PEMBELAJARAN ENKRIPSI METODE WORD AUTO KEY ENCRYPTION

Eddy, Mohammad Reza Pahlevi
Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak
Jalan Merdeka Barat No. 372 Pontianak, Kalimantan Barat
[1]Eddy3chi@yahoo.com, [2]reza_fahlevi@stmikpontianak.ac.id, rezarockbanget@gmail.com

Abstrak

Kriptografi Metode WAKE merupakan salah satu metode yang telah digunakan secara *komersial*. WAKE merupakan singkatan dari Word Auto Key Encryption. Metode ini ditemukan oleh David Wheeler pada tahun 1993 dan merupakan salah satu algoritma stream cipher yang cepat dalam implementasinya dalam perangkat lunak. Metode ini menggunakan kunci 128 bit, plaintext 32 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metoda ini menggunakan operasi XOR, AND, OR dan Shift Right. Inti dari metode WAKE terletak pada proses pembentukan tabel S-Box dan proses pembentukan kunci. Tabel S-Box dari metode WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran. Perancangan perangkat lunak menggunakan metode perancangan RAD (Rapid Application Development), adapun langkah-langkah yang dilakukan yaitu : Bussiness Modeling, Data modelling, Process Modeling, GenerationApplication

Kata Kunci : word autokey encryption, RAD (Rapid Application Development)

Abstract

Cryptographic method WAKE method is one method that has been used commercially. WAKE is an abbreviation of Word Auto Key Encryption. This method was invented by David Wheeler in 1993 and is one of the fast stream cipher algorithm in its implementation in the software. This method uses a key of 128 bits, 32 bits of plaintext and a table 256 x 32 bits. In the algorithm, this method uses XOR operations, AND, OR and Shift Right. The essence of the method lies in the process of forming WAKE table S-box and key establishment process. Table S-Box of the WAKE method is flexible and different for each round. Software design using design methods RAD (Rapid Application Development), while the measures undertaken are: Bussiness Modeling, Data Modeling, Process Modeling, Generation Application.

Keywords: *word autokey encryption,* RAD (*Rapid Application Development*)

1. PENDAHULUAN

Untuk menjamin kerahasiaan suatu informasi, dapat dilakukan dengan menggunakan kriptografi. Kriptografi sesungguhnya merupakan studi terhadap penyandian suatu tulisan atau informasi rahasia dengan menggunakan suatu teknik matematis. Dengan menggunakan kriptografi, informasi dapat disandikan ke dalam bentuk yang tidak bisa dimengerti sehingga informasi tersebut tidak dapat diakses oleh orang-orang yang tak berkepentingan.

Banyak sekali metode penyandian atau metode kriptografi yang dikembangkan oleh pakar-pakar kriptografi hingga saat ini. Hal ini dilakukan dikarenakan penyadap dan pencuri informasi atau yang lebih dikenal dengan sebutan cracker semakin handal dalam mempenetrasi suatu sistem untuk menggali berbagai macam informasi. Oleh karena itu dalam rangka melawan tindakan keji tersebut, pakar-pakar kriptografi terus mengembangkan metode ini secara berkesinambungan. Metode kriptografi dapat digunakan untuk mengamankan data yang bersifat rahasia agar data tersebut tidak diketahui oleh orang lain yang tidak berkepentingan.

Banyak sekali metode penyandian yang telah diciptakan oleh pakar-pakar kriptografi dunia, sebut saja Algoritma DES, Algoritma 3DES, Algoritma IDEA, Algoritma Blowfish,

Algotitma RSA, Algoritma MD4, Algotitma MD5, Algoritma SHA-1, Algoritma McEliecce dan sebagainya. Algoritma-algoritma diatas telah diuji kemampuannya oleh pakar-pakar kriptografi, namun tidak semua metode kriptografi diatas bertahan dari serangan para penyadap informasi atau dalam istilah kriptografi sering disebut dengan cryptanalist.

Metode WAKE merupakan salah satu metode yang telah digunakan secara komersial. WAKE merupakan singkatan dari Word Auto Key Encryption. Metode ini ditemukan oleh David Wheeler pada tahun 1993 dan merupakan salah satu algoritma stream cipher yang cepat dalam implementasinya dalam perangkat lunak. Metode ini menggunakan kunci 128 bit, plaintext 32 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metoda ini menggunakan operasi XOR, AND, OR dan Shift Right. Metode WAKE ini telah digunakan pada program Dr. Solomon Anti Virus versi terbaru.

