ISSN : ISSN 2962–5688
Website :
jurnal.umj.ac.id/index.php/TripleA
Email : triplea@umj.ac.id

TRIPLE A
Jurnal Pendidikan Teknologi Informasi

PENGGUNAAN PUBLIC KEY INFRASTRUCTURE KUNCI PERSETUJUAN (*KEY AGREEMENT*)

Surnawani[1]*), Sodikin Jarkasih[2]*), Umul Fatimah[3]*)
[1)] Psikologi, Depertemen Psikologi, Universitas Negeri Padang, Jln. Prof. Dr. Hamka, Air Tawar, Kec. Padang Barat, Padang, Sumatra Barat 25131
[2,3)]Pendidikan Teknologi Informasi, Fakultas Ilmu Pendidikan, Universitas Muhammadiyah Jakarta, Jl. K.H. Ahmad Dahlan, Cireundeu, Kec. Ciputat Timur, Kota Tangerang Selatan, Banten 15419

Surnawani10@gmail.com

ABSTRACT

Public-key cryptography is an encryption system that uses a pair of keys, a public key that can be shared and a private key known only to its owner. The generation of these keys relies on cryptographic algorithms that use mathematical properties to generate one-way functions. In such a system, anyone can encrypt a message using the recipient's public key. However, only the recipient can decrypt the result with the individual key. This lets them, for example, send a message to a server to encrypt it with their public key. The message may contain a new key used for symmetric cryptography. At this time, the client and server can exchange messages using the new symmetric key. This has the advantage that a higher speed of symmetric cryptography than asymmetric cryptography can be used.

Keywords*: Kriptografi, Key Infrastructure*

ABSTRAK

Kriptografi kunci publik adalah sistem enkripsi yang menggunakan sepasang kunci, yaitu kunci publik yang dapat dibagikan dan kunci privat yang hanya diketahui pemiliknya. Pembuatan kunci ini bergantung pada algoritma kriptografi yang menggunakan properti matematika untuk menghasilkan fungsi satu arah. Dalam sistem seperti itu, siapa pun dapat mengenkripsi pesan menggunakan kunci publik penerima. Namun, hanya penerima yang dapat mendekripsi hasil dengan kunci individu. Ini memungkinkan mereka, misalnya, mengirim pesan ke server untukmengenkripsinya dengan kunci publik mereka. Pesan mungkin berisi kunci baru yang

DOI:https://

digunakan untuk kriptografi simetris. Saat ini, klien dan server dapat bertukar pesan menggunakan kunci simetris yang baru. Ini memiliki keuntungan bahwa kecepatan kriptografi simetris yang lebih tinggi daripada kriptografi asimetris dapat digunakan.

Kata Kunci: *Kriptografi, Kunci Infrastruktur*

PENDAHULUAN

Kriptografi adalah ilmu menjaga keamanan informasi, termasuk proses enkripsi dan dekripsi. Enkripsi adalah proses memperbarui plaintext menjadi ciphertext, dan dekripsi adalah proses memperbarui ciphertext kembali menjadi plaintext. Enkripsi adalah landasan keamanan komputer dan jaringan karena fungsi utama komputer dan jaringan adalah data atau informasi. Komputer dan jaringan adalah alat untuk pertukaran data, sehingga data harus dilindungi dari penggunaan yang tidak sah. Salah satu metode yang paling umum digunakan untuk melindungi data adalah enkripsi. Kerahasiaan informasi penting saat ini. Informasi sensitif harus disembunyikan dari orang yang tidak berwenang.

Kriptografi, atau sering disebut ilmu data, adalah seni dan ilmu untuk melindungi kerahasiaan pesan dari pihak ketiga yang tidak sah yang mencoba mengaksesnya. Kriptografi awalnya digambarkan sebagai studi tentang penyembunyian pesan. Namun, dalam pengertian sekarang, kriptografi adalah ilmu yang didasarkan pada metode matematika yang terkait erat dengan keamanan informasi, seperti: kerahasiaan, keandalan data, integritas data, dan non-penolakan. Oleh karena itu, pemahaman kriptografi modern tidak hanya tentang penyembunyian pesan, tetapi juga tentang teknik yang menyediakan keamanan informasi.

