PENGAMANAN DATA PADA LALU LINTAS DATA MENGGUNAKAN FUNGSI KRIPTOGRAFI RSA DARI SERANGAN SNOOPING

Lia Cintia Purba[1],Lila Agustini[2],Sri Rahmayani[3],Indra Gunawan[4]
STIKOM Tunas Bangsa Pematangsiantar

Abstrak

Abstrak- Perkembangan teknologi saat ini begitu pesat kemajuan nya ,terutama pada perkembangan teknologi jaringan komputer. Perkembangan teknologi jaringan komputer menyebabkan terkaitnya satu komputer dengan komputer lainnya sehingga dapat melakukan pertukaran data . Dalam era ini yang dimaksud dengan pertukaran data antara dua buah komputer bisa menjadi hal yang sangat luas ,sebagai contoh perjalanan sebuah e-mail dari satu server ke server yang lainnya.Dan Dalam perkembangan teknologi ini membuka besar peluang dalam pengembangan aplikasi komputer akan tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data oleh pihak pihak yang tidak bertanggung jawab dan sangatlah merugikan sipemilik data. Saat ini kita sangat mebutuhkan pengamanan terhadap lalu lintas data pada jaringan. Dengan meningkatkan keamanan menggunakan fungsi kriptografi RSA kita bisa lebih percaya tingkat keamanan data lebih terjaga dari serangan yang dilakukan oleh pihak pihak tidak bertanggung jawab.Data juga dapat terjaga keasliannya dan lebih efisien.

Kata Kuci- Pengamanan data , Kriptografi, RS

1. Pendahuluan

1.1. Definisi snooping

Snooping merujuk pada kegiatan yang bermaksud mendapatkan data yang tengah terkirim pada jaringan biasanya melalui akses yang tidak berwenang, contoh aktifitas snooping misalnya sebuah email disadap oleh penyerang .untuk mengalahkan penyerang sehingga aktifitas snooping tidak bermakna data yang terkirim

DOI : https://doi.org/10.29103/techsi.v11i3.1971

dibuat tidak kasat mata (*nonintelligible*)dengan menggunakan mekanisme penyandian(*encipherment*) [1]. *Encipherment* adalah sebuah mekanisme keamanan jaringan yang digunakan menyembunyikan data dan menyediakan layanan kerahasiaan data.

1.2. Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani, "kryptós" yang berarti tersembunyi dan "gráphein" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan menjadi "tulisan tersembunyi". Menurut Request for Comments(RFC), kriptografi adalah ilmu matematika yang berhubungan dengan transformasi data agar arti dari data tersebut menjadi sulit untuk dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnyadari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga dapat diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang mudah dipahami.Sehingga, kriptografi juga dapat diartikan sebagai proses untuk melindungi data dalam artiyang luas [2].kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan.Namun pada pengertian modern Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi madern adalah tidak saja hanya berurusan dengan penyembunyian namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi[1]. Kriptografi berasal dari bahasa yunani, *crypto* dan *graphia. Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing*(tulisan).menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari satu tempat ke tempat yang lain[3]. Pengertian Kriptografi dalam kamus bahasa Inggris Oxford adalah sebagai berikut :" Sebuah teknik rahasia dalam penulisan, dengan karakterkhusus, dengan

DOI : https://doi.org/10.29103/techsi.v11i3.1971

mengguanakan huruf dan karakter di luarbentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci,juga semua hal yang ditulis dengan cara seperti ini."Jadi, secara umun kriptografi diartikan sebagai seni menulisatau memecahkan cipher [6]. Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat dilihat pada buku David Kahn yangberjudul *The Codebreakers*. Buku dengan tebal 1000 halaman ini menuliskan secara jelas tentang sejarahkriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang terdapatpada piramid) hingga penggunaan kriptografi pada abad ke-20 [7].Sehingga dengan menggunakan Kriftografi kita dapat mengamankan data lebih efisien dari serangan serangan yang dilakukan oleh pihak tidak bertanggung jawab.

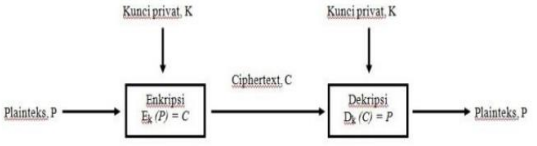
1). Jenis Kriptografi-:

1.1. Kriptografi kunci asimetri yang sering disebut juga kriptografi kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma asimetri ini disebut kunci publik karena kunci untuk enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya. Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (receiver). Hanya penerima pesan yang dapat mendekripsi pesan karena hanya dia yang mengetahui kunci privatnya sendiri [4]. *Algoritma Simetris* Algoritma simetris adalah salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Istilah lain untuk kriptografi kunci simetri adalah kriptografi kunci privat (*private-keycryptography*). Sistem kriptografi kunci-simetri diasumsikan sebagai pengirim dan penerima pesan yang sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan system kriptografi simetri terletak

