Implementasi Algorithma Stream Cipher RC4 dalam Aplikasi Pendataan Alumni STMIK Amik Riau

Syamsurizal Angga Agusta [1], Triyani Arita Fitri A[2]
Program Studi Teknik Informatika STMIK Amik Riau, Jalan Purwodadi Km 10 Panam Pekanbaru
Syamrizal.angga@gmail.com[1], triyani@stmikamikriau.ac.id[2],

Abstrack–Data security systems in the data collection application of alumni STMIK Amik Riau is a very important factor in doing ensuring the rights of access to the data contained in the database. The system currently has a weakness in the system keamannya, where data - stored data vulnerable to SQL Injection attacks and complicate administrator in decrypting data alumni. The weakness may provide a loophole to the parties undesirable to enter into application systems and manipulate data. Under these conditions, the system is implemented keamanann on the application by using cryptographic techniques to protect data stored in the data collection application system STMIK Amik alumni of Riau. The method used is the stream cipher RC4 algorithm, which is used to change the actual data into certain symbols, so that the data will not be understood by the parties that do not have access rights. RC4 stream cipher cryptographic system on a data collection application of alumni STMIK-AMIK Riau, can improve the security of access to the system - unauthorized parties.

Keywords - Algorithms, Stream Cipher, RC4, Data Security, Data Collection Alumni

Intisari—Sistem keamanan data pada aplikasi pendataan alumni STMIK Amik Riau merupakan faktor yang sangat penting dalam melakukan penjaminan hak akses terhadap data-data yang terdapat dalam databasenya. Sistem saat ini memiliki kelemahan dalam sistem keamanannya, dimana data – data yang tersimpan rentan terhadap serangan *SQL Injection* dan menyulitkan administrator dalam mendekripsi data alumni. Kelemahan tersebut dapat memberikan celah kepada pihak-pihak yang tidak diinginkan untuk masuk ke dalam sistem aplikasi dan memanipulasi data yang ada. Berdasarkan hal diatas maka diimplementasikan sistem keamanan pada aplikasi tersebut dengan menggunakan teknik kriptografi untuk melindungi data-data yang tersimpan dalam sistem aplikasi pendataan alumni STMIK Amik Riau. Metode yang digunakan adalah dengan algorithma stream chiper RC4 yang digunakan untuk merubah data yang sebenarnya menjadi simbol-simbol tertentu, sehingga data tidak akan dimengerti oleh pihak-pihak yang tidak memiliki hak akses. Sistem kriptografi stream chiper RC4 pada aplikasi pendataan alumni STMIK-AMIK Riau, mampu meningkatkan sistem keamanan dari akses pihak – pihak yang tidak berkepentingan.

Kata Kunci—Algoritma, Stream Cipher, RC4, Keamanan Data, Pendataan Alumni.

I. PENDAHULUAN

Seiring dengan banyaknya aplikasi, pengguna internet, dan data digital, maka makin banyak juga celah-celah yang terbuka bagi orang-orang yang ingin berbuat jahat. Oleh karena itu, faktor kemanan menjadi suatu hal yang serius dalam semua aplikasi yang ada di internet maupun aplikasi yang berbasis web. Kejahatan yang paling sering terjadi adalah kejahatan terhadap pencurian data atau informasi dari data server melalui aplikasi berbasis web. Ada beberapa faktor yang perlu diperhatikan untuk mencegah serangan melalui web yaitu, faktor perangkat keras, sistem operasi, aplikasi berbasis web, dan psysical tempat penyimpanan server. Pada keamanan aplikasi salah satu metode yang sering digunakan adalah *Algoritma Stream Cipher RC4. Algoritma Stream Cipher*

*RC4*merupakan sebuah algoritma yang termasuk ke dalam bagian dari teknik *kriptografi*, sehingga dengan mengimplementasikan algoritma tersebut dalam sebuah sistem aplikasi, kita dapat merubah data-data penting yang bersifat rahasia menjadi kumpulan simbol-simbol yang tidak dapat dimengerti oleh orang lain. Kelebihan dari algoritma tersebut yaitu, tidak memerlukan waktu lama untuk mengenkripsi ataupun mendekripsi data yang ada, karena algoritma ini termasuk ke dalam algoritma simetris.