Berdasarkan pembahasan tersebut, kriptografi memiliki sistem yang lebih spesifik untuk keamanan data, keaslian data yaitu kunci publik. Jadi apa artinya penguncian asimetris?

HASIL DAN PEMBAHASAN

Kriptografi kunci publik, juga dikenal sebagai kriptografi asimetris, adalah bentuk enkripsi di mana pengguna memiliki pasangan kunci. Kriptografi: kunci publik dan kunci privat. Kunci pribadi dirahasiakan sementara kunci publik dapat dibagikan secara luas. Kedua kunci tersebut berhubungan secara matematis, tetapi dalam prakteknya kunci privat tidak dapat diturunkan dari kunci publik. Pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat terkait.

Ada empat tujuan kriptografi, aspek yang mendasari tujuan kriptografi ini yang juga merupakan aspek keamanan kriptografi:

1) Confidentiality (Kerahasiaan)
   Dengan membuat pesan yang sangat sulit dipahami orang lain sehingga menjadi pesan rahasia.
2) Data Integrity (Integritas)
   Pesan dibuat seolah-olah belum pernah termanipulasi sebelumnya.
3) Autentication (Otentikasi)
   Mencari solusi pada orang yang sedang berkomunikasi.
4) Non-repudiation (Penyangkalan

Mencegah terjadinya pembatan pengiriman pesan dan juga sebaliknya.

Kunci asimetris adalah sepasang kunci enkripsi, satu digunakan untuk enkripsi dan yang lainnya digunakan untuk dekripsi. Siapapun yang menerima kunci publik dapat menggunakannya untuk mengenkripsi pesan, tetapi hanya satu orang yang memiliki rahasia khusus (dalam hal ini kunci privat) untuk mendekripsi kata sandi yang dikirim.

Misalnya, jika Lisa mengirim pesan ke Bob dengan cara ini, Alice dapat yakin bahwa hanya Pekka yang dapat membaca pesan tersebut karena hanya Bob yang dapat mendekripsi dengan kunci privatnya. Tentu saja, Alice harus memiliki kunci publik Bob untuk mengenkripsinya. Alice bisa mendapatkannya dari Bob atau dari pihak ketiga seperti Eve. Teknik enkripsi asimetris ini jauh lebih lambat daripada enkripsi simetris. Oleh karena itu, biasanya pesan itu sendiri tidak dienkripsi dengan kunci asimetris, hanya kunci simetris yang dienkripsi dengan kunci asimetris. Pesan dikirim setelah sebelumnya dienkripsi dengan kunci simetris. Contoh metode solusi yang dikenal dengan kunci asimetrik adalah RSA (singkatan berdasarkan penemunya yaitu Rivest, Shamir & Adleman) dan DSA (Digital Signature Algorithm) [1].

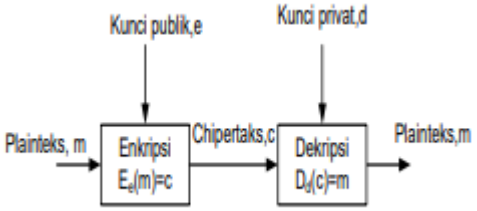
Enkripsi kunci publik yang digunakan dalam tanda tangan digital dapat dinyatakan sebagai berikut: Karena (M) = C D - (C) = M, dimana: E = enkripsi, D = dekripsi, M = pesan, C = enkripsi, kd = kunci privat, penerima = kunci publik [8]. Kunci enkripsi, juga dikenal sebagai kunci publik, tidak rahasia dan karenanya dapat dibagikan melalui saluran yang tidak aman. Meskipun kunci dekripsi juga dikenal sebagai kunci privat, namun bersifat rahasia dan harus dirahasiakan oleh pemilik kunci.

Kriptografi asimetris adalah algoritma yang menggunakan kunci berbeda dalam proses enkripsi dan dekripsi. Kunci enkripsi dapat dibagikan secara publik dan dikenal sebagai kunci publik, sedangkan kunci dekripsi disimpan untuk penggunaan pribadi dan dikenal sebagai kunci pribadi, oleh karena itu enkripsi ini juga dikenal sebagai kriptografi kunci publik. Contoh terkenal dari algoritma yang menggunakan kunci asimetris adalah RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Cryptography).

