Jurnal Computech & Bisnis, Vol. 4, No. 1, Juni 2010, 1-6
ISSN 1978-9629

ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA PADA POCKET PC MENGGUNAKAN METODE ENKRIPSI ALGORITMA RC-4

Bambang Siswoyo[1], Benny Kadarisman[2]
[1] Sekolah Tinggi Teknologi Informatika Sony Sugema Bandung
[1] Fakultas Teknik dan Ilmu Komputer, Jurusan Teknik Informatika, UNIKOM

Abstrak

Along with the rapid development of mobile technology at this time, especially Pocket PC, causing data security is a very important thing. Existing data on the Pocket PC may be a very important data and confidential access is not possible others. To overcome this problem so that data is secure from unauthorized users, we need software that can perform a process of encryption/decryption of data. In this paper discussed the implementation of RC - 4 algorithms separately secure the data on your Pocket PC.

Keywords: *Pocket PC, RC-4 Algorithms*

Abstrak

Seiring dengan makin pesatnya perkembangan teknologi mobile pada saat ini terutama Pocket PC, menyebabkan keamanan data merupakan suatu hal yang sangat penting. Data yang ada pada Pocket PC boleh jadi merupakan data yang sangat penting dan rahasia yang tidak dimungkinkan orang lain mengaksesnya. Untuk mengatasi hal tersebut agar data aman dari pengguna yang tidak berhak maka diperlukan suatu perangkat lunak yang bisa melakukan suatu proses enkripsi/dekripsi data. Dalam tulisan ini dibahas implemetasi algoritma RC-4 utnuk mengamankan data pada Pocket PC.

Kata Kunci: *Pocket PC, RC-4 Algorithms*

1. Latar Belakang

Perkembangan teknologi peranti bergerak (*mobile device*) dari hari ke hari semakin berkembang. Perkembangannya tidak hanya dari sudut teknologinya saja, tetapi dari sudut tampilannya yang semakin menarik. Hal ini dibuktikan dengan semakin bertambahnya pengguna *mobile device* terutama bagi mereka yang membutuhkan informasi yang cepat dan juga untuk meningkatkan produktifitas kerjanya.

Ada beberapa pilihan *mobile device* ini seperti handphone, smartphone, Pocket PC, laptop, dan lain-lain. Berbagai pilihan tersebut tentu saja disesuaikan dengan kebutuhan masing-masing. Kaitannya dalam penelitian kali ini penulis hanya akan membahas mengenai keamanan data teknologi Pocket PC. Pocket PC atau komputer saku dan lebih populer disebut dengan PDA merupakan salah satu teknologi di dunia *mobile device* yang diproduksi oleh Microsoft. Pocket PC adalah suatu komputer yang bisa digenggam yang memiliki kemampuan seperti PC (Personal Computer) yang bentuknya seukuran telapak tangan.

Salah satu hal yang penting bagi pengguna Pocket PC adalah adanya jaminan kerahasiaan informasi data. Informasi yang merupakan hasil pengolahan dari data, mempunyai nilai yang berbeda bagi setiap orang. Seringkali sebuah informasi menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya. Namun selalu saja ada pihak yang berusaha untuk mengetahui informasi dengan cara-cara yang tidak semestinya bahkan bermaksud untuk merusaknya. Hal ini sering mereka lakukan baik secara *on-line* (terhubung ke jaringan) atau pun secara *off-line* (tidak terhubung ke jaringan).

Berdasarkan kenyataan di atas, perlu ada suatu pengamanan informasi baik saat penyimpanan maupun pengiriman informasi. Untuk melakukan ini ada suatu cara yang biasa disebut penyandian data. Dalam penelitian ini penulis akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan "Cryptography" (kriptografi). Dengan kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti serta mengembalikannya kembali ke semula, proses ini disebut Enkripsi dan Dekripsi data.