Metode WAKE dapat dibagi menjadi beberapa proses yaitu proses pembentukan tabel dan kunci, enkripsi dan dekripsi. Proses penyelesaian metoda ini cukup rumit dan sulit untuk dikerjakan secara manual berhubung karena algoritmanya yang cukup panjang dan kompleks. Untuk memudahkan pemahaman cara kerja metoda WAKE tersebut diperlukan sebuah perangkat lunak yang dapat menjelaskan langkah-langkah dan hasil setiap langkah.

Inti dari metode dari Word Auto Key Encryption (WAKE) terletak pada proses pembentukan tabel S-Box dan proses pembentukan kunci. Tabel S-Box dari metode WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran.

Schneier (1996) melakukan penelitian mengenai Penerapan Algoritma Kriptografi WAKE pada Aplikasi Chatting & Internet Monitor Berbasis LAN. (Ryan Maulana A.2012) Penelitian bertujuan untuk memberikan informasi guna menyelesaikan masalah berdasar pada objek yang di teliti yaitu penerapan kriptografi WAKE(Word Auto Key Encryption) pada aplikasi chatting, setalah melakukan penelitian di dapati bahwa dengan menerapkan kriptografi WAKE pada aplikasi chatting akan meningkatkan level keamanan data/informasi saat kegiatan chatting berlangsung hal itu dilakukan untuk menghindari masalah yang bisa di timbulkan oleh pihak – pihak tidak bertanggung jawab, karena pihak – pihak tersebut bisa saja melakukan gangguan pada sistem aplikasi chatting bisa dengan cara mencuri, merubah, mengurangi, menambah pesan para user saat sedang melakukan chatting. Kholidya Yuli Wardani, M.Zen S.Hadi, Mike Yuliana (2012), melakukan penelitian mengenai Implementasi Metode Kriptografi WAKE pada Priority Dealer untuk Layanan Pemesanan dan Laporan Penjualan Handphone Berbasis Web. Tujuan dari penelitian ini mempermudah saling bertukar informasi / data secara jarak jauh sehingga lebih efisien dan tidak mengeluarkan biaya, namun kelemahan menggunakan system WEB yaitu keamanan kerahasiaan pengiriman data tidak terjamin.

Melalui pembelajaran ini dijelaskan tahap-tahap dari proses yang akan ditampilkan sehingga diharapkan dapat memberikan pemahaman yang lebih baik. Selain itu animasi yang mendukung juga dapat menambah efektifitas keberhasilan pembelajaran dan menambah minat user terhadap pembelajaran tersebut.Berdasarkan latar belakang dapat diketahui yang menjadi permasalahan dalam penulisan skripsi ini yaitu, bagaimana merancang suatu perangkat lunak pembelajaran kriptografi metode Word Auto Key Encryption atau WAKE.

Tujuan yang ingin dicapai dalam penelitian ini adalah merancang suatu program aplikasi pembelajaran yang dapat merahasiakan isi suatu informasi menggunakan teknik kriptografi dengan metode Word Auto Key Encryption atau WAKE.

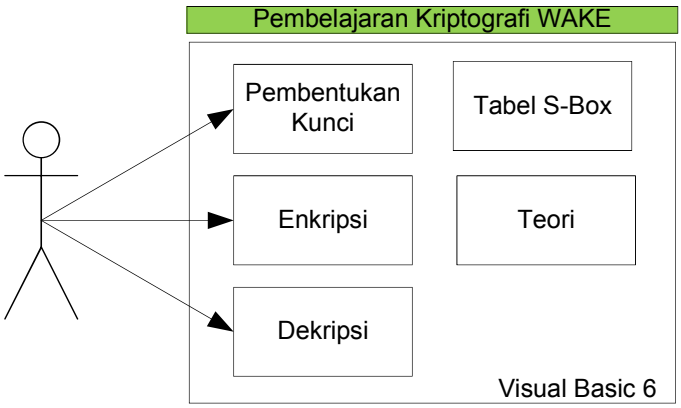
2. METODE PENELITIAN

Dalam penelitian ini, digunakan bentuk penelitian studi literatur dan eksperimen murni. Dilakukan kajian yang berkaitan erat dengan permasalahan yang hendak dipecahkan serta mendefinisikan masalah dengan melakukan eksperimen. Adapun instrumen atau alat (*tools)*

