka enskripsi atau acakan dari jenis acakan *BISS*. Dengan ditemukannya deskripsi dari acakan *BISS* tersebut, banyak pula siaran-siaran premium berbayar tersebut dapat disaksikan dengan cuma-cuma (*free*). Mengacu dari hasil deskripsi acakan *BISS* diatas, penelitian ini memfokuskan kepada pengamanan acakan *BISS* dengan Kriptografi, agar pengenskripsian keamanan acakan *BISS* dapat menjadi optimal.

Kemanan merupakan masalah besar dan mengamankan data yang penting sangat penting, sehingga data tersebut tidak dapat disadap atau disalah gunakan untuk tujuan ilegal sehingga merugikan pihak lain. Untuk itulah pemerintah dan lembaga lainnya berusaha mengamankan data mereka sekuat tenaga agar tidak terjadi pembobolan. Biarpun begitu tetap saja ada pihak-pihak yang berusaha membobol itu dengan menggunakan berbagai kunci dan juga metode. Untuk menghindari hal tersebut maka data yang dikirim diubah kedalam data yang tidak dapat dibaca oleh sang pembajak dan kemudian data tersebut diubah kembali kedalam bentuk yang bisa dibaca oleh penerimanya. Teknik dan ilmu untuk membuat data yang tidak dapat dibaca sehingga hanya orang yang berwenang yang mampu membaca data, inilah yang disebut dengan kriptografi [2].

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Ada 4 (empat) tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi, yaitu : [3]

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang mempunyai otoritas atau kunci rahasia untuk membuka/menghapus informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirim melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman dan lain-lain.
4. Non repudiasi, adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan / membua informasi tersebut.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin [4].

Tingkat keamanan algoritma penyandian RSA sangat bergantung pada ukuran kunci sandi tersebut (dalam bit), karena semakin besar ukuran kunci, maka semakin besar pula kemungkinan kombinasi kunci yang bisa dijebol dengan mengecek kombinasi satu persatu kunci atau lebih dikenal dengan istilah *Brute Force Attack*.

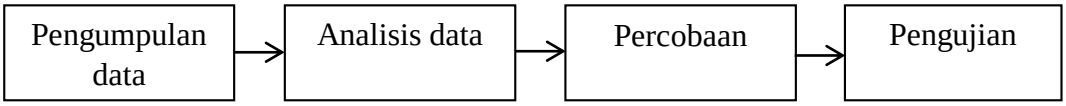
Jika dibuat suatu sandi RSA dengan panjang 256 bit, maka metode *Brute Force Attack* akan menjadi tidak ekonomis dan sia-sia, dimana para *hacker* pun tidak mau/sanggup untuk menjebol sandi tersebut [5].

Algoritma kriptografi RSA dianggap dapat memenuhi tingkat sekuriti yang tinggi. Dengan kombinasi hasil kali 2 (dua) bilangan prima, akan sulit untuk ditemukan dan akan memakan waktu yang sangat lama jika menggunakan *bruteforce*. Kunci RSA dengan panjang 1024 bit akan menghabiskan waktu 1.43 x 10-213 tahun. Waktu yang diperlukan melebihi perkiraan umur alam semesta yang dikalkulasi hanya sekitar 13.75 x 109 tahun [6].

2. METODOLOGI PENELITIAN

Tujuan dari penulisan jurnal ini adalah untuk menganalisis keamanan acakan *BISS* dengan menggunakan algoritma RSA. Pengamanan data yang dihasilkan dari algoritma RSA akan mengacak ulang nilai data/frekuensi siaran yang menggunakan acakan *BISS* menjadi lebih kompleks.

Secara detail, metodologi penelitian ini dirancang seperti diagram blok yang terlihat dalam gambar 3.1.



Gambar 1. Diagram Blok Penelitian

a. *Pengumpulan Data*
   Pengumpulan data dilakukan dengan cara melakukan perekaman data dari beberapa jenis siaran yang terdeteksi menggunakan jenis acakan *BISS* dengan menggunakan *Digital Reciever Matrix Prolink HD Ethernet New Youtube* untuk dijadikan sampel data.
b. *Analisis Data*
   Pada tahapan analisis data ini meliputi pengecekan sampel data/atau signal siaran yang terdeteksi menggunakan acakan *BISS* untuk disesuaikan kembali sebagai formula dengan algoritma RSA.
c. *Percobaan*
   Percobaan dilakukan dengan melihat hasil dari *script* acakan *BISS* yang berikutnya disesuaikan kembali dengan algoritma RSA yang kemudian, barulah dapat dilakukan pengiriman data.
d. *Pengujian*
   Data yang didapat dalam proses perekaman siaran yang terdeteksi menggunakan acakan *BISS* selanjutnya diuji dengan menggunakan algoritma RSA agar keamanan acakannya lebih kuat.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Perekaman data yang dilakukan