Aplikasi pendataan alumni STMIK Amik Riau merupakan sebuah aplikasi berbasis web yang dirancang dengan tujuan untuk mendata setiap alumni yang ada secara cepat, serta mempermudah komunikasi antara alumni dengan intitusi (almamater). Dengan adanya sistem tersebut, diharapkan alumni dapat memperbaharui informasi mengenai data diri mereka secara cepat. Kelemahan yang terdapat dalam sistem keamanan yang ada pada aplikasi saat ini antara lain adalah sulitnya admin dalam mendeskripsikan data akses dan memungkinkan terjadinya serangan *SQL Injection.*

Untuk menjamin keamanan sistem pendataan alumni diperlukan metode yang dapat melindungi data akses alumni ataupun administrator yang akan mengelola sistem nantinya. Upaya tersebut dilakukan untuk memperkuat sistem pengamanan yang ada dalam aplikasi yang akan dirancang, sehingga pihak-pihak yang tidak diinginkan tidak dapat masuk ke dalam sistem aplikasi. Algoritma *Stream Cipher RC4* dipilih untuk melakukan sistem keamanan, karena algoritma ini terbukti dapat mengamankan data dalam beberapa rancangan aplikasi yang ada sebelumnya serta tidak memerlukan waktu lama untuk mengenkripsi ataupun mendekripsi data yang akan diamankan, sehingga tidak memperlambat kinerja dari aplikasi. Tujuan yang ingin dicapai dari penelitian ini adalah mengimplementasikan Algoritma *StreamCipher* RC4 pada aplikasi pendataan alumni STMIK Amik Riau yang memiliki tingkat keamanan yang tinggi.

II. TINJAUAN PUSTAKA

2.1.Definisi Algoritma

Algoritma pada umumnya memiliki beberapa definisi antara lain [1]:

1. Teknik penyusunan langkah-langkah penyelesaian masalah dalam bentuk kalimat dengan jumlah kata terbatas tetapi tersusun secara logis dan sistematis.
2. Suatu prosedur yang jelas untuk menyelesaikan suatu persoalan dengan menggunakan langkah-langkah tertentu dan terbatas jumlahnya.
3. Susunan langkah yang pasti, yang bila diikuti maka akan mentranformasi data input menjadi output yang berupa informasi.

2.2. Kriptografi

Kriptografi (*Cryptography*) berasal dari bahasa yunani, yaitu dari kata *crypto* dan *graphia* yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan pesan secara rahasia [2]. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptopology*. Teminologinya, kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang berbeda [3]. Dari defenisi diatas dapat disimpulkan bahwa kriptografi merupakan suatu teknik yang memiliki keterkaitan dengan hitungan matematis dan memiliki tujuan untuk menjaga keamanan dari sebuah pesan dengan cara menyamarkan pesan asli menjadi simbol-simbol yang tidak dimengerti oleh orang lain.

2.3 Algoritma Stream Chiper RC4

A. Pengertian

RC4 merupakan sistem sandi stream berorientasi byte. Masukkan algoritma enkripsi RC4 merupakan sebuah byte kemudian dilakukan operasi XOR dengan

sebuah byte kunci, dan menghasilkan sebuah byte sandi [4].

B. Penjadwalan Kunci RC4

Sistem sandi RC4 menggunakan state yaitu larik byte berukuran 256 yang terpermutasi dan tercampur oleh kunci. Kunci juga merupakan larik byte berukuran 256. Sebelum melakukan enkripsi dan dekripsi sistem sandi RC4 melakukan inisialisasi terhadap state dengan algoritma sebagai berikut [4]:

```
Input        : Kunci
Output : {S[1], ... ,S[256]}
    For i = 0 → 255 do
       S[i] = i
    End for
    J = 0
    For i = 0 → 255 do
       J = (j + S[i] + Kunci[i mod
    |Kunci|]) mod 256
       Swap (S[i],S[j])
    End for
```

Algoritma diatas dikenal dengan istilah penjadwalan kunci (*key scheduling*) .