yang digunakan penulis dalam penelitian yaitu menggunakan algoritma, *flowchart* (bagan alir). Penggunaan metode perancangan RAD (*Rapid Application Development*) karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat dan pemanfaatan fungsi yang telah ada sebelumnya. Data yang dikumpulkan sesuai dengan tujuan penelitian. Sumber data ada dua yaitu: data Sekunder dan data Primer. Dalam mengumpulkan data penulis menggunakan metode studi literatur dan dokumentasi, yaitu dokumentasi data yang berisi definisi-definisi dari item-item data, termasuk di dalamnya semua variabel-variabel yang digunakan dalam proses perancangan aplikasi kriptografi *Word Auto Key Encryption* atau *WAKE*. Data yang dikumpulkan menjadi dasar pengembangan sistem serta dasar bila akan memodifikasi atau memperbaiki sistem kemudian hari. Untuk memastikan perangkat lunak dapat berjalan sebagaimana mestinya, maka perlu dilakukan pengujian terhadap kerja perangkat lunak. Metode pengujian yang dipakai penulis adalah metode *black-box*. Pengujian dilakukan terhadap fungsi-fungsi yang ada dengan menginput data masukan dan meneliti data hasil outputnya.

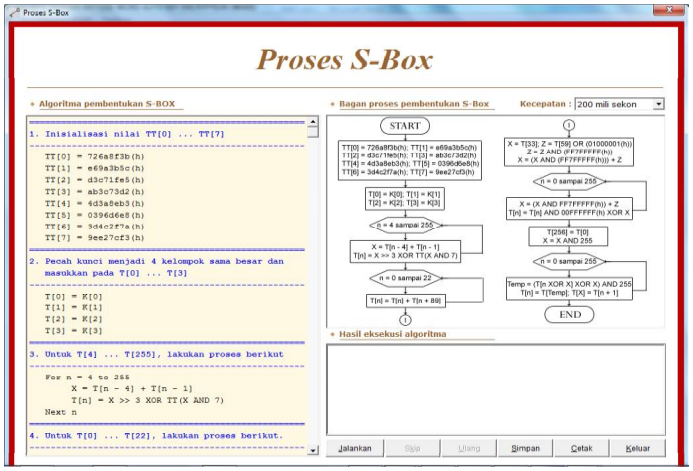
3. HASIL DAN PEMBAHASAN

Business Modeling Pada tahap ini, penulis mendaftar dan mendefinisikan fungsi-fungsi yang akan dipakai dalam pembuatan aplikasi dalam bentuk modul-modul. Perangkat lunak pembelajaran ini akan dibuat dalam modul-modul seperti pada gambar 1. Adapun modul-modul pada perangkat lunak pembelajaran kriptografi WAKE terdiri dari : modul teori Kriptografi metode WAKE, modul tentang penjelasan tabel S-Box, modul tentang penjelasan proses pembentukan kunci, modul tentang Penjelasan Proses Enkripsi, modul tentang Penjelasan Proses Dekripsi



Gambar 1. Arsitektur Aplikasi

Form Proses S-Box Pada Form Proses S-Box dirancang terdiri dari daerah tampilan algoritma untuk pembentukan tabel S-Box, *vertical scroll bar*, berfungsi untuk menggulung (*scroll*) tampilan algoritma secara vertical, *combo box* 'Kecepatan', berfungsi untuk memilih kecepatan proses, daerah tampilan hasil eksekusi proses, tombol 'Jalankan', berfungsi untuk memulai proses pembentukan tabel *S-Box*, tombol 'Skip', berfungsi untuk menghasilkan tabel *S-Box* tanpa melalui animasi tahapan– tahapan proses yang ada, tombol 'Ulang', berfungsi untuk mengulangi proses pembentukan tabel *S-Box*, tombol 'Simpan', berfungsi untuk menyimpan hasil eksekusi, tombol 'Cetak', berfungsi untuk mencetak hasil eksekusi, dan tombol 'Keluar', berfungsi untuk keluar dari *form* 'Proses S-Box'.

