Implementasi Algoritma Kriptografi XXTEA untuk Enkripsi dan Dekripsi Query Database pada Aplikasi Online Test (Studi Kasus : SMK Immanuel Pontianak)

Yuricha[#1], Tursina[#2], Helfi Nasution[#3]
[#]*Program Studi Teknik Informatika Universitas Tanjungpura*
Jl. Prof Dr H. Hadari Nawawi, Kota Pontianak, 78115
[1]esteryuricha@yahoo.com,[2]tursina15@yahoo.com,[3]helfi_nasution@yahoo.com

***Abstrak*— Aplikasi *Online Test* berbasis *web* SMK Immanuel Pontianak digunakan dalam pelaksanaan ulangan tengah semester dan ulangan umum. Aplikasi tersebut tersimpan pada *server* sekolah yang dapat diakses melalui jaringan dalam/LAN dan jaringan luar/*internet*. Namun, sistem keamanan dalam aplikasi tersebut baru memanfaatkan *session browser*, sedangkan aplikasi tersebut memerlukan sistem keamanan yang dapat melindungi data sensitif seperti data soal dan jawaban yang tersimpan pada *database*. Penelitian ini bertujuan untuk meningkatkan sekuritas pada aplikasi *Online Test* tersebut dengan mengimplementasikan algoritma kriptografi. Metode yang digunakan adalah algoritma kriptografi XXTEA (*Corrected Block Tiny Encryption Algorithm*) yaitu algoritma kriptografi yang dapat diimplementasikan pada level keamanan terutama pada aplikasi berbasis *web*. Penerapan algortima kriptografi XXTEA pada aplikasi *Online Test* dilakukan pada *form-form* seperti *form* soal, *form* ujian dan *form login* dengan menambahkan modul enkripsi dan modul dekripsi pada sisi *client* dan sisi *server*-nya. Modul pada sisi *client* dibangun dengan JQuery sedangkan modul pada sisi *server* menggunakan PHP. Transmisi data antara *client* dan *server* menggunakan format pertukaran data JSON. Enkripsi data *query* dari *client* dilakukan sebelum memasuki jaringan dan didekripsi kembali oleh *server* sebelum *query* tersebut diproses. Sedangkan enkripsi data hasil *query database* dilakukan sebelum data ditransmisikan pada jaringan dan didekripsi kembali setelah diterima pada modul *client*. Hasil implementasi algoritma kriptografi pada *form* soal dan *form* ujian, diuji menggunakan *sniffing* terhadap transmisi *query* dari sisi *client* ke sisi *server* dan sebaliknya untuk mendapatkan data yang tertangkap telah terenkripsi atau tidak. Data enkripsi yang tertangkap menggunakan *sniffing*, diuji menggunakan *brute force* untuk memastikan apakah data yang terenkripsi dapat terdekripsi menggunakan *tool brute force*, sedangkan pengujian pada *form login* menggunakan SQL *Injection* dengan memasukkan beberapa variabel injeksi pada *input username* dan *password* di sisi *client* untuk memastikan enkripsi XXTEA memberikan peningkatan sekuritas dalam otentikasi *user*. Kesimpulan dari penelitian ini adalah dengan mengimplementasikan algoritma kriptografi XXTEA pada aplikasi *Online Test* dapat meningkatkan sekuritas yang diujikan secara *online* menggunakan teknik penyerangan terhadap keamanan jaringan seperti *sniffing, brute force*, serta *SQL Injection*.**

***Kata Kunci*—Brute Force, Online Test, Sniffing, SQL Injection, XXTEA**

I. PENDAHULUAN

Aplikasi *Online Test* berbasis web digunakan dalam pelaksanaan ulangan tengah semester maupun ulangan akhir semester di SMK Immanuel Pontianak. Aplikasi tersebut tersimpan pada *server* sekolah yang dapat diakses melalui jaringan dalam/LAN dan jaringan luar/*internet*. Namun, sistem keamanan dalam aplikasi tersebut baru memanfaatkan *session browser*, sedangkan aplikasi tersebut memerlukan sistem keamanan yang dapat melindungi data sensitif seperti data soal dan jawaban yang tersimpan pada *database*.

