 ISBN 978-602-18615-7-8

TEKNIK PENGAMANAN KUNCI JAWABAN DENGAN METODE ENKRIPSI

Reza Andrea[1]
Teknik Informatika, STMIK Widya Cipta Dharma[1]
Jl. Prof.M. Yamin No.25, Samarinda, 75123
E-mail : reza@bibirdesign.com[1]

Abstrak

Ujian dalam bentuk multiple choice (pilihan ganda) yang telah berbasis komputer, pada umumnya memiliki database berupa tabel bank soal. Dimana di dalam tabel bank soal tersebut terdapat soal ujian dan kunci jawaban. Keamanan database bank soal sangat rentan dari kebocoran soal dan kunci jawabannya. Teknik pengamanan soal ujian dan kunci jawaban menggunakan metode enkripsi merupakan teknik yang kurang tepat apabila penggunaaanya tidak maksimal. Hal ini dikarenakan karakter untuk kunci jawaban hanya 1 karakter dan mempunyai range hanya dari huruf A sampai E atau F.

***Kata Kunci*: Pengamanan Kunci Jawaban, Soal Ujian, Enkripsi**

I. PENDAHULUAN

Ujian yang telah terkomputerisasi dalam bentuk soal pilihan ganda pasti memiliki bank soal serta kunci jawaban. Bank soal dan kunci jawaban tersebut dapat tertanam di dalam *script* aplikasi dan dapat juga berupa database bank soal baik online maupun tidak.

Database yang berisi data soal ujian maupun kunci jawaban, pastinya akan menjadi sasaran penyusup yang ingin mengetahui informasi yang ada di dalamnya.

Dari banyaknya teknik pengamanan database, pengamanan database bank soal dengan metode enkripsi adalah jalan terakhir pengamanan database yang telah dimasuki oleh penyusup. Teknik pengacakan teks soal ujian dan kunci jawaban menjadi *chiper* teks adalah teknik yang tepat agar informasi tidak mudah dibaca dan dibocorkan oleh penyusup.

Tabel 1. Tabel Bank Soal yang telah terenkripsi

No	Soal	Kunci_jawaban
1	b2+$0&<!}/&<1/)<G<a<-}!}<*0J4,/!<}!})}%<[	$
2	u}+$<~2(}+<*"/2-}(}+<!}/&<,-"/}0&<0&01"*H<(" 2})&<[	$

Dapat dilihat pada tabel 1 soal ujian dan kunci jawaban telah terenkripsi menjadi *chipertext.* Hal ini tentu saja akan membingungkan penyusup. Tetapi teknik ini mempunyai kelemahan, dikarenakan penggunaan teknik enkripsi yang tidak maksimal dan tidak tepat. Dapat dilihat pada tabel 1 *field* kunci jawaban pada no. 1 dan no. 2 memiliki *chipertext* yang sama yaitu kharakter '$', yang dapat dianalisi soal ujian no.1 dan no.2 memiliki pola jawaban yang sama, kemungkinan A dan A, B dan B, atau bahkan mungkin D dan D.

Maka teknik pengamanan kunci jawaban yang tepat adalah merusak atau mengacak pola kunci jawaban tersebut.

II. METODELOGI PENELITIAN

1. Ujian Terkomputerisasi

Di era globalisasi ini, ujian atau tes kemampuan sebagian besar sudah dilaksanakan secara tekomputerisasi baik secara online maupun tidak. Dikarenakan ujian secara terkomputerisasi lebih praktis dan akurat untuk mendapatkan hasil atau nilai tes dengan skala peserta yang besar dalam waktu yang singkat, dibandingkan dengan ujian yang dilakukan dengan kertas ataupun dengan lembar jawaban komputer.

Ujian terkomputerisasi dalam bentuk pilihan ganda pada umumnya mempunyai tabel yang terdiri dari 3 field, yaitu : no_soal, soal_ujian, dan kunci_jawaban, dan ada juga yang mempunyai lebih dari 3 field, yaitu : no_soal, soal_ujian, optionA, optionB, optionC, optionD, optionE dan kunci_jawaban.