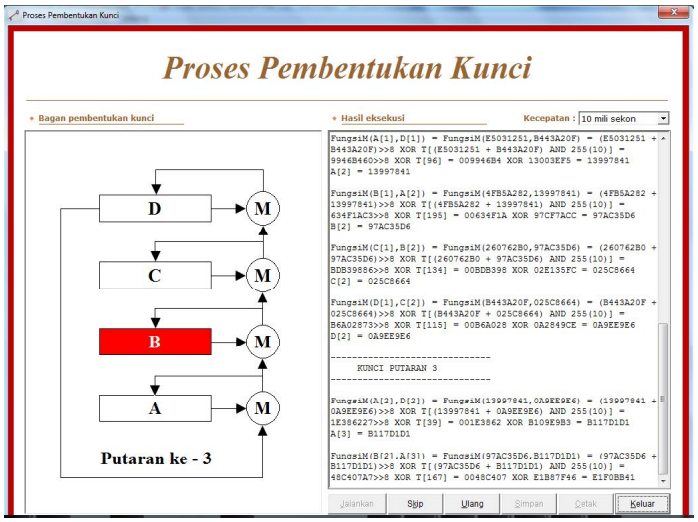


Gambar 2. Form Proses S-Box

Untuk melihat proses pembentukan kunci, pilih menu 'Pembelajaran WAKE' dan klik sub menu 'Proses Pembentukan Kunci'. Muncul *form input* berikut.

Gambar 3. Tampilan Form Input Proses Pembentukan Kunci

Form Proses Pembentukan Kunci Pada Form Proses Pembentukan Kunci dirancang terdiri dari daerah tampilan diagram pembentukan kunci, *combo box* 'Kecepatan', berfungsi untuk memilih kecepatan proses, daerah tampilan hasil eksekusi proses, tombol 'Jalankan', berfungsi untuk memulai proses pembentukan kunci, tombol 'Skip', berfungsi untuk menghasilkan kunci tanpa melalui animasi tahapan– tahapan proses yang ada, tombol 'Ulang', berfungsi untuk mengulangi proses pembentukan kunci, tombol 'Simpan', berfungsi untuk menyimpan hasil eksekusi, tombol 'Cetak', berfungsi untuk mencetak hasil eksekusi dan tombol 'Keluar', berfungsi untuk keluar dari *form* 'Proses Pembentukan Kunci'.

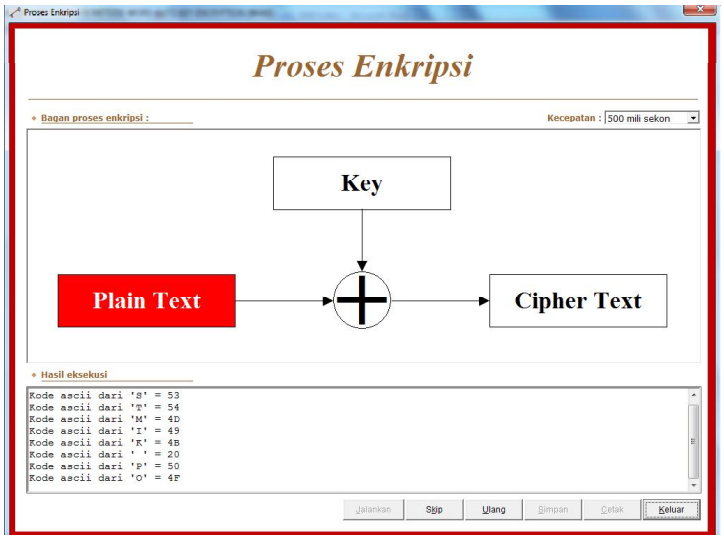


Gambar 4. *Form Proses Pembentukan Kunci*

Form Proses Enkripsi / Dekripsi Pada Form Proses Enkripsi/Dekripsi dirancang terdiri dari *label*, untuk menampilkan nama proses (proses enkripsi atau dekripsi), *combo box* 'Kecepatan', berfungsi untuk memilih kecepatan proses, daerah tampilan diagram enkripsi atau dekripsi, daerah tampilan hasil eksekusi proses, tombol'Jalankan', berfungsi untuk memulai proses enkripsi atau dekripsi, tombol 'Skip', berfungsi untuk menghasilkan *plaintext* atau *ciphertext* tanpa melalui animasi tahapan– tahapan proses yang ada, tombol 'Ulang', berfungsi untuk mengulangi proses enkripsi atau dekripsi, tombol 'Simpan', berfungsi untuk menyimpan hasil eksekusi, tombol 'Cetak', berfungsi untuk mencetak hasil eksekusi, dan tombol 'Keluar', berfungsi untuk keluar dari *form*.