Database yang digunakan dalam menampung data pada aplikasi *Online Test* juga hanya memanfaatkan keamanan yang telah dimiliki oleh MySQL, sementara pengamanan *database* pada saat proses transmisi merupakan syarat mutlak yang harus dipenuhi agar tidak terjadi penyadapan, pencurian, modifikasi maupun perusakan data oleh orang-orang yang tidak berwenang. Aplikasi *Online Test* yang dapat diakses secara *public* dan *private* tidak dapat hanya mengandalkan fasilitas standar yang disediakan oleh *service* seperti MySQL. Aplikasi *Online Test* memerlukan pengamanan ekstra terutama dalam pengiriman data dari dan ke *database*.

Pengamanan pada data dapat dilakukan pada beberapa level keamanan seperti keamanan sistem operasi, keamanan sistem manajemen *database*, keamanan fisik, keamanan jaringan dan keamanan dari segi manusia. Algoritma kriptografi XXTEA (*Corrected Block Tiny Encryption Algorithm*) merupakan salah satu metode kriptografi yang dapat diimplementasikan pada level keamanan jaringan yang dapat dilakukan untuk enkripsi dan dekripsi transmisi *query database*.

Algoritma kriptografi XXTEA memiliki keunggulan dalam enkripsi data *query* dari *client* yang dilakukan sebelum memasuki jaringan dan di-dekripsi kembali oleh *server*

Submitted 11-01-2017; Revised 11-01-2017; Accepted 11-01-2017

sebelum *query* tersebut diproses dalam *database*. Oleh karena itu, aplikasi *Online Test* di SMK Immanuel Pontianak dapat menggunakan algoritma kriptografi XXTEA sebagai pendukung sekuritas untuk enkripsi dan dekripsi *query database*.

II. URAIAN PENELITIAN

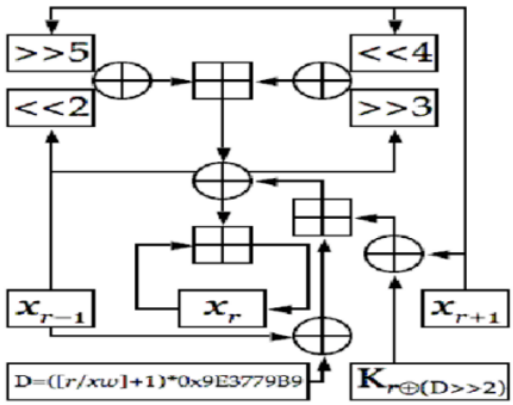
Penelitian menggunakan algoritma kriptografi bukanlah penelitian pertama yang pernah dilakukan, peneliti Radityo Basith dari Universitas Telkom menganalisis dan mengimplementasikan algoritma kriptografi yang serupa dengan penelitian ini yaitu XXTEA untuk transmisi hasil dan *query database* yang dilakukan pada sisi *server* menggunakan *Microsoft Access* 2007 dan pada sisi *client*. Pada penelitian tersebut, modul enkripsi/dekripsi ditambahkan untuk peningkatan keamanan data selama ditransmisikan dijaringan. Keamanan yang ditingkatkan diuji menggunakan serangan keamanan seperti *sniffing* dan SQL *Injection* [1].

Pada penelitian yang dilakukan oleh Siti Mariyam dari Universitas Narotama Surabaya, studi literatur dilakukan dengan mempelajari sistem pengamanan data yang dibangun dalam bentuk aplikasi yang dapat melakukan enkripsi menggunakan algoritma RC4. Pengujian yang dilakukan terhadap *plaintext* dan juga *file* yang dienkripsi dan hanya dapat didekripsi menggunakan aplikasi yang dibuat dalam penelitian tersebut [2].