2. Kriptografi

Kriptografi atau Enkripsi adalah sebuah metode penyandian sebuah teks atau kalimat (*plaintext)* menjadi kata sandi (*chipertext*) yang acak dengan metode penguncian tertentu. Dengan tujuan untuk menjaga informasi dari teks tersebut agar tidak dapat diambil oleh pihak yang tidak diizinkan.

Salah satu teknik penyandian adalah kriprografi sandi *caesar*, atau sandi geser. Sandi *caesar* atau

geseran *caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, A akan menjadi D, C menjadi F. Nama *Caesar* diambil dari *Julius Caesar*, jendral, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya [3].

Teknik lainnya adalah kriptografi *vigenère*, sandi *vigenère* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi *caesar* berdasarkan huruf-huruf pada kata kunci. Sandi *vigenère* merupakan bentuk sederhana dari sandi substitusi *polialfabetik*. Kelebihan sandi ini dibanding sandi *caesar* dan sandi *monoalfabetik* lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi [4].

Contoh implementasi metode *caesar* :

Plaintext: **A**TT**A**CK**A**TD**A**WN
Key: 3
*Ciphertex*t: **D**WW**D**FN**D**WG**D**ZQ

Contoh implementasi metode *vigenère* :

Plaintext: **A**TT**A**CK**A**TD**A**WN
Key: LEMONLEMONLE
Ciphertext: **L**XF**O**PV**E**FR**N**HR

Dapat dilihat pada 2 contoh implementasi teknik penyandian di atas. Terlihat penyandian *vigenère* dapat menghilangkan pola teks yang sama (*monoalfabetik*) yaitu huruf **"A**" menjadi *plaintext* : "**L, O, E,** dan **N**". Dibandingkan dengan teknik penyandian *caesar* yang tidak dapat menghilangkan pola teks **"A**" menjadi *plaintext* hanya : "**D**", hal ini tentu saja akan memudahkan pemecahan dengan analisis ferkuensi.

3. Penelitian

Penelitian dilakukan penulis dalam penerapan sistem kriptografi pengamanan bank soal aplikasi ujian E-SOAL pada ujian tengah semester (UTS) dan akhir semester (UAS) beberapa mata kuliah di STMIK Widya Cipta Dharma. E-Soal dikembangkan mulai dari ver 1.0 sampai ver. 4.0. E-Soal sendiri adalah aplikasi ujian akhir yang telah terkomputerisasi berbentuk ujian pilihan ganda dengan 4 pilihan jawaban yaitu A sampai E. Berikut adalah perkembangan versi E-SOAL dapat dilihat pada tabel 2 :

Tabel 2. Hasil Penelitian pada Perkembangan Pengamanan E-SOAL

Semester	E-SOAL	Hasil
UAS Ganjil 2012	Ver 1 Tanpa pengamanan apapun (hanya password untuk log-in)	30 dari 58 mahasiswa mendapatkan nilai 100
		Wawancara : Mahasiswa mengaku berhasil membaca soal ujian dan kunci jawaban
UTS Genap 2013	Ver 3 Pengamanan kriptografi pada soal dan kunci jawaban dengan metode *caesar*	6 dari 117 mahasiswa mendapatkan nilai 100
		Wawancara : Mahasiswa mengaku berhasil membaca pola kunci jawaban

III. HASIL DAN PEMBAHASAN

Dapat dilihat pada tabel 2 di metodologi penelitian, mahasiswa berhasil membaca pola dari kunci jawaban yang ada di dalam aplikasi E-SOAL. Hal ini dikarenakan kunci jawaban hanya terdiri dari 1 karakter. Metode penguncian atau dengan *key* (kunci) apapun, mengenkripsi 1 karakter kunci jawaban akan tetap menciptakan pola yang mudah untuk dianalisis oleh penyusup. (dapat dilihat pada tabel 3)