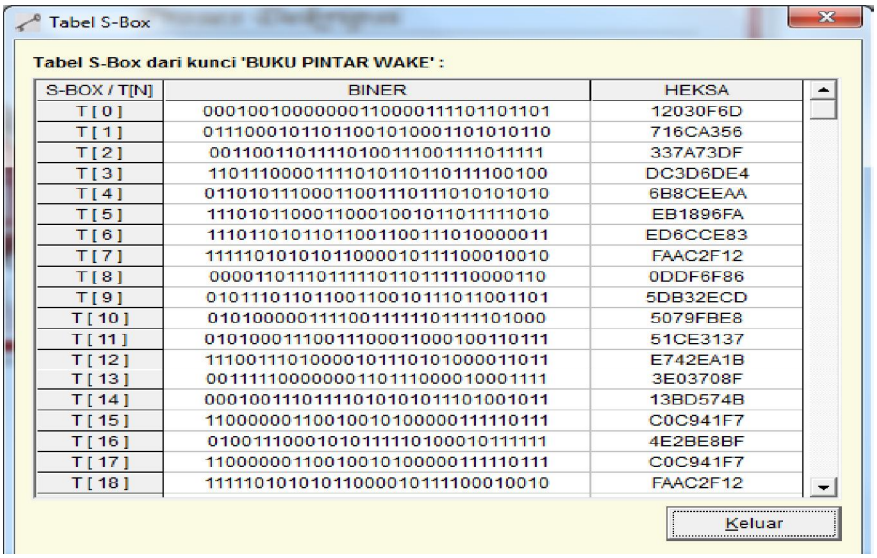
Gambar 5. Tampilan Form Input Proses Enkripsi

Klik pada tulisan biru 'Lihat Tabel S-Box' di sebelah kiri bawah *form* akan memunculkan *form* 'Tabel S-Box' pada gambar 5, sedangkan klik pada tulisan biru 'Kunci yang terbentuk' akan memunculkan *form* 'Hasil Pembentukan Kunci' pada gambar Untuk melihat dan mengikuti prosedur kerja proses enkripsi secara bertahap, maka klik pada tombol 'Proses'. Selanjutnya, muncul *form* 'Proses Enkripsi'.



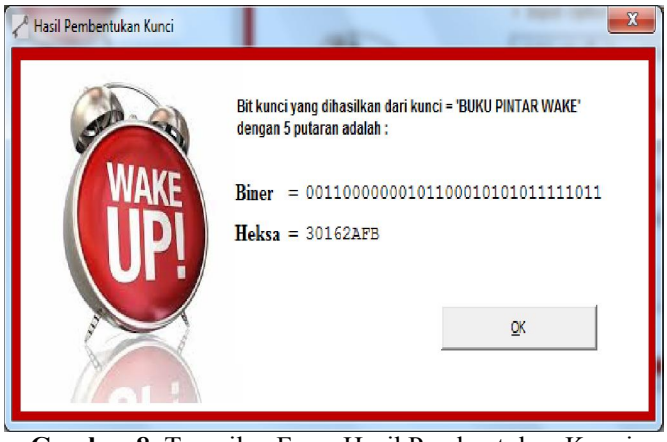
Gambar 6. Form Proses Enkripsi

Form Tabel S-Box Pada Form Tabel S-Box dirancang terdiri dari Sebuah tabel S-Box, *vertical scroll bar,* untuk menggulung (*scroll*) tabel S-Box secara horizontal, dan tombol 'Keluar', berfungsi untuk keluar dari form 'Tabel S-Box'.



Gambar 7. Tampilan Form Tabel S-Box

Pada Form Hasil Pembentukan Kunci dirancang terdiri dari Sebuah *label* untuk menampilkan *input key*,*label* untuk menampilkan *input* putaran kunci, *label* untuk menampilkan hasil pembentukan kunci dalam bentuk biner, *label* untuk menampilkan hasil pembentukan kunci dalam bentuk heksa dan tombol 'OK', berfungsi untuk keluar dari *form*.



Gambar 8. Tampilan Form Hasil Pembentukan Kunci

Proses enkripsi dari metode WAKE untuk menghasilkan *ciphertext* adalah berupa hasil operasi XOR dari *plaintext* dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci.