Studi literatur juga dilakukan dengan melihat referensi terhadap penelitian yang dilakukan oleh Mohamad Firda Fauzan. Dalam penelitian tersebut, pengamanan dilakukan terhadap transmisi hasil dan data *query* basis data dengan cara enkripsi/dekripsi data yang melewati jaringan menggunakan algoritma RC4 [3]. Implementasi pengamanan tersebut dilakukan dengan membangun sebuah perangkat lunak berbasis *web* yang ditempatkan pada komputer *client* untuk mengakses data pada komputer *server* dengan DBMS-nya adalah SQL *Server* 2005.

Pemilihan XXTEA sebagai alat dalam penelitian ini juga didukung setelah melakukan studi literatur terhadap analisis yang dilakukan oleh Khandar William yang memaparkan mengenai TEA, XTEA, dan XXTEA serta sejarah perkembangan hingga menjadikan XXTEA menjadi pilihan utama dan terbaik diantara TEA dan XTEA [4].

Letak perbedaan penelitian ini dengan penelitian lainnya adalah algoritma kriptografi yang digunakan yaitu XXTEA yang diimplementasikan langsung pada aplikasi *Online Test* yang telah digunakan di SMK Immanuel Pontianak. Enkripsi dan dekripsi dilakukan terhadap *query database* pada sisi *server* dan sisi *client*. Teknik pengujian yang digunakan adalah *sniffing*, *brute force* dan SQL *Injection*.



Gambar. 1. Cara Kerja Algoritma XXTEA.

A. XXTEA

XXTEA (*Corrected Block Tiny Encryption Algorithm*) merupakan turunan dari *Block* TEA yang beroperasi dengan ukuran blok berkelipatan 32 *bit* dan panjang kunci 128 [5]. XXTEA tidak memiliki batas ukuran blok, sehingga XXTEA dapat digunakan untuk mengenkripsi satu buah pesan tanpa memerlukan mode operasi *cipher*.

Algoritma XXTEA didesain oleh Roger Needham dan David Wheeler dari Laboratorium Komputer Cambridge. XXTEA juga merupakan algoritma enkripsi efektif yang mirip dengan DES yang dapat digunakan untuk aplikasi *web* yang membutuhkan keamanan. Penggunaan algoritma ini memungkinkan perubahan dari *plaintext* akan mengubah sekitar setengah dari *ciphertext* tanpa meninggalkan jejak dimana perubahan berasal.

XXTEA beroperasi pada blok yang berukuran tetap yang merupakan kelipatan 32 *bit* dengan ukuran minimal 64 *bit*. Jumlah dari putaran lengkap bergantung pada ukuran blok, tetapi terdapat minimal 6 (bertambah hingga 32 untuk ukuran blok yang lebih kecil). Algoritma ini menggunakan lebih banyak fungsi pengacakan yang menggunakan kedua blok tetangganya dalam pemrosesan setiap kata dalam blok seperti yang terlihat pada Gambar 1 [6].

XXTEA banyak diaplikasikan ke perangkat-perangkat elektronik *mobile* seperti *handphone* karena proses enkripsi dan dekripsinya tidak memakan *resource* yang terlalu berat.

B. Query

Query merupakan bahasa SQL (*Structured Query Language*) yang ditampilkan dalam bentuk visual, yang dapat digunakan untuk melihat, memodifikasi, dan menganalisa data dengan berbagai jalan yang berbeda. *Query* juga merupakan suatu *extracting* data dari suatu database dan digunakan untuk pengolahan data selanjutnya [7].

Query digunakan untuk menampilkan data yang didapat dari penggabungan beberapa tabel menjadi satu tampilan *datasheet*. *Query* dapat juga digunakan sebagai sumber data (*record source*) untuk *object form* dan *report*.