DOI : https://doi.org/10.29103/techsi.v11i3.1971

pada kerahasiaan kuncinya.Kriptografi simetri adalah jenis kriptografi yang diketahui masuk ke dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam system kriptografi simetri. Salah satu kelebihan pada algoritma simetris yaitu proses enkripsi dan deskripsinya jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahannya yaitu pada permasalahan distribusi kunci (*keydistribution*). Seperti yang telah dibahas sebelumnya, proses enkripsidan deskripsi pada kriptografi simetri menggunakan kunci yang sama. Sehingga timbul persoalan untuk menjaga kerahasian kunci. Contohnya pada saat pengiriman kunci dilakukan melalui media yang tidak aman seperti internet.Jika kunci ini hilang atau sudah diketahui oleh orang yang tidak berhak, maka kriptosistem ini dinyatakan tidak aman lagi. Kelemahan lain adalah masalah efisiensi jumlah kunci.Jika terdapat n user, maka diperlukan $n(n\text{-}1)/2$ kunci, sehingga untuk jumlah user yang sangat banyak, sistem ini

tidak efisien lagi [7]



Gambar 1. Skema Kriptografi Simetri

.

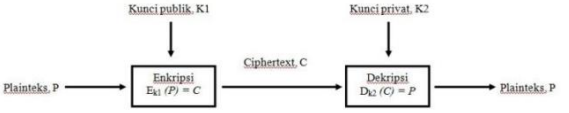
1.3. Algoritma Asimetris

Algoritma Asimetris atau dapat disebut juga dengan algoritma kunci public, didesain sebaik mungkin sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci dekripsinya. Dimana kunci untuk enkripsi tidak rahasia (diumumkan ke publik), sementara kunci dekripsinya bersifat rahasia (hanya diketahui oleh penerima pesan). Pada kriptografi asimetris, setiap orang yang akan berkomunikasi harus mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim pesan akan

DOI : https://doi.org/10.29103/techsi.v11i3.1971

mengenkripsi pesan menggunakan kunci publik si penerima pesan dan hanya penerima pesan yang dapat mendekripsi pesan tersebut karena hanya ia yang mengetahui kunci privatnya sendiri. Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci.Sistem ini memiliki dua keuntungan. Yang pertama yaitu, tidak ada kebutuhan untuk mendistribusikan kunci privatsebagaimana pada sistem kriptografi simetri. Kunci public dapat dikirim ke penerima pesan melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman. Kedua, jumlah kunci yang digunakan untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetris yangmembuat kunci sebanyak jumlah pihak yang diajak berkorespondensi.Meski masih terbilang baru (sejak 1976), kriptografi kunci-publik mempunyai kontribusi yang luar biasa dibandingkan dengan sistem kriptografi simetri. Kontribusi yang paling penting adalah tanda-tangan digital pada pesan untuk memberikan aspek keamanan otentikasi, integritas data, dan nirpenyangkalan. Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Pengirim pesan mengenkripsi pesan (yang sudah diringkas) dengan kunci privatnya, hasil enkripsi inilah yang dinamakan tanda-tangan digital. Tanda-tangan digital dilekatkan (embed) pada pesan asli. Penerima pesan memverifikasi tanda-tangan digital dengan menggunaklan kunci public [8].

DOI : https://doi.org/10.29103/techsi.v11i3.1971



Gambar 2. Skema Kriptografi Asimetri

2. Metode Penelitian

2.1. Algoritma RSA

Algoritma RSA adalah algoritma yang ditemukan oleh tiga orang peniliti Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman pada tahun 19977,dengan merumuskan implementasi kunci publik . Dalam kriptografi, RSA adalah algoritma untuk enkripsi kunci publik (public-key encryption). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (signing) dan untuk enkripsi (encryption) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapanpenerapannya yang sangat up-to-date(mutakhir). Terdapat 3 algoritma pada system kriptografi RSA yaitu algoritma pembangkitan kunci, algoritma enkripsi dan algoritma dekripsi.