C. Enkripsi RC4

State S terinisialisasi oleh penjadwalan kunci setiap byte pada teks asli dikenakan operasi XOR dengan kunci byte untuk menghasilkan byte pada teks sandi. Kunci byte yang digunakan pada enkripsi dibangkitkan dengan memanfaatkan state S. Adapun algoritma untuk enkripsi RC4 dapat dilihat seperti berikut [5]:

```
Input  : P { Stream Teks Asli }
Output : C { Stream Text Sandi }
     I = 0, j = 0 { Bisa diisi nilai
     lain }
     While P masih memiliki byte do
         I = (i+1) mod 256
         J = (j+S[i]) mod 256
         Swap (S[i],S[j])
         K = S[S[i] + S[j]] mod 256
         C = P ⊕ K
     End while
```

D. Dekripsi RC4

Algoritma dekripsi sistem sandi RC4 serupa dengan algoritma enkripsi sistem sandi RC4. Berdasarkan teori mengenai Algoritma Stream Cipher RC4 dapat disimpulkan bahwa untuk melakukan dekripsi menggunakan RC4 diperlukan kunci yang sama pada saat dilakukan proses enkripsi dengan RC4 [4].

2.4 Fungsi Hash

Fungsi hash adalah sebuah fungsi yang masukkannya adalah sebuah pesan dan keluaran sebuah sidik pesan (*message fingerprint*). Sidik pesan sering juga disebut message digest. Fungsi hash dapat digunakan untuk mewujudkan beberapa layanan keamanan jaringan misalnya untuk keutuhan data dan otentikasi pesan [4].

2.5 Fungsi Hash MD5

Fungsi *hash* yang banyak digunakan dalam kriptografi MD5 dan SHA. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit. MD5 dapat diartikan sebagai fungsi yang berfungsi untuk mengubah pesan dengan input apapun menjadi sebuah pesan yang memiliki nilai hash yang bersifat tetap yaitu 128 bit atau setara dengan 32 karakter hexadecimal [5].

2.6 SQL Injection

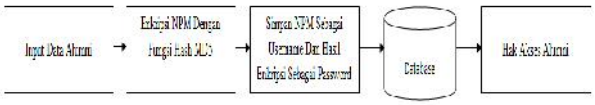
SQL Injection merupakan sebuah istilah yang sudah tidak asing lagi didunia perhacking-an. Istilah *SQL* Injection ini sangat terkenal sekali, bahkan menjadi selebritis dunia hacking yang tidak boleh terlewatkan. *SQL* Injection menjadi naik daun di Indonesia semenjak dibobolnya situs KPU pada pemilu 2004 lalu. *SQL Injection* dapat diartikan sebagai suatu teknik yang dapat digunakan untuk membobol keamanan sebuah website dengan cara menyisipkan karakter-karakter *SQL* tertentu pada perintah *SQL* yang ada dalam sebuah website [6].

III. ANALISA, PERANCANGAN DAN HASIL

A. *Analisa Sistem Keamanan yang digunakan*

Sistem keamanan yang digunakan dalam aplikasi pendataan alumni STMIK Amik Riau saat ini dapat digambarkan sebagai berikut :

1. Proses Penyimpanan Data Login Alumni.



Gambar 1. Proses Penyimpanan Data Login Alumni

2. Proses Login ke Sistem

Gambar 2. Proses Login Ke Sistem

Sistem keamanan pada aplikasi pendataan alumni ini memiliki kelemahan sebagai berikut :

1. Rawan terhadap *serangan sql injection*, yang merupakan serangan dengan cara menyisipkan karakter *SQL* saat melakukan login. Alasanya, data username yang dilakukan saat login langsung divalidasi dengan perintah *SQL*, sehingga dengan menyisipkan beberapa karakter *SQL* kita dapat masuk ke dalam sistem tanpa harus mengetahui password dan username.
2. Pengamanan masih menggunakan *Fungsi Hash MD5*, sehingga kurang efisien jika diterapkan dalam penyimpanan di database. Alasannya, karena *Fungsi Hash MD5* melakukan enkripsi untuk menghasilkan nilai hash yang panjang yang tetap yaitu 32 karakter *hexadecima*l.
3. Kelemahan lain dengan penggunaan *Fungsi Hash MD5*, yaitu tidak memungkinkan untuk melakukan dekripsi terhadap data yang telah terenkripsi, sehingga akan membuat administrator kesulitan dalam melihat data login alumni. Kejadian tersebut dapat menyebabkan administrator tidak memiliki akses penuh terhadap data yang ada di sistem.