Ciphertext (C) = Plaintext (P) XOR Key (K)

Misalkan Plain Text = "STMIK PONTIANAK" maka Proses Enkripsinya sebagai berikut :

Plain Text : 'STMIK PONTIANAK'
Kode ascii dari 'S' = 53
Kode ascii dari 'T' = 54
Kode ascii dari 'M' = 4D
Kode ascii dari 'I' = 49
Kode ascii dari 'K' = 4B
Kode ascii dari ' ' = 20
Kode ascii dari 'P' = 50
Kode ascii dari 'O' = 4F
Kode ascii dari 'N' = 4E
Kode ascii dari 'T' = 54
Kode ascii dari 'I' = 49
Kode ascii dari 'A' = 41
Kode ascii dari 'N' = 4E
Kode ascii dari 'A' = 41
Kode ascii dari 'K' = 4B
Plain Text (dalam heksa) = 53544D494B20504F4E5449414E414B

Kunci dari proses pembentukan kunci = A2CE14A2

Cipher Text = Plain Text XOR Key
53 XOR A2 = F1 = 'ñ'
54 XOR CE = 9A = 'š'
4D XOR 14 = 59 = 'Y'
49 XOR A2 = EB = 'ë'
4B XOR A2 = E9 = 'é'
20 XOR CE = EE = 'î'
50 XOR 14 = 44 = 'D'
4F XOR A2 = ED = 'í'
4E XOR A2 = EC = 'ì'

54 XOR CE = 9A = 'š'
49 XOR 14 = 5D = ']'
41 XOR A2 = E3 = 'ã'
4E XOR A2 = EC = 'ì'
41 XOR CE = 8F = '□'
4B XOR 14 = 5F = '_'

Hasil proses enkripsi = ñšYëéîDíiš]ãì□_

Proses dekripsi dari metode WAKE untuk menghasilkan *plaintext* adalah berupa hasil operasi XOR dari *ciphertext* dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci.

Plaintext (P) = *Ciphertext* (C) XOR *Key* (K)
Misalkan Cipher Text hasil Enkripsi dari proses sebelumnya maka Proses Dekripsinya sebagai berikut :
Cipher Text : 'ñšYëéîDíiš]ãì□_'
Kode ascii dari 'ñ' = F1
Kode ascii dari 'š' = 9A
Kode ascii dari 'Y' = 59
Kode ascii dari 'ë' = EB
Kode ascii dari 'é' = E9
Kode ascii dari 'î' = EE
Kode ascii dari 'D' = 44
Kode ascii dari 'í' = ED
Kode ascii dari 'ì' = EC
Kode ascii dari 'š' = 9A
Kode ascii dari ']' = 5D
Kode ascii dari 'ã' = E3
Kode ascii dari 'ì' = EC
Kode ascii dari '□' = 8F
Kode ascii dari '_' = 5F
Cipher Text (dalam heksa) = F19A59EBE9EE44EDEC9A5DE3EC8F5F

Kunci dari proses pembentukan kunci = A2CE14A2

Plain Text = Cipher Text XOR Key
F1 XOR A2 = 53 = 'S'
9A XOR CE = 54 = 'T'
59 XOR 14 = 4D = 'M'
EB XOR A2 = 49 = 'I'
E9 XOR A2 = 4B = 'K'
EE XOR CE = 20 = ' '
44 XOR 14 = 50 = 'P'
ED XOR A2 = 4F = 'O'
EC XOR A2 = 4E = 'N'
9A XOR CE = 54 = 'T'
5D XOR 14 = 49 = 'I'
E3 XOR A2 = 41 = 'A'
EC XOR A2 = 4E = 'N'
8F XOR CE = 41 = 'A'