1) Pembangkitan kunci dalam algoritma kriptografi RSA :

a) Memilih dua bilangan prima yang diberi symbol sebagai p dan q (nilai $p \neq q$).

b) Menghitung nilai n = p.q ($p \neq q$, karena jika p = q , maka nilai n = p2 sehingga nilai p dapat diperoleh dengan menarik akar pangkat dua dari n).

c) Hitung $\varphi(n) = (p - 1)(q - 1)$.

d) Memilih kunci publik e yang relatif prima terhadap (n).

e) Bangkitkan kunci privat dengan persamaan e . d ≡ 1 (mod (n)) dimana 1< < ( ). Perhatikan bahwa persamaan e . d ≡ 1 (mod (n))

DOI : https://doi.org/10.29103/techsi.v11i3.1971

ekivalen dengan e . d = 1 + k (n), sehingga untuk mencari nilai d dapat dihitung dengan

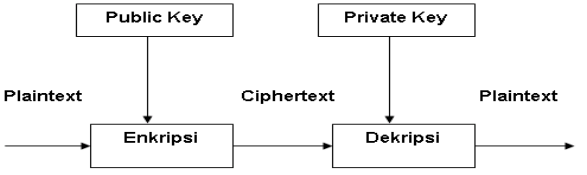
$$d = \frac{1 + k(n)}{e}$$

Hasil dari pembentukan pasangan kunci di atas adalah

a) Kunci publik (e, n)

b) Kunci rahasia (d, n)

Nilai n tidak bersifat rahasia karena diperlukan pada saat perhitungan proses enkripsi dan dekripsi.



Gambar 1. Diagram algoritma RSA

2) Proses enkripsi dalam algoritmakriptografi RSA-:

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption)[5]. Ciphertext adalah data yang telah tersandi dan tidak dapat dibaca oleh seseorang yang tidak memiliki kunci sandi tersebut.

Proses enskripsi:

a) Ambil kunci publik penerima pesan *e* dan modulus *n* atau (*e,n*).

b) Pilih plainteks *m* dan ubah isi pesan *m* menjadi pesan dengan nilai ASCII.

c) Potong pesan menjadi blok-blok pesan *m*1, *m*2, *m*3, ... dengan nilai setiap bloknya adalah $0 \le m \le n - 1$.

d) Setiap blok *m* dihitung dengan rumus *c*i = *mie* **mod** *n*.

e) Susun nilai *c* hasil enkripsi dengan susunan *c*1, *c*2, *c*3,....,*c*n sehingga diperoleh cipherteks dari pesan *m*.

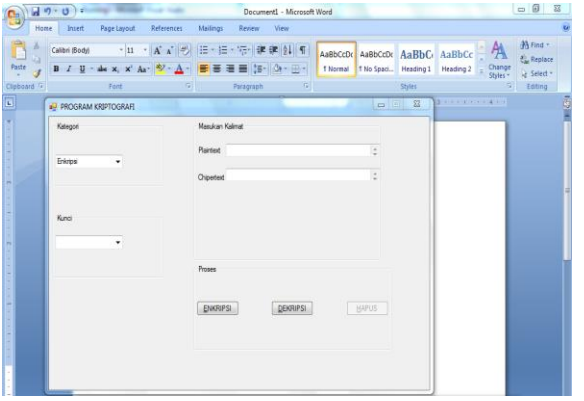
DOI : https://doi.org/10.29103/techsi.v11i3.1971

3) Proses dekripsi dalam algoritma kriptografi RSA - :
Dekripsi merupakan proses yang dilakukan untuk mengembalian data ke bentuk semula dari proses penyandian atau dengan kata lain proses pengubahan (data tersandi) ciphertext menjadi (data asli) plaintext. Plaintext adalah data yang masih murni belum tersandi atau bisa disebut dengan data asli.
Proses Deskripsi:
a) Ambil pesan (cipherteks) yang telah diterima.
b) Kemudian ambil kunci rahasia *d* dan modulus *n* atau (*d*,*n*).
c) Potong pesan menjadi blok-blok pesan *c*1, *c*2, *c*3, ... dengan nilai setiap bloknya adalah $0 \leq c \leq n - 1$. 4) Hitung $mi = cid \bmod n$. 5) Susun nilai *m* hasil dekripsi dengan susunan *m*1, *m*2, *m*3,....,*m*n sehingga diperoleh plainteks (pesan asli) dari cipherteks yang diterima.

3. Hasil dan Diskusi

3.1. Tampilan Awal Form
Pembuatan Form dihalaman ini dirancang menggunakan Visual Basic. NET.2010. pada saat merancang di aplikasi ini proses enkripsi dan dekripsi berada di satu halama yang sama atau di form yang sama.