Enkripsi merupakan salah satu cara yang dilakukan untuk mengamankan sistem atau informasi dari hal yang akan menyebabkan aspek-aspek diatas tidak terpenuhi, seperti untuk menjaga integritas data atau informasi. Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari, seperti Data Encryption Standard (DES), RC-4, TwoFish, Blowfish dan lain-lain. Tulisan ini membahas algoritma RC-4 yang dikemukakan oleh **Ronald L.Rivest** dari MIT Laboratory for Computer Science. Metode penulisan dilakukan dengan studi literatur terhadap buku dan bahasan-bahasan di internet yang berhubungan dengan algoritma enkripsi terutama algoritma RC-4.

Berdasarkan uraian diatas maka penulis mengambil judul skripsi **Analisis dan Implementasi Sistem Keamanan data Pada Pocket PC Menggunakan Metode Enkripsi Algoritma RC-4 .**

2. Identifikasi Masalah

Berdasarkan uraian latar belakang diatas, maka penulis mengidentifikasi beberapa hal yang berhubungan dengan masalah keamanan data pada pocket PC antara lain :

1. Rentannya sistem keamanan data karena selalu ada pihak-pihak yang bermaksud mengetahui bahkan merusak sebuah informasi, sehingga perlu dicari pemecahannya. Pemecahan masalah ini dapat dipecahkan diantaranya dengan menggunakan suatu metode yaitu metode enkripsi dengan menggunakan algoritma kriftografi.
2. Banyaknya penyusup didalam jaringan komunikasi data, mengakibatkan penggunaan password saja menjadi kurang efektif dalam proses pengamanan data karena mudahnya untuk ditembus dengan waktu yang relatif singkat.
3. Adanya kesulitan didalam merancang sistem keamanan data, sehingga menjadi suatu tuntutan untuk pembuatan perancangan perangkat lunak.
4. Masih sedikit orang yang mengimplementasikan kriptografi sebagai dukungan dalam keamanan sistem informasi terutama untuk Pocket PC, sehingga diperlukan sebuah perancangan perangkat lunak yang dapat mengamankan data yang ada pada Pocket PC.
5. Data yang ada pada Pocket PC bisa jadi merupakan suatu hal yang sangat penting dan berharga, sehingga tidak boleh data tersebut jatuh kepada orang yang tidak berhak memakainya.

Dari kelima hal tersebut diatas, maka penulis mencoba untuk membuat analisis dan mengimplementasikan suatu sistem keamanan yang menggunakan kriptografi yang pada penelitian kali ini penulis menggunakan algoritma RC-4.

3. Batasan Masalah

Dalam penulisan tugas akhir ini penulis akan membatasi masalah pada beberapa hal berikut ini :

1. Menggunakan metode Algoritma RC-4 untuk mengenkripsi data pada Pocket PC.
2. Pada algoritma ini menggunakan kunci sepanjang 128 bit
3. Menganalisa kinerja dari algoritma RC-4 sejauh mana mentode ini bisa melindungi data atau informasi pada Pocket PC.
4. Mengimplementasikan sistem keamanan ini pada emulator Microsoft Windows Platform SDK for Pocket PC 2000.
5. Data atau file yang akan dicoba diamankan adalah *.txt, *.psw, *.pwi

RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang-kadang bit. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Contoh *stream cipher* adalah RC4, Seal, A5, Oryx, dan lain-lain. Tipe lainnya adalah *block cipher* yang memproses sekaligus sejumlah tertentu data (biasanya 64 bit atau 128 bit blok), contohnya : Blowfish, DES, Gost, Idea, RC5, Safer, Square, Twofish, RC6, Loki97, dan lain-lain.