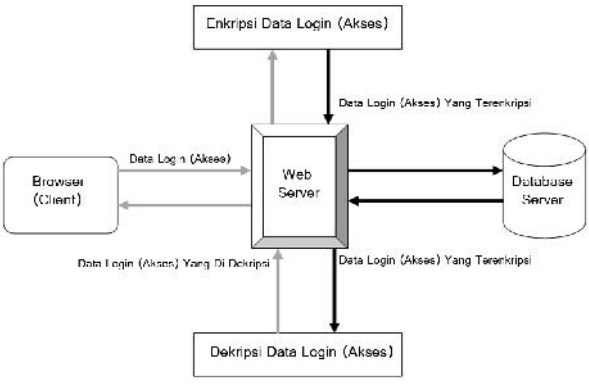
Berdasarkan hal diatas maka untuk meningkatkan sistem keamanan serta melindungi data-data alumni dari pihak-pihak yang tidak diinginkan digunakan sebuah sistem keamanan pada aplikasi pendataan alumni berbasis web, dengan menggunakan metode *Algoritma Stream Cipher RC4.*

B. *Perancangan*

a. *Rancangan Arsitektur Keamanan Aplikasi*

Pada Aplikasi Pendataan Alumni STMIK Amik Riau akan dirancang sistem keamanan dengan menggunakan metode *Algoritma Stream CipherRC4.* Algoritma ini akan diterapkan dalam bahasa pemograman php. Fungsi dari implementasi algoritma ini yaitu untuk mengenkripsi ataupun mendekripsi data akses yang akan digunakan untuk masuk ke sistem, sehingga data akses berada dalam kondisi terenkripsi saat tersimpan di dalam database. Fungsi tersebut dapat mencegah pihak-pihak yang tidak diinginkan untuk masuk ke sistem walaupun pihak tersebut dapat mengakses database.

Adapun gambaran secara umum mengenai keamanan penyimpanan data pada sistem yang akan dirancang yaitu sebagai berikut:

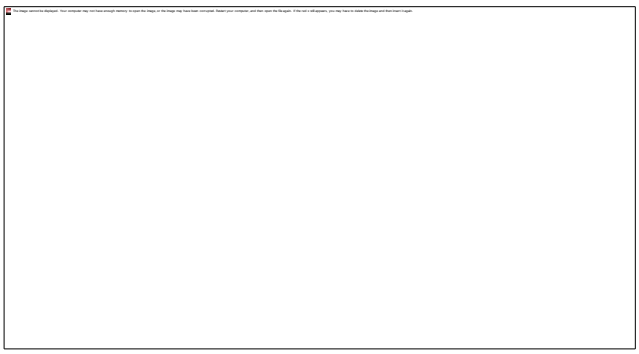


Gambar 3. Rancangan Keamanan Sistem Secara Umum

Dari gambar 3 diatas dapat dijelaskan rancangan system keamanan secara umum pada aplikasi pendataan alumni STMIK Amik Riau sebagai berikut:

1. Client mengirimkan data akses melalui web browser ke web server, karena pemograman php membutuhkan web server untuk menterjemahkan bahasanya.
2. Dalam web server dilakukan proses enkripsi menggunakan *Algoritma Stream Cipher RC4* untuk menghasilkan *Ciphertext* (pesan dalam bentuk simbol-simbol) dari data akses yang diinput.
3. Data login (akses) yang telah terenkripsi disimpan ke dalam database server melalui web server.
4. Untuk mendekripsi data akses atau mengembalikan data akses seperti semula, dilakukan dengan cara memanggil data akses yang telah terenkripsi di database server melalui web server.
5. Setelah itu, dari web server dilakukan proses dekripsi menggunakan *Algoritma Stream Cipher RC4*, kemudian barulah data akses yang telah di dekripsi dikirimkan ke web browser melalui web server.

