Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Vol.20. No.1, Februari 2021, pp. 38~43
P-ISSN : 1978-6603
E-ISSN : 2615-3475

Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks

Adriansyah Tampubolon
Program Studi Teknik Informatika Fakultas Teknik dan Komputer Universitas Harapan Medan

Article Info
Article history:
Received Jul 12th, 2020
Revised Aug 20th, 2020
Accepted Oct 26th, 2020

Keyword:
Kriptografi, Pengamanan Data, Pesan Teks, Algoritma RSA, Algoritma DES

ABSTRACT
Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data. Kriptografi sangat dibutuhkan dalam pengamanan data. Salah satu masalah dalam pengamanan data adalah pencurian data. Pencurian data biasanya dilakukan untuk melakukan tindakan kejahatan, seperti penyalahgunaan data untuk kriminalitas. Penulis berkeinginan untuk melakukan pengamanan pesan teks menggunakan kombinasi algoritma RSA dengan algoritma DES. Jika hanya menggunakan algoritma RSA, keamanan dari suatu pesan teks masih terancam. Tingkat keamanan algoritma RSA bergantung pada ukuran kunci yang dipakai, semakin kecil ukuran kunci maka semakin mudah ditembus menggunakan metode *bruteforce*. Pesan teks akan dienkripsi terlebih dahulu menggunakan algoritma RSA kemudian menggunakan algoritma DES. Dalam proses dekripsi pesan teks didekripsi menggunakan algoritma DES kemudian menggunakan algoritma RSA agar mendapatkan plainteks awal. Hasil dari penelitian ini ditujukan untuk masyarakat, khususnya di bidang keamanan data.

Corresponding Author:
Nama : Adriansyah Tampubolon
Program Studi : Program Studi Teknik Informatika Fakultas Teknik dan Komputer
Universitas Harapan Medan
Email:

1. PENDAHULUAN

Dalam perkembangan ilmu pengetahuan dan teknologi saat ini, masalah dalam pengamanan data masih merupakan suatu aspek penting di dalam penyimpanan data, khususnya dokumen yang sangat penting dan sangat sering digunakan dalam kehidupan. Salah satu masalah dalam pengamanan data adalah pencurian data. Pencurian data biasanya dilakukan untuk melakukan tindakan kejahatan, seperti penyalahgunaan data untuk kriminalitas. Dengan adanya kejahatan pencurian data mengakibatkan pengguna merasa tidak aman jika tidak melakukan suatu tindakan dalam mengamankan dokumen yang disimpan. Dalam mengamankan dokumen, dapat dilakukan dengan metode – metode yang ada dalam kriptografi. Kriptografi merupakan ilmu atau seni untuk menjaga atau mengamankan sebuah informasi yang dikirim dari suatu tempat ke tempat lain. Peran kriptografi dalam mengamankan dokumen yaitu menggunakan teknik enkripsi yang menyebabkan dokumen tidak dapat dibaca oleh kriptanalis. Kriptanalis adalah orang yang memecahkan *chipertext* menjadi *plaintext* tanpa mengetahui kunci dan algoritma yang digunakan.

Salah satu metode dalam kriptografi adalah algoritma RSA. Algoritma RSA dibuat oleh tiga orang peneliti dari MIT *(Massachussets Institute of Technology)* pada tahun 1976, yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. Algoritma RSA adalah salah satu teknik kriptografi di mana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci *private*.

Penulis akan melakukan kombinasi algoritma RSA dengan salah satu algoritma yang cukup kuat dan populer yaitu algoritma DES. Kombinasi dilakukan karena, jika hanya menggunakan algoritma RSA tingkat keamanan dari suatu *file* masih terancam. Tingkat keamanan algoritma RSA bergantung pada ukuran kunci yang digunakan sebagai sandi. Semakin kecil ukuran kunci, maka semakin mudah ditembus menggunakan metode *bruteforce* (memeriksa satu per satu kombinasi kunci). Sehingga penulis yakin, jika algoritma RSA dan algoritma DES dikombinasikan akan menghasilkan tingkat keamanan yang bagus, karena rumitnya proses di dalam algoritma DES.