DOI : https://doi.org/10.29103/techsi.v11i3.1971

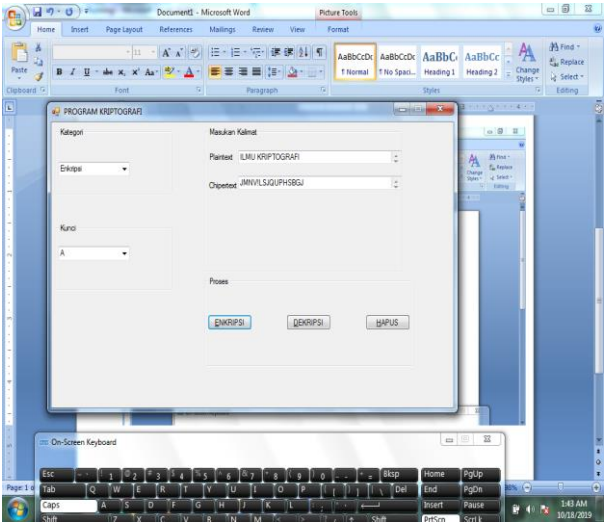


Gambar 1. Tampilan awal Form dari Enkripsi & Dekripsi

3.2. Tampilan Form Enkripsi

Button "Enkripsi" pada form ini berfungsi sebagai pengenkripsi (penyembunyi) text asli(plaintext) akan berubah menjadi text tersandi (Chipertext) jika button tersebut kita tekan. Maka text yang kita ketik pada kolom plaintext akan berubah menjadi text yang tersandi seperti yang ada dikolom chiphertext : pada gambar dibawah kita ketik text "ILMU KRIPTOGRAFI" dan kita pilih kunci yang kita inginkan disini kami menggunakan kunci "A" setelahitu kita tekan tombol "Enkripsi" maka plaintext akan berubah menjadi chipertext "JMNV!LSJQUPHSBGJ".

DOI : https://doi.org/10.29103/techsi.v11i3.1971

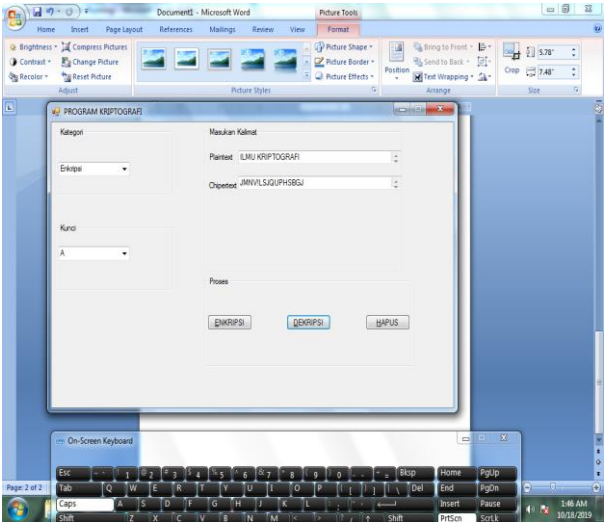


Gambar 2. Tampilan dari form hasil Enkripsi

3.3. Tampilan form Dekripsi

Button" Deskripsi" ini berfungi untuk mengembalikan text yang telah tersandi (Chipertext) menjadi (teks asli)plaintext. Dengan cara pilih kunci yang sama ketika kita mengenkripsi text tersebut kemudian ketik text tersandi tersebut kedalam textbox chipertext dan kemudian tekan button "Deskripsi" maka text tersandi akan berubah kembali menjadi text asli atau (plaintext) ditextbox Plaintext . Pada gambar dibawah kita ketik hasil dari enkripsi text tersebut pada textbox chipertext yaitu "JMNV!LSJQUPHSBGJ" kemudian kita tekan button "Dekripsi" maka chipertext akan berubah menjadi plaintext yaitu "ILMU KRIPTOGRAFI"

DOI : https://doi.org/10.29103/techsi.v11i3.1971



Gambar 3. Tampilan dari Form Hasil Dekripsi

4. Kesimpulan

Dari proses perancangan dan implementasi Kriptografi RSA dengan enkripsi dan dekripsi didapat kesimpulan bahwa Kriptografi RSA ini dapat membantu untuk memberi pengamanan pada data kita dari serangan snooping. Sehingga dengan menggunakan kriptografi RSA ini kita bisa mengurangi rasa khawatir kita terhadap serangan serangan sooping .

Referensi

Sadikin,Rifki.2012.Kriftografi Untuk Keamanan Jaringan. Andi Offset: Yogyakarta.

Oppliger, Rolf. 2005. *Contemporary Cryptography*. USA: Artech House, Inc.

Ariyus, D 2008. Pengantar Ilmu Kriptografi. Andi Offset : Yogyakarta.

Munir, R. 2006. Kriptografi. Informatika: Bandung.

DOI : https://doi.org/10.29103/techsi.v11i3.1971

Aulia, N. Aplikasi Enkripsi dan Dekripsi menggunkan Visual Basic 2012 dengan Algoritma Triple DES,20 Mei 2016.

Talbot, Jhon dan Dominic Welsh. 2006. Complexity and Cryptography. USA : Cambridge University Press.

Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography.* USA : CRC Press, Inc.

Zelvina Anandia, Efendi Syahril, Arisandi Dedy" Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa" JURNAL DUNIA TEKNOLOGI INFORMASI Vol. 1, No. 1, (2012) 56-62

DOI : https://doi.org/10.29103/techsi.v11i3.1971