RC4 adalah algoritma enkripsi *stream cipher* dan *symmetric key*, dimana algoritma ini melakukan proses enkripsi/dekripsi dalam satu byte dan menggunakan kunci yang sama. Proses dari algoritma RC4 ini terdiri atas 2 bagian yaitu Key Scheduling Algorithm(KSA) dan Pseudo Random Generation Algorithm(PRGA). Output dari KSA ini digunakan PRGA untuk menghasilkan random key yang di XOR kan dengan plaintext untuk menghasilkan stream cipher (enkripsi) dan dekripsi

Kunci utama RC-4 maksimal sepanjang 2048 bit (256 byte), namun yang biasa

digunakan hanya sepanjang 40 bit atau 128 bit. Sisanya (2048 – 40 = 2048 bit atau 2048 – 128 = 1920 bit) diisi dengan perulangan kunci tersebut. Jadi jika kuncinya berupa 16 byte (128 bit) kuncinya = 0123456789abcdef dimana setiap angka merupakan bilangan hexadesimal maka byte ke-17 sampai byte ke-256 berisi kunci tersebut secara berulang.

Proses pertama dalam algoritma RC-4 adalah Key Scheduling Algorithm. KSA ini merupakan inisialisasi untuk pentabelan S-BOX dan kunci. RC4 mempunyai sebuah *S-Box*, $S_0,S_1,...,S_{255}$, yang berisi permutasi dari bilangan 0 sampai 255. Terdapat dua indeks yaitu i dan j yang diinisialisasi dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut :

For i ← 0 to 255
S[i] ← i

Dalam operasi selanjutnya, RC-4 akan mengubah isi kotak-S tergantung kunci K dengan operasi sebagai berikut :

j=0
for i ← 0 to 255
j ← (j +S[i] +K[i]) mod 256
pertukarkan isi S[i] dan isi S[j]

Dengan demikian berakhirlah proses KSA. Untuk selanjutnya untuk membangkitkan kunci enkripsi, dilakukan proses PRGA atau Pseudo Random Generation Algorithm.

Algoritma PRGA adalah sebagai berikut :

i ← 0
j← 0
i ←(i + 1) mod 256
j ←(j + S[i]) mod 256
pertukarkan isi S[i] dan S[j]
k = S [S[i] + S [j]] mod 256

perhatikan bahwa k kecil merupakan kunci yang langsung beroperasi terhadap plaintext, sedangkan K besar adalah kunci utama induk

Bila terdapat plaintext P, maka operasi enkripsi berupa :
C = P XOR k

Sedangkan operasi dekripsi berupa :
P = k XOR C

4. Keamanan RC4

Salah satu kelemahan dari RC-4 adalah terlalu tingginya kemungkinan terjadi tabel S-box yang sama, hal ini terjadi karena kunci user diulang-ulang untuk mengisi 256 bytes, sehingga 'aaaa' dan 'aaaaa' akan menghasilkan permutasi yang sama. Kekurangan lainnya ialah karena enkripsi RC-4 adalah XOR antara data bytes dan *pseudo-random byte stream* yang dihasilkan dari kunci, maka penyerang akan mungkin untuk menentukan beberapa byte pesan orisinal dengan meng-XOR dua *set cipher byte*, bila beberapa dari pesan input diketahui (atau mudah untuk ditebak

Kotak S RC-4 terdiri dari array 256 byte yang dioperasikan secara permutasi. Artinya isi S[0] sekarang akan menjadi S[45] berikutnya, atau isi S[234] sekarang akan menjadi isi S[143] berikutnya setelah operasi swap (pertukaran isi S). Bila S[0] telah terisi suatu nilai dari 256 kemungkinan nilai, maka S[1] berisi salah satu dari 255 nilai, dan S[2] berisi salah satu dari 254 nilai. Sehingga kemungkinan isi kotak S menjadi 256 X 225 X 254 X 253 X ...X 1 atau 256! kemungkinan. Sebagai contoh, kemungkinan pertama isi S[0]=0, isi S lainnya tidak mungkin =0, kemungkinan ke-2nya berisi S[0]=1 dan isi S lainnya tidak mungkin sama dengan 1, kemungkinan ke-3 S[0] berisi 2 dan seterusnya.