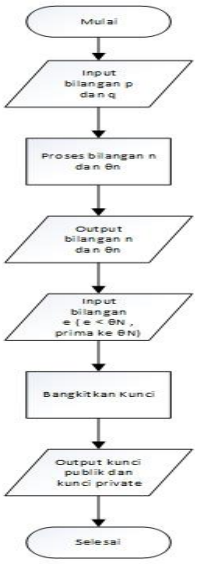
Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST *(National Institue of Standards and Technology)* sebagai standar pengolah informasi Federal AS. *Plaintext* dienkrip dalam blok-blok 64 bit menjadi 64 bit data *ciphertext* menggunakan kunci 56 bit kunci internal *(internal key).* DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, algoritma DES termasuk ke dalam algoritma *block cipher*. Berdasarkan tahapan dan kunci yang sama, algoritma DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal *(external key)* 64 bit. Algoritma DES beroperasi pada ukuran blok 64 bit. Algoritma DES mengenkripsikan 64 bit *plaintext* menjadi 64 bit *ciphertext* dengan menggunakan 56 bit kunci internal *(internal key)* atau up-kunci *(subkey).* Kunci internal dibangkitkan dari kunci eksternal *(external key)* yang panjangnya 64 bit.

Telah dilakukan sebuah penelitian mengenai implementasi Algoritma Data Encryption Standard pada penyandian *record database*. Hasil dari penelitian ini membuktikan bahwa penyandian *record database* berdasarkan algoritma DES mampu mempersulit pihak-pihak lain untuk memahami dan mengerti isi dari *record database*. [1] (Yanti, N. R et al, 2018)

2. PERANCANGAN

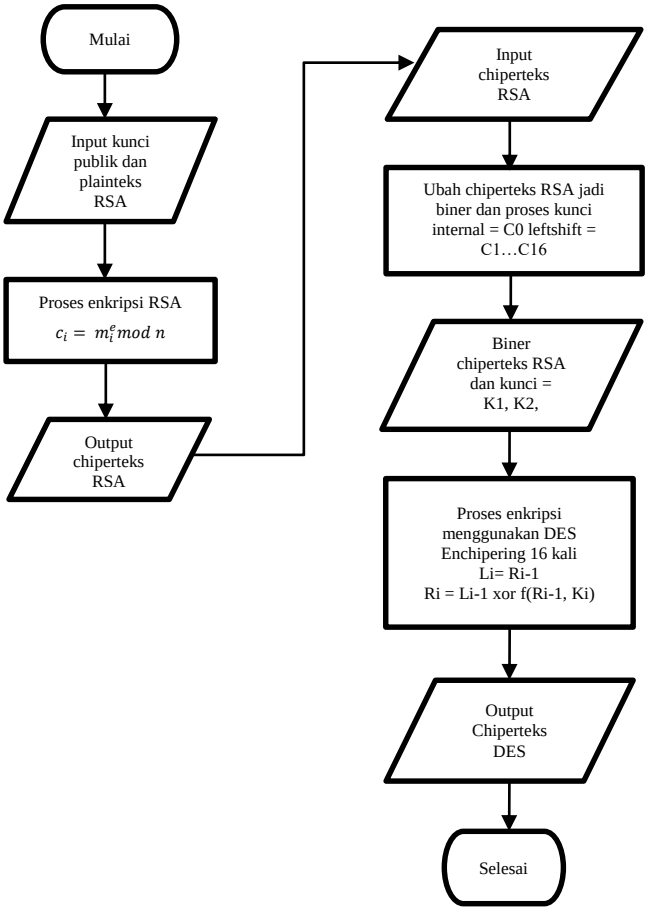
Perancangan proses pembangkitan kunci RSA dapat dilihat pada *flowchart* di bawah ini.

3.



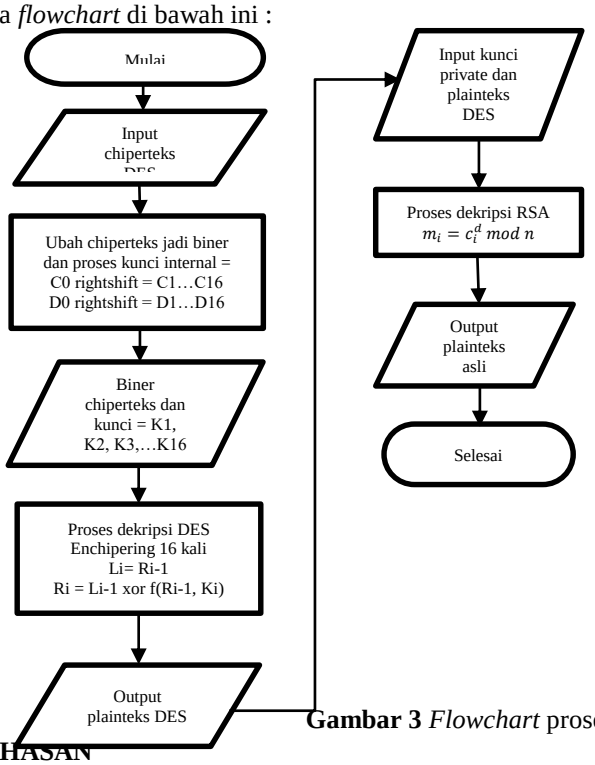
Gambar 1 *flowchart* kunci RSA

Proses enkripsi dilakukan melalui beberapa tahap, yaitu proses enkripsi menggunakan algoritma RSA kemudian hasil dari proses enkripsi RSA dienkripsi lagi menggunakan algoritma DES. Perancangan proses enkripsi dapat dilihat pada *flowchart* di bawah ini :