Sedangkan rancangan sistem keamanan login untuk masuk ke sistem ditunjukan pada gambar 4 dibawah ini .



Gambar 4. Keamanan Login Aplikasi

Uraian dari gambar 4 diatas adalah sebagai berikut :

1. User memasukkan data akses ke dalam sistem, kemudian akan dienkripsi melalui web server.
2. Setelah itu panggil data yang ada di dalam database server sesuai dengan hasil enkripsi.
3. Kemudian tampilkan hasil, jika data yang dimasukkan benar maka user dapat mengakses sistem dan jika tidak user harus memasukkan data lagi hingga benar.

Keungguluan dari penerapan metode Algoritma Stream Cipher RC4 pada aplikasi pendataan alumni ini adalah sebagai berikut:

1. Pihak-pihak yang tidak diinginkan tidak akan dapat masuk ke dalam sistem, walaupun data login dalam database berhasil dibobol. Alasanya, data login dalam database berada dalam keadaan terenkripsi sehingga tidak akan dapat dimengerti oleh orang lain.
2. Terhindar dari serangan *sql injection*, karena saat melakukan login data yang diinput tidak langsung divalidasi dengan perintah *sql*, melainkan diolah terlebih dahulu dengan*Algoritma Stream Cipher RC4.*
3. Lebih menghemat memori penyimpanan dalam database, karena jumlah karakter yang terenkripsi sama dengan jumlah karakter teks asli.
4. Penerapan *Algoritma Stream Cipher RC4* tidak akan memperlambat kinerja aplikasi, karena algoritma ini termasuk ke dalam algoritma simetris yang dapat mengenkripsi dan mendekripsi data secara cepat.

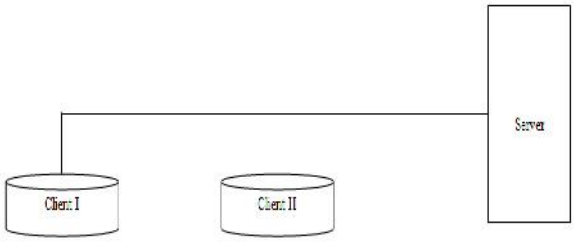
b. Simulasi Pengujian Aplikasi

Simulasi akan dilakukan untuk menguji tingkat keamanan serta kelebihan dari metode Algoritma Stream Cipher RC4 dalam aplikasi pendataan alumni STMIK Amik Riau. Simulasi yang dilakukan terdiri dari :

1. Pengujian menggunakan perintah *sql injection*, pengujian ini akan dilakukan untuk menguji tingkat keamanan sistem dari serangan *sql injection* serta untuk melakukan perbandingan antara sistem yang biasa dengan sistem yang

menerapkan *Algoritma Stream Cipher RC4*.

2. Pengujian dengan aplikasi *wireshark*,pengujian ini akan dilakukan untuk melihat data yang terekam saat client membuka database server yang didalamnya tersimpan database pendataan alumni. Dengan adanya pengujian ini, akan terlihat perbandingan antara sistem yang biasa dengan sistem yang menerapkan *Algoritma Stream Cipher RC4*. Untuk melakukan pengujian ini diperlukan sebuah simulasi jaringan. Adapun gambaran dari simulasi jaringan ini adalah sebagai berikut :



Gambar 5. Simulasi Jaringan

Simulasi dari jaringan diatas menggambarkan dua unit client yang terhubung dengan server. Setiap bagian nantinya akan memiliki peranan yang berbeda untuk menguji keamanan aplikasi dengan adanya implementasi *Algoritma Stream Cipher RC4.* Adapun rincian mengenai peranan setiap bagian dapat dilihat dari tabel spesifikasi berikut:

TABELI
SPESIFIK VIRTUAL JARINGAN

No	Bagian	Peranan
1	Server	Komputer server, yang berfungsi sebagai web dan database server.
2	Client I	Sebagai komputer client, yang berfungsi untuk mengakses database alumni yang berada pada komputer server.
3	Client II	Sebagai komputer client, yang berfungsi untuk merekam paket data pada Komputer I saat Komputer I membuka database

3. Pengujian hasil enkripsi, simulasi ini dilakukan untuk membandingkan jumlah data asli dengandatayang telah terenkripsi.