Data dari hasil perekaman beberapa video dari frekuensi yang terdeteksi dengan acakan *BISS* dijadikan sebagai sampel untuk dilakukan uji pengamanan

ulang dengan menggunakan algoritma RSA. Berikut ini merupakan tabel dari siaran video yang terekam dan terdeteksi dengan acakan *BISS*.

Tabel 1. Sampel Daftar Siaran Video

No	Frekuensi Video	Siaran Video	Service ID	Key Data BISS
1	3765	HBO	2	2408194562200486
2	3712	Bein Sport	1	1111111111111111
3	3463	Fox Sports	1	1000001012345096
4	3880	Fox Premium Movie	1617	31fcf522aad337d4
5	3880	Fox Chanel	1615	a788f9284604665af
6	3440	HBO Family	906	940d6b0c03a4ea91
7	3920	MetroTV	1618	723923ce5ed9e920
8	3756	SCTV	1619	410c5aa7ab71607c
9	3545	Trans7	0	0240a1e32563b73f
10	3764	SportsTV	0	2468110011975300
11	4086	KompasTV	1	2a2bf5fa53d35177
12	4090	NikeTV	4	71d3a9aac7f61eaa
13	3920	GlobalTV	605	4332e358a8d948c9
14	3920	GlobalTV	606	5a01e944788c3e42
15	4165	MotogpTV	40002	2121aaecaa1212ce
16	4117	CNN Indonesia	0001	acdeab35df9183f3
17	3786	TV One	0001	1a2b3c003c2b1a00
18	3922	Indonesia Network	0002	4544bb00bb445400
19	4186	MNCTV	0001	2233110011332200
20	4186	RCTI	0002	AABB010010BBAA00
21	4186	I-News	0003	0100010010110100
22	4186	Global-TV	0004	1111110011111100
23	4085	IPM1	0001	Aabbcc00ccbbaa00
24	4085	IPM2	0002	1233330022112200
25	4085	IPM3	0003	1212120021212100
26	4085	IPM4	0004	2122230023222100
27	4085	IPM5	0005	1212120021212100
28	4086	IPM6	0006	Aa01bb00bb101100
29	4953	Fox Sports 1	0021	Aabbaaa1aabbaa02
30	4953	Fox Sports 2	0022	3233220022112200
31	4953	Fox Sports 3	0023	Aaaa0100bbbb1000
32	3863	R-TV	0001	1211000022220000

3.2. Analisis penggunaan Algoritma RSA untuk pengamanan acakan BISS

Pada tahapan ini dilakukan pengujian untuk *men-generate* atau mengacak ulang karakter hexa dari acakan *BISS* menggunakan algoritma RSA. Fungsi *men-generate* ulang karakter hexa dari acakan *BISS* secara random adalah untuk

meningkatkan keamanan hasil dari karakter hexa tersebut tanpa harus menentukan variabel *p, q* dan *n* secara manual.

Dari hasil *key* data *BISS* yang terdapat pada tabel 4.1, dijadikan sebagai sampel 16 digit teks bilangan hexa yang dibutuhkan untuk di *generate* ulang menggunakan algoritma RSA.

Menentukan kunci algoritma RSA, Untuk mencari nilai modulus, dibutuhkan 16 (enam belas) digit karakter hexa yang sudah didapatkan dari *key* data *BISS* yang terdapat pada tabel 1.

Input :	16 (enam belas) digit karakter hexa *key* data *BISS*
Proses :	*p* dan *q* bilangan prima yang ditentukan secara *random* (acak) *n = p*q* dimana *n* merupakan nilai modulus, maka $\phi(n)= (p-1) * (q-1)$
output :	n / $\phi(n)$