Gambar 2 *flowchart* proses enkripsi

Proses dekripsi dilakukan melalui beberapa tahap, yaitu proses dekripsi menggunakan algoritma DES kemudian hasil dari proses dekripsi DES didekripsi lagi menggunakan algoritma RSA. Perancangan proses dekripsi dapat dilihat pada *flowchart* di bawah ini :



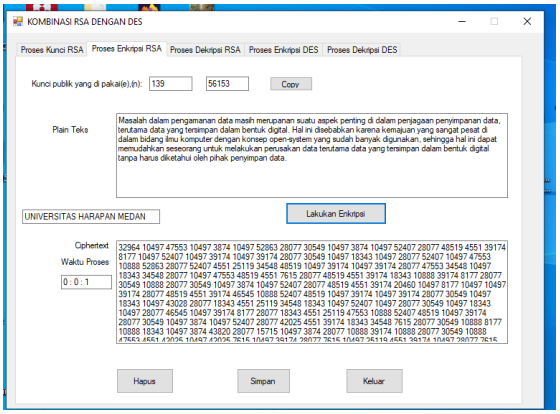
Gambar 3 *Flowchart* proses dekripsi

3.HASIL DAN PEMBAHASAN

Hasil kombinasi dari algoritma RSA dan algoritma DES dilakukan secara terpisah. Plainteks awal dienkripsi menggunakan algoritma RSA terlebih dahulu. *Chiperteks* RSA yang berbentuk bilangan desimal dienkripsi lagi menggunakan algoritma DES, sehingga hasil dari enkripsi DES sudah berbentuk simbol – simbol yang tidak dapat dipahami. Pada proses dekripsi juga dilakukan secara terpisah, *chiperteks* awal didekripsi menggunakan algoritma DES terlebih dahulu, sehingga mendapatkan hasil bilangan desimal. Kemudian *chiperteks* bentuk desimal didekripsi lagi menggunakan algoritma RSA sehingga mendapatkan plainteks awal.

3.1.1 Implementasi Form Proses Enkripsi RSA

Form proses enkripsi RSA akan ditampilkan jika *user* memilih *tab* proses enkripsi RSA. Penulis memasukkan kunci publik = (139, 22499). Selanjutnya memasukkan *plainteks* pada kolom yang disediakan. Penulis memasukkan *plainteks* "Microsoft visual studio 2012 merupakan sebuah perangkat lunak lengkap (suite) yang dapat digunakan untuk melakukan pengembangan aplikasi, baik itu aplikasi bisnis, aplikasi personal, ataupun komponen aplikasinya, dalam bentuk aplikasi console, aplikasi windows, ataupun aplikasi web. Visual studio 2012 mencakup kompiler, sdk, integrated development environment (ide), dan dokumentasi (umumnya berupa msdn library) ".



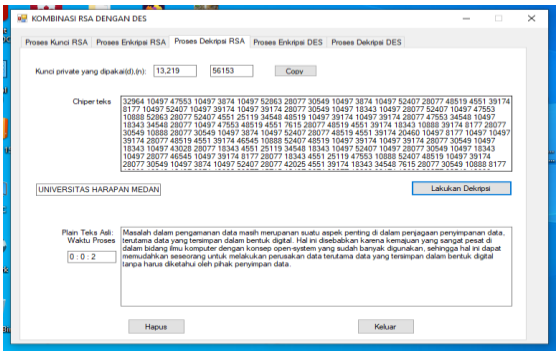
Gambar 3 Implementasi *form* proses enkripsi RSA

Pada gambar 3 dapat dilihat waktu yang digunakan untuk proses enkripsi RSA adalah 1 detik.