C. Online Test

Online Test atau tes berbasis komputer (*Computer Based Test*) merupakan tes yang diselenggarakan dengan menggunakan komputer [8]. Karakteristik dari tes ini sama dengan tes secara konvensional yaitu menggunakan satu perangkat tes untuk beberapa peserta dengan panjang tes yang sama (*fixed test length*). Perbedaan antara tes berbasis komputer dan tes konvensional terletak pada teknik penyampaian setiap butir soal yang tidak lagi menggunakan kertas (*paperless*), baik untuk naskah soal maupun lembar jawaban. Sistem penilaian dilakukan secara langsung oleh komputer. *Online Test* dapat dilakukan dengan menggunakan komputer sebagai media dan jaringan *internet*.

Korespondensi : Yuricha

III. PERANCANGAN DAN HASIL

A. *Metodologi Penelitian*

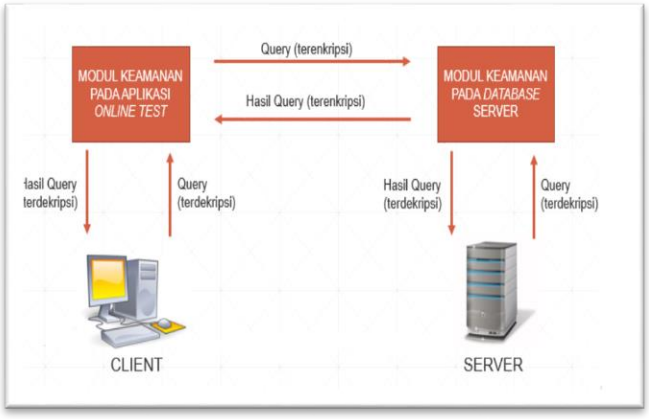
Langkah-langkah penelitian yang dilakukan dapat dilihat pada Gambar 2.

Gambar. 2. *Flowchart* Penelitian.

Flowchart penelitian merupakan gambaran tahapan penelitian yang dimulai dari studi literatur, analisis kebutuhan, pemodelan metode, pengembangan aplikasi, implementasi, pengujian. Melalui tahap pengujian akan diketahui apakah hasil implementasi telah sesuai dengan rancangan atau tidak. Setelah itu dilakukan penarikan kesimpulan.

B. *Pemodelan Metode*

Pemodelan metode dengan menggunakan algoritma kriptografi XXTEA terhadap transmisi hasil dan *query database* dapat dilihat pada Gambar 3.



Gambar. 3. Pemodelan Metode Algoritma XXTEA.

Enkripsi dilakukan selama data ditransmisikan dalam jaringan. Enkripsi dilakukan sebelum data memasuki jaringan dan didekripsi kembali oleh *database server* sebelum *query* diproses dan begitu juga pada saat *query* diterima oleh *client*. Penerapan algoritma kriptografi XXTEA dilakukan dengan menambahkan modul enkripsi dan dekripsi pada *client* dan *server*.

Modul keamanan pada aplikasi *Online Test* di *code* menggunakan bahasa PHP yang dilengkapi dengan AJaX dan JQuery. Format pertukaran data dari *client* ke *server* dan sebaliknya menggunakan JSON. Data yang dibawa menggunakan JSON adalah data yang terenkripsi baik *query* maupun hasil *query* dari *database*.

C. *Pengembangan Aplikasi*

Pada modul *client*, terdapat dua proses besar yaitu *login* pada *form login* dan eksekusi *query* pada *form* soal dan *form* ujian. Proses eksekusi *query* juga dibedakan menjadi dua yaitu *query* yang melakukan *retrieve* data dan *query* yang tidak melakukan *retrieve* data. Dekripsi yang dilakukan terhadap hasil *query database* yang ditransmisikan dari *database server* seperti pada Gambar 4.

Gambar. 4. Alur Enkripsi-Dekripsi pada *Form* Soal.