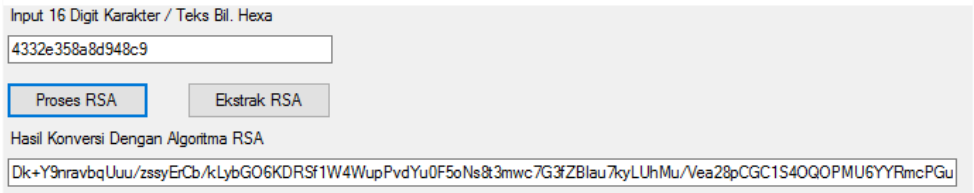
Sampel key data *BISS* yang dijadikan sebagai *input* data adalah *4332e358d948c9*, selanjutnya key data *BISS* tersebut akan dienkripsi ulang dengan menggunakan algoritma RSA. Untuk nilai *p* dan *q* adalah bilangan prima yang ditentukan secara *random* (acak). Maka hasil dari sampel key data *BISS* yang sudah dienkripsi diatas adalah " KuaOAoAgBut23JQ02u2mVSZJdj1RoQ0ReAZ + M3cl9UIrQOYNljG0BFvPb2M + 7gNo0nqveh14P/+ p7zvqp3QFZJyUDKQ9tSCYaffIWVd9pYRqC1t/2Ift9l7OYJeWx9lSfZQq3B5WFM7KF 7GKG0NmiVgoQVAj0Sn + dWG4/78iDTo= "

3.3. Pembahasan

Tampilan rancangan antar muka yang akan muncul.

Gambar 2. Tampilan Antarmuka Aplikasi pengamanan acakan BISS

Pada gambar 2. merupakan tampilan dari aplikasi yang digunakan untuk meningkatkan keamanan sebuah acakan BISS. Karakter ini diisi berdasarkan dari nilai key data *BISS* yang didapat dari perekaman siaran video pada *Receiver Matrix Prolink HD Eithernet New Youtube*. Sebagai sampel data yang sudah didapat adalah terdapat pada tabel 1.



Gambar 3. Input karakter hexa dan proses enkripsi

Setelah memasukkan 16 digit karakter hexa key data *BISS*, sampel datanya adalah "*4332e358a8d948c9*" selanjutnya dilakukan proses enkripsi dengan menggunakan algoritma RSA dengan mengklik tombol Proses RSA. Maka hasilnya akan muncul pada objek Hasil Konversi dengan Algoritma RSA. Hasilnya adalah " KuaOAoAgBut23JQ02u2mVSZJdj1RoQ0ReAZ + M3cl9UIrQOYNljG0BFvPb2M + 7gNo0nqveh14P/+ p7zvqp3QFZJyUDKQ9tSCYaffIWVd9pYRqC1t/2Ift9l7OYJeWx9lSfZQq3B5WFM7KF 7GKG0NmiVgoQVAj0Sn + dWG4/78iDTo= ".

4. SIMPULAN

Kesimpulan yang dapat diambil adalah:

a. Diperoleh suatu model yang dapat meningkatkan keamanan acakan *BISS* dengan menggunakan algoritma RSA.
b. Berdasarkan hasil pengujian aplikasi dengan menggunakan algoritma RSA, dapat memberikan masukan-masukan data secara acak dan otomatis serta menghasilkan daftar nilai kunci yang juga secara acak.
c. Dengan menambahkan algoritma RSA didalam pengacakan. Akan peningkatkan sistem algoritma pengacakan kunci, sehingga tingkat kesulitan untuk pembobolan akan membutuhkan waktu yang lama.
d. Jika tidak menambahkan algoritma RSA didalam sistem acakan diatas, siaran yang terdeteksi dengan acakan BISS sangat mudah untuk dibobol dengan waktu yang singkat, apalagi jika sudah mempunyai kumpulan data acakan (*chain word*).

DAFTAR PUSTAKA

[1] Gani, D. 2013. *Jenis Acakan Dengan System BissKey*. http://mahasiswa.ung.ac.id/521413035/home/2013/9/page/39. Diakses pada tanggal 4 Januari 2016.

[2] Goyal, Kashish & Kinger, Supriya. 2013. *Modified Caesar Ciper for Better Security Enhancement*. International Journal of Computer Applications 73(3) : 0975 – 8887.

[3] Ariyus, Dony. 2008. *PENGANTAR ILMU KRIPTOGRAFI Teori Analisis dan Implementasi*. Yogyakarta : Andi.

[4] Wahyuni, A., 2011. *Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid : Diffie-Hellaman dan RSA*. Majalah Ilmiah Informatika, Vol 2, No. 2.

[5] Wicaksono, P. A., 2013. *Enkripsi Menggunakan Algoritma RSA*, Makalah Ilmu Komputer. Institut Teknologi Bandung.

[6] Rahman, A. 2016. *Analisa Algoritma RSA Pada Penggunaan QR-Code*. Malang : Universitas Muhammadiyah Malang.