3.1.2 Impelementasi Form Proses Dekripsi RSA

Form proses dekripsi RSA akan ditampilkan jika *user* memilih *tab* proses dekripsi RSA. Penulis memasukkan kunci *private* = (11659, 22499). Selanjutnya memasukkan *chiperteks* pada kolom yang disediakan. Penulis memasukkan *chiperteks* "20722 3024 5796 9770 17499 7214 17499 12939 12890 14679 11594 3024 7214 11396 14212 21607 14679 7214 12890 11396 69 3024 17499 14679 14170 5499 13788 14170 14679 19594 21768 9770 11396 7205 14212 7893 14212 17545 14679 7214 21768 16758 11396 14212 2092 14679 7205 21768 9770 14212 17545 7336 7893 14212 12890 14679 21607 11396 17545 14212 7893 14679 21607 21768 17545 7336 7893 14212 7205 14679 15570 7214 11396 3024 12890 21768 13259 14679 916 14212 17545 7336 14679 69 14212 7205 14212 12890 14679 69 3024 7336 11396 17545 14212 7893 14212 17545 14679 11396 17545 12890 11396 7893 14679 19594 21768 21607 14212 7893 11396 7893 14212 17545 14679 7205 21768 17545 7336 21768 19594 16758 14212 17545 7336 14212 17545 14679 14212 7205 21607 3024 7893 14212 7214 3024 10982 14679 16758 14212 3024 7893 14679 3024 12890 11396 14679 14212 7205 21607 3024 7893 14212 7214 3024 14679 16758 3024 7214 17545 3024 7214 10982 14679 14212 7205 21607 3024 7893 14212 7214 3024 14679 7205 21768 9770 7214 17499 17545 14212 21607 10982 14679 14212 12890 14212 11396 7205 11396 17545 14679 7893 17499 19594 7205 17499 17545 21768 17545 14679 14212 7205 21607 3024 7893 14212 7214 3024 17545 916 14212 10982 14679 69 14212 21607 14212 19594 14679 16758 21768 17545 12890 11396 7893 14679 14212 7205 21607 3024 7893 14212 7214 3024 14679 5796 17499 17545 7214 17499 21607 21768 10982 14679 14212 7205 21607 3024 7893 14212 7214 3024 14679 11142 3024 17545 69 17499 11142 7214 10982 14679 14212 12890 14212 11396 7205 11396 17545 14679 14212 7205 21607 3024 7893 14212 7214 3024 14679 11142 21768 16758 8905 14679 380 3024 7214 11396 14212 21607 14679 7214 12890 11396 69 3024 17499 14679 14170 5499 13788 14170 14679 19594 21768 17545 5796 14212 7893 11396 7205 14679 7893 17499 19594 7205 3024 21607 21768 9770 10982 14679 7214 69 7893 10982 14679 3024 17545 12890 21768 7336 9770 14212 12890 21768 69 14679 69 21768 11594 21768 21607 17499 7205 19594 21768 17545 12890 14679 21768 17545 11594 3024 9770 17499 17545 19594 21768 17545 12890 14679 15570 3024 69 21768 13259 10982 14679 69 14212 17545 14679 69 17499 7893 11396 19594 21768 17545 12890 14212 7214 3024 14679 15570 11396 19594 11396 19594 17545 916 14212

14679 16758 21768 9770 11396 7205 14212 14679 19594 7214 69 17545 14679 21607 3024 16758 9770 14212 9770 916 13259 8905’’

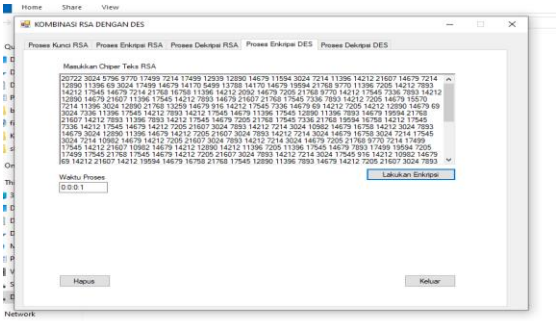


Gambar 4 Implementasi *form* dekripsi RSA

Pada gambar 3 dapat dilihat waktu yang digunakan untuk proses dekripsi RSA sedikit lebih lama dari proses enkripsi yaitu 2 detik.

3.1.3 Implementasi Form Proses Enkripsi DES

Form proses enkripsi DES akan ditampilkan jika *user* memilih *tab* proses enkripsi DES. Pada penggunaannya kolom chiperteks RSA akan otomatis terisi pada saat penulis melakukan proses enkripsi RSA sebelumnya.