C. *Hasil Pengujian Sistem*

a. *Hasil Pengujian Dengan SQL Injection*

SQL Injection merupakan teknik yang dapat digunakan untuk dapat masuk ke dalam sistem aplikasi dengan cara menyisipkan fungsi *SQL* saat sistem melakukan proses pengolahan data. Salah satu teknik populer yang termasuk ke dalam *SQL* Injection adalah Bypass Halaman Login. Cara kerja teknik tersebut dapat dilakukan dengan menyisipkan karakter *SQL* saat melakukan proses login. Berikut merupakan hasil pengujian sistem menggunakan cara Bypass Halaman Login.

Gambar 6. Hasil Pengujian *SQL Injection* (Bypass Halaman Login)

Keamanan sistem pada umumnya menggunakan perintah berikut untuk memverifikasi data login.

```
$result = mysql_query (" select * from tabel_login where username = ' $username ' and password = ' $password ' ");
```

Dengan menyisipkan karakter seperti pada halaman login di atas maka perintah yang akan dieksekusi akan menjadi seperti berikut:

```
$result = mysql_query (" select * from tabel_login where username = ' ' Or 1=1 limit 2,1 # ' and password = ' $password ' ");
```

Tanda ‘#’ diatas berfungsi untuk membuang atau mengabaikan perintah sql

yang ada dibelakang tanda '#', sehingga perintah yang akan dieksekusi adalah sebagai berikut:

```
$result = mysql_query (" select * from
tabel_login where username = ' ' Or
1=1 limit 2,1 # ' ");
```

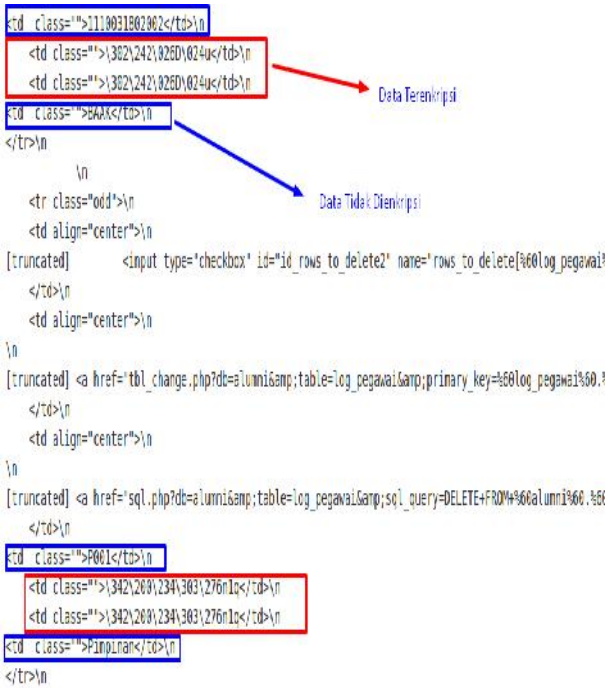
Eksekusi perintah diatas akan menyebabkan seseorang dapat login ke dalam sistem tanpa harus mengetahui username dan password. Salah satu cara yang dapat digunakan untuk mengatasi masalah diatas adalah dengan mengolah data yang digunakan terlebih dahulu sebelum dilakukan proses verifikasi dengan perintah sql. Setelah dilakukan pengujian menggunakan beberapa perintah diatas, dapat diketahui bahwa sistem pendataan alumni memiliki ketahanan terhadap serangan tersebut, karena data login diolah terlebih dahulu dengan menggunakan Algoritma Stream Cipher RC4.

b. Hasil Pengujian Dengan Aplikasi Wireshark

Pengujian ini dilakukan dengan menggunakan konsep virtual jaringan seperti yang telah dibahas pada sub bab sebelumnya. Pada pengujian ini dibutuhkan bantuan aplikasi *VM-Ware* untuk membuat virtual jaringan yang dibutuhkan. Langkah-langkah pengujian yang dilakukan akan dijelaskan sebagai berikut:

1. Client I melakukan akses terhadap database server untuk membuka data login administrator.
2. Client II melakukan proses perekaman terhadap paket data yang diakses oleh komputer client I dengan menggunakan aplikasi wireshark.