Pada modul *server*, *server* melakukan dekripsi terhadap *request* yang dilakukan *client* kemudian hasil yang telah diproses dalam *database* akan dienkripsi sebelum dikirimkan kembali ke *client*. Enkripsi dan dekripsi pada *client* dilakukan menggunakan bahasa PHP menggunakan pemanggilan fungsi xxtea.php. *Query* yang dienkripsi berupa hasil eksekusi CRUD (*Create*, *Read*, *Update*, *Delete*) sebagai *response* terhadap *client*.

D. *Hasil Pengujian*

Pengujian dilakukan untuk memastikan bahwa implementasi telah sesuai dengan tujuan pembuatannya. Proses enkripsi terjadi pada saat sebelum *query* dikirimkan oleh *client* ke *server database* dan pada saat sebelum hasil *query* dikirimkan kembali oleh *server* ke *client*. Pengujian dilakukan dengan menguji pengimplementasian algoritma kriptografi XXTEA terhadap *sniffing* pada ketiga *form* yang diteliti, *brute force* pada hasil enkripsi algoritma kriptografi yang ditangkap menggunakan aplikasi *sniffing* dan SQL *Injection* pada *form login* ke *database* secara langsung.

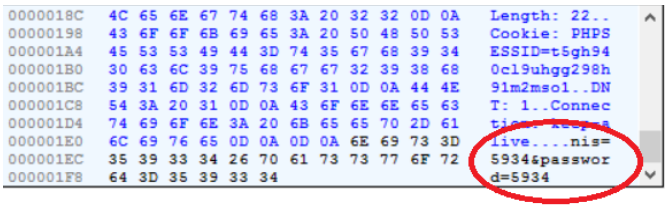
D.1 Hasil Pengujian Sniffing

Pengujian terhadap *sniffing* dilakukan dengan memanfaatkan aplikasi *Fiddler* untuk memonitor/menangkap transmisi hasil dan *query database*. Pengujian dilakukan untuk memastikan bahwa hasil dan *query database* terenkripsi selama *client* dan *server* berada dalam jaringan.

Setelah penggunaan fungsi enkripsi XXTEA dalam *form login*, dapat dilihat pada Gambar 5 parameter yang menjadi masukan *client* dalam keadaan terenkripsi ketika dikirimkan

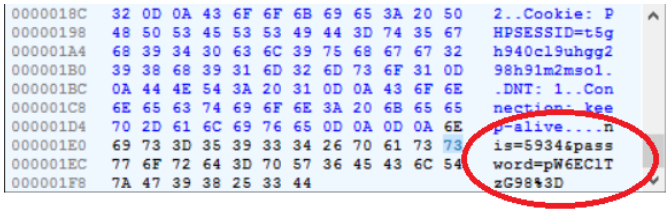
Korespondensi : Yuricha

ke *server* untuk autentikasi.



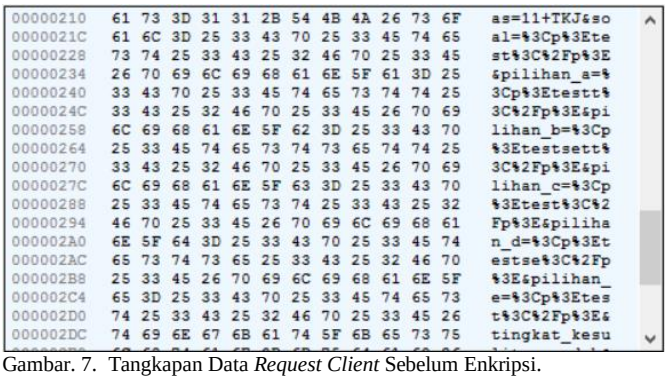
Gambar. 5. Tangkapan Data *Form Login* Sebelum Enkripsi.

Hasil *query* yang dikirimkan oleh *server database* ke *client* juga dalam keadaan terenkripsi seperti terlihat pada Gambar 6.