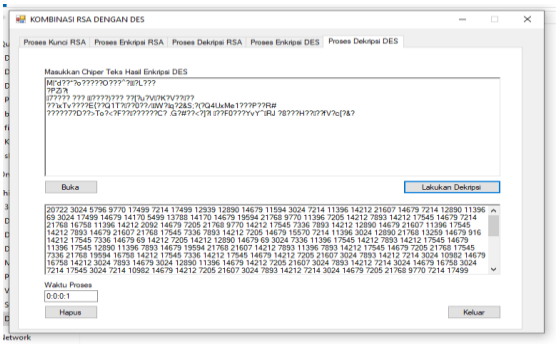


Gambar 5 Implementasi *form* enkripsi DES

Pada gambar 5 dapat dilihat waktu yang dibutuhkan untuk proses enkripsi DES sama dengan waktu yang dibutuhkan pada proses enkripsi RSA yaitu 1 detik.

3.1.4 Implementasi Form Proses Dekripsi DES

Form proses dekripsi DES akan ditampilkan jika *user* memilih *tab* proses dekripsi DES. Pada penggunaannya kolom chiperteks hasil enkripsi DES akan otomatis terisi pada saat penulis melakukan proses enkripsi DES sebelumnya.



Gambar 6 Implementasi *form* dekripsi DES

Pada gambar 6 dapat dilihat waktu yang dibutuhkan untuk proses dekripsi DES sama dengan waktu yang dibutuhkan pada proses enkripsi DES yaitu 1 detik.

4. PENUTUPAN

1.1 Kesimpulan

Berdasarkan hasil penulisan ini, dapat disimpulkan beberapa hal mengenai implementasi kombinasi Algoritma RSA (Riverst Shamir Adleman) dan Algoritma DES (Data Encryption Standard*)* pada aplikasi pengaman pesan teks. Kesimpulannya adalah sebagai berikut:

1. Pesan teks diamankan menggunakan kombinasi algoritma RSA dan algoritma DES. Proses pengamanan pada aplikasi ini dilakukan terpisah. Hasil dari enkripsi algoritma RSA dienkripsi lagi menggunakan algoritma DES, begitupula pada proses dekripsinya.
2. Aplikasi yang menerapkan kombinasi algoritma RSA dan algoritma DES ini berjalan dengan baik dan mampu mengenkripsi dan mendekripsi pesan teks sehingga dapat meningkatkan keamaan suatu pesan.
3. Pada aplikasi yang dibangun, satu *plainteks* dapat menghasilkan bermacam – macam *chiperteks* menggunakan algoritma RSA dikarenakan proses pembangkitan kunci RSA didasarkan oleh bilangan prima p dan q yang diinputkan
4. Hasil dari kombinasi algoritma RSA dan algoritma DES menjadi simbol – simbol yang lebih rumit, sehingga lebih sulit untuk ditembus menggunakan metode *bruteforce.*

1.2 Saran

Berdasarkan hasil penulisan ini, aplikasi dapat dikembangkan lagi agar menjadi lebih baik, sehingga penulis mengajukan beberapa saran. Saran tersebut adalah sebagai berikut:

1. Untuk meningkatkan keamanan algoritma DES, dapat dilakukan penelitian lebih lanjut mengenai pengembangan dari algoritma DES, yaitu algoritma *Triple* DES.

2. Aplikasi yang dibangun masih memiliki banyak kekurangan, terutama dalam masalah penampungan nilai yang terbatas, diharapkan untuk ke depannya aplikasi dapat dikembangkan agar menjadi lebih baik lagi.

5. DAFTAR PUSTAKA

[1] Yanti, N. R., Alimah, A., & Ritonga, D. A. (2018). Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, *2*(1), 23.

[2] Basri. (2016). Kriptografi simetris dan asimetris dalam perspektif keamanan data dan kompleksitas komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2).

[3] Devha, C. (2013). Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA). *Universitas Pendidikan Indonesia*, 39–73.

[4] Donzilio Antonio Meko. (2018). Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu. *Jurnal Teknologi Terpadu*, *4*(1), 8–15.

[5] Hasibuan, A. Z., Asih, M. S., & Harahap, H. (2019). Penerapan QR Code dan Vigenere Cipher Dalam Sistem Pelaporan Juru Parkir Ilegal. *Jurnal Sistem Informasi*, *5341*(April), 53–61.

[6] Kurniawan, R. (2017). Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan RSA. *Jurnal Ilmu Komputer Dan Informatika*, *01*(November), 46–52.

[7] Maryanto, B. (2008). Penggunaan Fungsi Hash Satu-Arah untuk Enkripsi Data. *Media Informatika*, *7*(3), 1–10.

[8] Pahrizal, P., & Pratama, D. (2016). Implementasi Algoritma Rsa Untuk Pengamanan Data Berbentuk Teks. *Pseudocode*, *3*(1), 44–49.

[9] Primartha, R. (2011). Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). *Sriwijaya Journal of Information Systems*, *3*(2), 371–387.