Hasil dari pengujian berdasarkan langkah-langkah diatas dapat dilihat dalam gambar sebagai berikut:



Gambar 7. Database Alumni Yang Terekam Oleh Wireshark

Gambar 7 diatas menunjukkan bahwa tabel login pegawai yang berada dalam database alumni dapat direkam dengan menggunakan aplikasi wireshark. Berdasarkan gambar tersebut dapat diketahui perbedaan antara pesan yang tidak dienkripsi dengan pesan yang dienkripsi menggunakan Algoritma Stream Cipher RC4. Pada pengujian diatas terlihat data yang berada dalam keadaan terenkripsi dengan menggunakan Algoritma Stream Cipher RC4 hanya dapat dibaca oleh aplikasi dalam bentuk angka desimal, sehingga tidak akan dapat dimengerti oleh orang lain. Pengujian ini membuktikan bahwa sistem akan tetap aman walaupun database berhasil dibobol oleh pihak yang tidak bertanggung jawab.

c. Pengujian Hasil Enkripsi.

Berikut merupakan perbandingan antara jumlah enkripsi yang dihasilkan oleh Algoritma Stream Cipher RC4 dengan Fungsi Hash MD5.

TABEL II. PERBANDINGAN STREAM CIPHER RC4 DENGAN FUNGSI HASH MD5

Username_ASLI	Password_ASLI	Username_MD5	Password_MD5	Username_RC4	Password_RC4
syamrizal	password1	[illegible]	[illegible]	[illegible]	[illegible]
angga	12345	[illegible]	[illegible]	[illegible]	[illegible]
alumni	alumni password	[illegible]	[illegible]	[illegible]	[illegible]

Berdasarkan tabel II diatas dapat diketahui bahwa hasil enkripsi Algoritma Stream Cipher RC4 lebih baik jika dibandingkan dengan Fungsi Hash MD5, karena Algoritma Stream Cipher RC4 menghasilkan enkripsi yang sama jumlahnya dengan karakter aslinya, sehingga akan lebih efisien jika dilakukan proses penyimpanan dalam database.

IV. KESIMPULAN

Dengan adanya implementasi Algoritma Stream Cipher RC4 dalam rancangan aplikasi pendataan alumni STMIK Amik Riau diperoleh beberapa hasil sebagai berikut:

1. Algoritma Stream Cipher RC4 dapat mencegah terjadinya serangan SQL Injection.
2. Data yang dienkripsi dengan Algoritma Stream Cipher RC4 berada dalam kondisi aman saat tersimpan pada database.
3. Algoritma Stream Cipher RC4 memiliki tingkat efisiensi yang baik dalam penyimpanan data pada database, karena hasil enkripsi yang dihasilkan sama jumlahnya dengan karakter aslinya.

REFERENSI

[1] Suarga, *Algoritma dan Pemrograman*, Andi, Yogyakarta, 2012

[2] Simarmata, Jenner, *Pengamanan Sistem Komputer*, Andi, Yogyakarta, 2006

[3] Arius, Dony *Kriptografi Keamanan Data dan Komunikasi*, Graha Ilmu, Yogyakarta, 2006

[4] Sadikin, Rifki, (2012), *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*, Andi, Yogyakarta, 2012

[5] Inayatullah, Analisis Penerapan Algoritma MD5 untuk Pengamanan Password, Jurnal Ilmiah, STMIK MDP Palembang, 2007

[6] Zam, Efvy, *SQL Injection*, Elex Media Komputindo, Jakarta, 2012