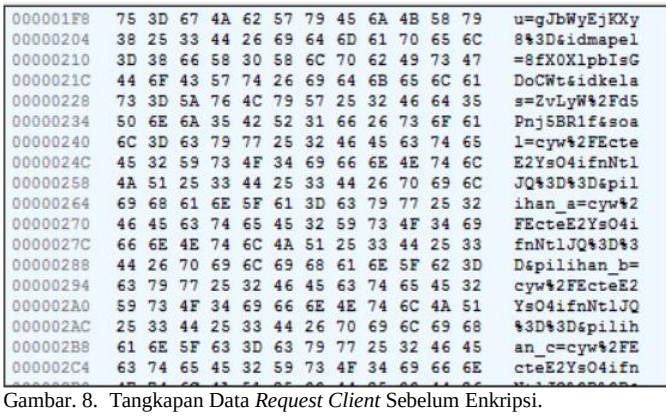
Gambar. 6. Tangkapan Data *Form Login* Setelah Enkripsi.

Hasil pengujian terhadap *sniffing* juga dilakukan pada *form* soal, soal yang dimasukkan oleh guru, masih terbaca langsung melalui *capture* paket data menggunakan *Fiddler* seperti pada Gambar 7.



Gambar. 7. Tangkapan Data *Request Client* Sebelum Enkripsi.

Setelah modul *client* diberikan enkripsi sebelum data ditransmisikan, paket data yang tertangkap menggunakan *Fiddler* telah terlihat seperti pada Gambar 8.



Gambar. 8. Tangkapan Data *Request Client* Sebelum Enkripsi.

D.2 Hasil Pengujian Brute Force

Pengujian aplikasi terhadap *brute force* dilakukan terhadap hasil enkripsi yang tertangkap melalui *Fiddler*. Hasil enkripsi kemudian diujikan terhadap *brute force* menggunakan aplikasi Wfuzz. Wfuzz dijalankan dengan menggunakan *Command Prompt Windows*. *Brute force* yang dilakukan dengan menggunakan metode *by-wordlist* sehingga data yang terenkripsi diserang menggunakan *brute force* sesuai dengan data *dictionary* yang telah didefinisikan.

Pengujian *brute force* juga dilakukan terhadap aplikasi secara langsung yaitu melalui serangan dengan melakukan komputasi yang dicoba satu-per-satu. Hal ini memiliki peluang bagi pihak yang tidak berwenang untuk membobol hasil enkripsi menggunakan algoritma kriptografi XXTEA. Namun untuk dapat membobol hasil enkripsi tersebut, diperlukan waktu yang relatif lama. Algoritma kriptografi XXTEA menggunakan kelipatan blok 32 *bit* dengan minimum 64 *bit* sehingga melalui perhitungan matematis diperlukan waktu 4,2 x 10^9 tahun untuk data 32 *bit* untuk mencoba semua kemungkinan yang mungkin menjadi hasil dari enkripsi yang ter-*capture* melalui *sniffing*.

D.3 Hasil Pengujian SQL Injection

Pengujian aplikasi *Online Test* terhadap SQL *Injection* difokuskan pada *form login* yang menjadi pintu utama untuk dapat memasuki sistem aplikasi *Online Test* dan digunakan untuk autentikasi pengaksesan *Online Test* apakah sebagai guru, siswa maupun staff TU. Pengujian dilakukan pada *textbox input username* dan *password* pada *form login* pada halaman aplikasi yang diakses pertama kali untuk otentikasi *user*.

Pengujian SQL *Injection* dengan secara langsung memasukkan perintah injeksi, sehingga menghasilkan dua tabel yaitu Tabel 1 dan Tabel 2 yang membandingkan serangan SQL *Injection* terhadap *form login* ketika tidak menggunakan algoritma kriptografi XXTEA dan ketika menggunakan algoritma kriptografi XXTEA.