RC4 juga berisi indek i dan j yang berisi masing-masing bernilaidari 0 hingga 255. Setiap perubahan i dan j juga akan mempengaruhi keluaran k. Sehingga kemungkinan keadan yang internal RC4 yang dipengaruhi oleh i dan j adalah 256 X $256=256^2$.

Total keadaan internal RC4 yang dipengaruhi i, j dan permutasi kotak S

menjadi sebanyak 256! X 256^2 kemungkinan atau 2^{1700} kemungkinan keadaan yang dapat terjadi didalam RC4, suatu jumlah yang sangat besar.

Pada kondisi nyata, semua algoritma enkripsi data yang ada masih dapat dipecahkan kuncinya oleh para kriptanalis, hal ini menunjukan tidak ada algoritma enkripsi data yang sempurna termasuk juga disini algoritma RC-4

1. Lingkungan Perangkat Lunak Implementasi

Spesifikasi perangkat keras yang digunakan dalam implementasi perangkat lunak adalaha seperti pada tabel 5.1 dibawah ini :

Tabel 5.1 Spesifikafi perangkat keras implementasi

No	Spesifikasi Perangkat Keras Lingkungan Implementasi	
1	Prosessor	AMD Athlon XP 1700+
2	Memory	256 MB DDR
3	Harddisk	40 GB
4	Monitor	Samsung 15”
5	Perangkat keras lainnya	Mouse, Keyboard, dll

2. Lingkungan Perangkat Lunak Implementasi

Spesifikasi perangkat lunak dalam implementasi perangkat lunak adalah seperti pada table 5.2 dibawah ini :

Tabel 5.2 Spesifikafi perangkat lunak implementasi

Perangkat Lunak	Spesifikasi
Sistem Operasi	Windows 2000 Profesional
Perangkat Lunak Pengembangan	Windows Embedded Visual Tools
Emulator	Microsoft Windows Flatform SDK for Pocket PC

5. Kesimpulan

Kesimpulan yang didapatkan dari implementasi kriptografi algoritma RC4 yaitu :

1. Berdasarkan analisis penghitungan manual dengan menyederhanakan kunci dan state array, kemudian diuji dengan aplikasi yang dibuat maka hasilnya sama, sehingga algoritma yang dibuat berdasarkan perancangan dan penghitungan manual telah sesuai.
2. Secara umum aplikasi yang dibuat dikatakan berhasil berdasarkan pengujian-pengujian yang dilakukan sehingga tujuan dari penulisan tugas akhir ini tercapai.
3. Semakin panjang kunci yang digunakan tidak terlalu mempengaruhi waktu proses enkripsi maupun dekripsi.
4. Untuk kapasitas yang cukup besar, aplikasi ini kurang efektif karena akan membutuhkan waktu yang lama bahkan bisa terjadi *crash.* Hal ini akan mempengaruhi kinerja dari Pocket PC. Untuk kapasitas 227973 Byte saja membutuhkan waktu lebih kurang 278 detik.
5. Semakin besar kapasitas file yang dienkripsi atau didekripsi maka semakin lama waktu proses enkripsi dan dekripsi
6. Kapasitas file sebelum ataupun sesudah proses enrkipsi/dekripsi tidak mengalami perubahan.

7. Daftar Pustaka

Hariyanto, Bambang., Hendrowati, Retno,. 2000..*Logika Matematika.* Bandung : Informatika.

Hartono, Jogiyanto. 1999. *Pengenalan Komputer*. Yogyakarta : ANDI.

Halvorson, Michael. 1999. *Step By Step Microsoft Visual Basic 6.0*

Professional. Jakarta : Elex Media Komputindo.

Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung : Informatika.

Pressman, Roges S. 2002. *Rekayasa Perangkat Lunak Pendekatan Praktis Buku Satu*. ANDI Yogyakarta.

Rahardjo, Budi. 2002. *Keamanan Sistem informasi Berbasis Intenenet*. Bandung : PT Insan Komunikasi Indonesia.

Schneier, Bruce. 1996. *Applied Cryptography 2nd Edition.*