Tabel 3. Hasil Perbandingan Enkripsi *Record* Kunci Jawaban dengan menggunakan 2 Metode Enkripsi yang Berbeda

No soal	Kunci_jawaban (*plaintext)*	Kriptografi *Caesar* (*chipertext)*	Kriptografi *Vigenère* (*chipertext)*
1	A	D	$
2	A	D	$
3	B	E	/
4	C	F	=
5	B	D	$

Pembuatan kunci jawaban menjadi *record* yang terstruktur dalam sebuah tabel seperti pada tabel 3 adalah cara tidak tepat. Untuk menghilangkan pola tersebut, maka kunci jawaban harus dibuat dalam 1 *record* saja. Membuat teks kunci jawaban dalam 1 *record* data akan membuat kunci jawaban yang sebelumnya hanya terdiri dari 1 karakter dapat berubah menjadi banyak karakter yang berderet. . (Lihat pada tabel 4)

Tabel 4. Kunci Jawaban yang Dibuat Menjadi 1 *Record Data*

Kunci_jawaban (*plaintext)*
AABCB

Tabel 5. Hasil Enkripsi *Record* Kunci Jawaban dari Tabel 4 dengan menggunakan 2 Metode Enkripsi yang Berbeda

Kriptografi *Caesar* (*chipertext)*
DDEFD
Kriptografi *Vigenère* (*chipertext)*
$(#/>

Dapat dilihat pada tabel 5, *record* yang berisi teks kunci jawaban "AABCB" telah dienkripsi dengan metode kriptografi *vigenère*, teknik ini membuat enkripsi berhasil menghilangkan pola dari teks kunci jawaban. Dibandingkan dengan kriptografi *caesar,* kriptografi ini tidak berhasil menghilangkan pola dari teks kunci jawaban tersebut, hal ini dikarenakan enkripsi *caesar* masih bersifat *monoalfabetik*.

Setelah teknik pengamanan ini diterapkan pada E-SOAL ver. 4 di ujian akhir semester (UAS) genap 2013, dari 113 mahasiswa tidak ada satupun yang mendapatkan nilai 100. Hasil wawancara didapatkan ternyata tidak ada mahasiswa yang berhasil memecahkan teknik pengamanan ini.

IV. KESIMPULAN

Teknik yang tepat untuk mengamankan *record* teks kunci jawaban yang hanya terdiri dari 1 karakter dalam database bank soal ujian pilihan ganda, yaitu dengan teknik menggabungkannya menjadi 1 deret teks dalam 1 *record* data. Kunci jawaban yang telah tergabung dalam 1 *record* data inilah yang akan dienkripsi menjadi *chipertext.*

Dengan menggunakan metode enkripsi yang bersifat *polialfabetik,* teks kunci jawaban yang telah menjadi 1 deret dalam 1 *record* data, dapat di enkripsi sampai menghilangkan pola dari subtitusi teksnya.

V. DAFTAR PUSTAKA

[1] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996

[2] Akbar, Haryus Aminul, *Analisis Serangan Dictionary Attack pada Cipherteks Berbasis Substitusi Monoalfabetik*, Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011

[3] Arius, Doni "Pengantar Ilmu KRIPTOGRAFI, Teori, Analisis dan Implementasi". Yogyakarta : Erlangga. 2008

[4] Singh, Yumnam Kirani. *Generalization of Vigenere Cipher*, ARPN Journal of Engineering and Applied Sciences, VOL. 7, NO. 1, January 2012

[5] Grounlund, NE. *Measurement and evaluation in Teaching*, 5th edition. New York: Macmillan Publishing Company. 1985.

[6] Panduan Penulisan Soal Pilihan Ganda. Pusat Penilaian Pendidikan BALITBANG-DEPDIKNAS

[7] Y. K. Singh. 2011. A Simple, *Fast and Fecure Cipher*. RPN Journal of Engineering and Applied Sciences. 6(10): 61-69.