Transmisi data dalam jaringan publik berdasarkan satu sistem ke sistem lainnya bisa dilindungi menggunakan enkripsi. Enkripsi data memakai prosedur pemecahan enkripsi berbasis kunci. Hanya pengguna menggunakan akses ke kunci yg sama yg bisa mendekripsi data terenkripsi. Teknik ini dikenal menjadi kriptografi kunci misteri atau kunci simetris. Ada beberapa baku buat prosedur pemecahan simetris, misalnya AES & 3DES. Dalam pengujian, prosedur pemecahan kunci simetris terbukti aman.

Konsep Kriptografi Kunci Publik

Konsep kriptografi kunci publik sederhana, namun penggunaannya mempunyai akibat penting. Setiap pengguna mempunyai pasangan kunci, kunci publik buat enkripsi & kunci privat buat dekripsi. Gambar 1 menerangkan enkripsi kunci publik.



Gambar 1. Skema Kriptografi Kunci Publik

Konsep pada Gambar 1 digunakan untuk memastikan pertukaran data antara dua entitas yang berkomunikasi. Misalnya,

Alice berkomunikasi dengan Bob. Bob memilih pasangan kunci (e,d). Bob mengirimkan kunci enkripsinya (kunci publik) ke Alice melalui saluran apa pun, tetapi merahasiakan kunci dekripsi (kunci pribadi) miliknya. Kemudian Alice ingin mengirim pesan m menggunakan kunci publik Bob untuk menerima c=Ee(m) dan mengirimkan c sebagai saluran komunikasi (yang harus aman). Bob mendekripsi ciphertext c dengan kunci privatnya untuk mendapatkan m=Dd(c).

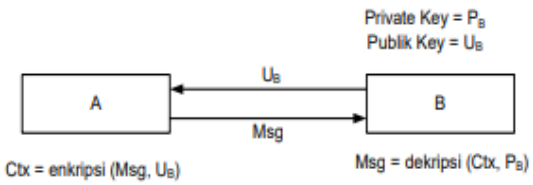
APLIKASI KUNCI PUBLIK

Kunci persetujuan (*Key agreement*)

Metode di mana perangkat yang berkomunikasi di jaringan membuat rahasia bersama tanpa bertukar informasi rahasia. Metode ini mengharuskan perangkat untuk berbagi rahasia dengan bertukar kunci publik. Dua perangkat menerima kunci publik dan menggunakan kunci pribadi untuk menghasilkan kunci untuk mengambil rahasia bersama.

Kerahasiaan data (Data encryption)

Enkripsi adalah sebuah proses pengamanan data dengan mengubah plaintext menjadi chipertext.



Gambar 2. Proses Data Encryption

Perangkat B memiliki kunci PB pribadi dan kunci UB publik, sedangkan semua perangkat lainnya dapat memiliki kunci UB publik. Untuk mengirim pesan dengan aman ke Perangkat B, data terlebih dahulu dienkripsi menggunakan kunci publik UB untuk mendapatkan ciphertext "Ctx". Pesan terenkripsi (ciphertext) hanya dapat didekripsi dengan kunci privat PB. Hanya B yang mengetahui kunci privat PB. Menurut perangkat B, perangkat A harus mendapatkan kunci publik yang valid. Tanda tangan digital membantu mentransfer kunci publik dalam proses otentikasi.

DISTRIBUSI KUNCI DAN SISTEM KUNCI PUBLIK

Teknologi digital telah mengurangi biaya Enkripsi ke tingkat yang hampir dapat diabaikan, di sana adalah masalah utama lainnya yang terlibat dalam mengamankan jaringan komunikasi. Salah satu persing adalah distribusi kunci, masalah aman mentransmisikan kunci ke pengguna yang membutuhkannya. Situasinya dianalogikan seperti memiliki sebuah ruangan penuh dengan orang-orang yang belum pernah bertemu sebelumnya dan yang memiliki kemampuan matematika yang sama.