Tabel 1 Pengujian SQL *Injection* Sebelum Enkripsi

No	Variabel SQL *Injection*	Hasil
1	‘or 1=1#	Berhasil *Login*
2	‘’or 1=1-	Gagal *Login*
3	‘or’’a’=’a’#	Gagal *Login*
4	‘or ‘x’=’x’#	Berhasil *Login*
5	‘or 0=0#	Berhasil *Login*
6	‘or’’a’=’a’	Gagal *Login*
7	‘or 0=0 #	Berhasil *Login*
8	‘or 0=0 --	Berhasil *Login*
9	admin’ or ‘x’=’x	Berhasil *Login*
10	1' or '1' = '1	Berhasil Login

Tabel 2 Pengujian SQL *Injection* Setelah Enkripsi

No	Variabel SQL *Injection*	Hasil
1	‘or 1=1#	Gagal Login
2	‘’or 1=1-	Gagal Login
3	‘or’’a’=’a’#	Gagal Login
4	‘or ‘x’=’x’#	Gagal Login
5	‘or 0=0#	Gagal Login
6	‘or’’a’=’a’	Gagal Login
7	‘or 0=0 #	Gagal Login
8	‘or 0=0 --	Gagal Login
9	admin’ or ‘x’=’x	Gagal Login
10	1' or '1' = '1	Gagal Login

Korespondensi : Yuricha

IV. KESIMPULAN/RINGKASAN

Berdasarkan hasil dan analisis terhadap implementasi algoritma kriptografi XXTEA pada aplikasi Online Test di SMK Immanuel Pontianak, dapat disimpulkan bahwa :

1. Implementasi algoritma kriptografi XXTEA meningkatkan sekuritas pada aplikasi *Online Test* di SMK Immanuel Pontianak dengan diujikan pada *server* secara *online* menggunakan *sniffing*, *brute force* dan SQL *Injection*.
2. Pengujian menggunakan *sniffing* terhadap paket-paket data yang ditangkap membuktikan bahwa tangkapan informasi yang dilakukan dengan aplikasi *Fiddler* pada *form* soal, *form* ujian dan *form login* terenkripsi.
3. Pengujian menggunakan *brute force* memungkinkan untuk membobol enkripsi yang telah diimplementasi pada aplikasi, namun memerlukan waktu yang relatif lama karena XXTEA beroperasi pada blok 32 *bit* dengan minimum bit adalah 64 *bit*.
4. Pengujian dengan menggunakan SQL *Injection* menghasilkan tabel perbandingan ketika variabel SQL *Injection* dimasukkan pada aplikasi sebelum dan setelah dienkripsi terutama pada *form login* aplikasi *Online Test* untuk otentikasi *user*.

DAFTAR PUSTAKA

[1] Basith, Radityo. 2010. *Analisis dan Implementasi Algoritma Kriptografi XXTEA untuk Enkripsi dan Dekripsi Transmisi Query serta Hasil Query Basis Data*, Jurnal Fakultas Teknik Informatika Universitas Telkom.

[2] Mariyam, Siti. 2008. *Aplikasi Sistem Pengamanan Data dengan Metode Enkripsi menggunakan Algoritma RC4*. Ejurnal.

[3] Fauzan, Mohamad Firda. 2008. *Pengamanan Transmisi Hasil dan Data Query Basis Data dengan Algoritma Kriptografi RC4*. Informatika.

[4] William, Khandar. 2009. Studi Mengenai Tiny Encryption Algoritm (TEA) dan Turunan-turunannya (XTEA dan XXTEA). Informatika.

[5] Yarrkov, Elias. 2010. *Crypanalysis of XXTEA*. http://eprint.iacr.org/2010/254.pdf.

[6] Rankly. 2012. *Best Cipher of All Time*. https://rankly.com/list/best-cipher-off-all-time.

[7] Paendong, Jovi. 2014. *Pengertian dan Fungsi JQuery*. http://cyber-cre4tive.blogspot.co.id/2014/04/pengertian-dan-fungsi-jquery.html.

[8] Suprananto. *Tes Berbasis Komputer (Computer Based Test)*. http://www.suprananto.org/index.php/welcome/artikel/10/Tes-Berbasis-Komputer-Computer-Based-Test.

Korespondensi : Yuricha