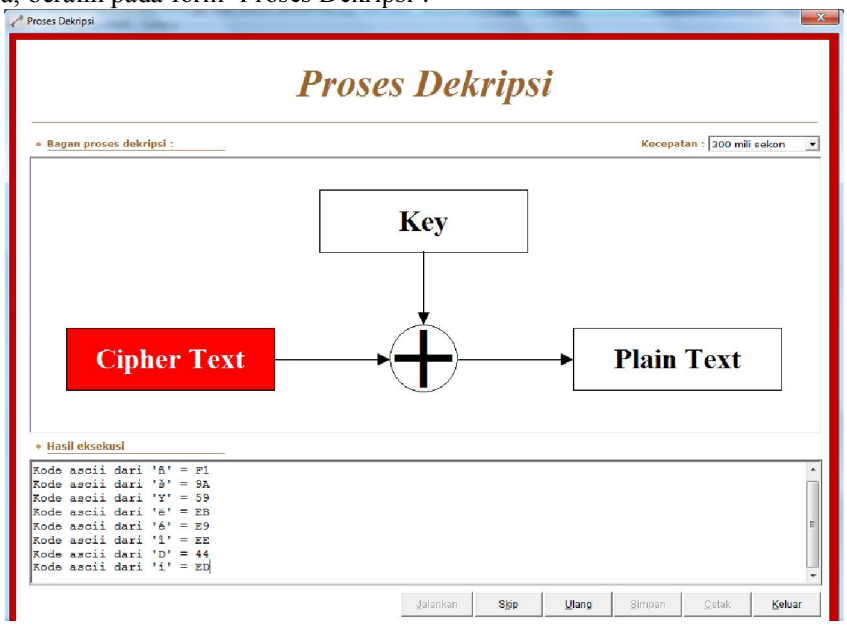
5F XOR 14 = 4B = 'K'

Hasil proses dekripsi = STMIK PONTIANAK

Untuk melihat proses dekripsi, pilih menu ‘Pembelajaran WAKE’ dan klik sub menu ‘Proses Dekripsi’. Muncul form input berikut.

Gambar 9. Tampilan Form Input Proses Dekripsi

Untuk melihat dan mengikuti prosedur kerja proses dekripsi secara bertahap, maka selanjutnya, beralih pada form ‘Proses Dekripsi’.



Gambar 10. Tampilan Form Proses Dekripsi

4. KESIMPULAN

Perangkat lunak ini menunjukkan setiap langkah dan tahapan proses – proses (proses pembentukan table S-Box, proses pembentukan kunci, proses enkripsi dan proses dekripsi) yang terdapat di dalam kriptografi metode WAKE, sehingga dapat membantu pemahaman atau pembelajaran prosedur kerja atau algoritma dari metode kriptografi tersebut. Semakin banyak putaran dari proses pembentukan kunci, maka keamanan data akan sema kinterjamin. Proses penyelesaian metode ini cukup rumit dan sulit untuk dikerjakan secara manual berhubung karena algoritmanya yang cukup panjang dan kompleks. Untuk memudahkan pemahaman cara kerja metoda WAKE tersebut diperlukan sebuah perangkat lunak yang dapat menjelaskan langkah-langkah dan hasil setiap langkah

5. SARAN

Beberapa saran yang mungkin dapat membantu dalam pengembangan perangkat lunak pembelajaran metode kriptografi yaitu :

a. Perangkat lunak dapat ditambahkan fasilitas Multimedia agar lebih menarik dan lebih mendukung pembelajaran metode WAKE.
b. Metode WAKE dapat dimodifikasi untuk mempertangguh keamanan dari metode tersebut seperti mengganti operasi-operasi logika dalam metode WAKE dengan metode rancangan sendiri

DAFTAR PUSTAKA

[1]. Firdaus, 2010, Study Mengenai Algoritma WAKE Hash, Makalah ITB, Bandung
[2]. Miranthy, Wulan Tunjung Sari, 2011, Algoritma WAKE, Program Studi Teknik Informatika, Skripsi Sarjana Komputer, STMIK MDP
[3]. Booth, Paul A., *An Introduction to Human-Computer Interaction*, Lawrence Erlbaum Associates Ltd., Inggris, 1989
[4]. Kurniawan J., Ir. , M.T., Kriptografi, Keamanan Internet dan Jaringan Komunikasi, Penerbit Informatika Bandung, April 2004.
[5]. Pramono D., Mudah Menguasai *Visual Basic 6*, PT. Elex Media Komputindo, 2002.
[6]. Rahadian H., Pemrograman *Windows API* dengan *Microsoft Visual Basic*, PT. Elex Media Komputindo, 2002.
[7]. Schneier B., Applied Crytography, Second Edition, John Wiley & Sons, Inc., 1996.
[8]. Suryokusumo A., *Microsoft Visual Basic 6.0*, PT. Elex Media Komputindo, 2001.