Saya memilih satu orang lain di ruangan itu dan, dengan semua orang lain mendengarkan, memberinya instruksi yang memungkinkan Kami berdua untuk melakukan percakapan yang orang lain dapat mengerti. Saya kemudian memilih yang lain orang dan melakukan hal yang sama dengan dia. Ini terdengar agak mustahil dan, dari Satu sudut pandang, itu. Jika cryptanalyst punya waktu komputer tak terbatas yang bisa dia pahami Semua yang kami katakan. Tapi itu juga berlaku untuk sebagian besar Sistem kriptografi konvensional-kriptografi Analis dapat mencoba semua kunci sampai dia menemukannya Yang menghasilkan penguraian yang bermakna dari Pesan yang disadap.

Pertanyaan sebenarnya adalah Apakah kita bisa, dengan perhitungan yang sangat terbatas,Bertukar pesan yang akan

mengambil cryptan-Alyst ribuan tahun untuk memahami menggunakan yang paling kuat Komputer dapat dibayangkan.Sebuah kriptosistem kunci publik memiliki dua kunci,Satu untuk penyandian dan satu untuk penguraian. Sementara dua tombol efek operasi invers dan oleh karena itu terkait, tidak boleh ada yang mudah Metode komputasi untuk menurunkan penguraian kunci dari kunci penyandian. Penyandian kunci kemudian dapat dibuat publik tanpa kompromi Salah kunci penguraian sehingga siapa pun bisa Mengenkripsi pesan, tetapi hanya penerima yang dimaksud Ent dapat menguraikan pesan.

Pengirim dan penerima menggunakan saluran aman untuk menyepakati kombinasi (kunci) dan kemudian dapat dengan mudah mengunci dan membuka kunci (mengenkripsi dan mendekripsi) pesan, tetapi tidak ada orang lain yang bisa. Sistem enkripsi kunci publik dapat dibandingkan dengan brankas matematika dengan reset - kunci kombinasi tabel baru dengan dua kombinasi ion, satu untuk membuka kunci dan satu untuk membuka kunci.

Dengan membuat kombinasi penguncian (enciphering kuncinya) publik siapa pun dapat mengunci informasi, Tetapi hanya penerima yang dituju yang mengetahui Kombinasi unlocking (deciphering key) bisa Buka kunci kotakuntuk memulihkan informasi.

SIMPULAN

Kita berada di tengah-tengah revolusi komunikasi yang akan berdampak pada banyak aspek kehidupan masyarakat Setiap hari hidup. Kriptografi adalah hal yang penting bahan dalam revolusi ini, dan diperlukan untuk Menjaga privasi dari sensor terkomputerisasi Mampu memindai jutaan halaman dokumen Ments bahkan untuk satu datum sensitif. Masyarakat konsep kunci dan tanda tangan digital diperlukan dalam sistem komersial karena banyaknya ber interkoneksi yang mungkin, dan karena kebutuhan untuk menyelesaikan perselisihan.

Masalah utama yang dihadapi kriptografi adalah sertifikasi sistem ini. Bagaimana kita bisa memutuskan sistem yang diusulkan mana yang benar-benar aman, dan mana yang hanya tampak aman? Buktinya tidak mungkin menggunakan teori yang dikembangkan saat ini kompleksitas komputasi dan, sementara itu bukti mungkin di masa depan, sesuatu harus segera dilakukan. Saat ini menerima-teknik untuk sertifikasi system kriptografi seaman mungkin untuk membuatnya terkena serangan pura-pura dalam keadaan yang sangat menguntungkan-mampu cryptanalyst dan tidak menguntungkan untuk sistem. Jika system menolak seperti terpadu menyerang dalam kondisi yang tidak menguntungkan, diharapkan bahwa itu juga akan menahan serangan lawan seseorang dalam kondisi yang lebih realistis.Pemerintah telah membangun keahlian dalam area sertifikasi, namun karena kendala keamanan, saat ini tidak tersedia untuk sertifikasi sistem yang berorientasi komersial. Sebaliknya, ini keahlian di tangan pemerintah asing menimbulkan ancaman tersendiri bagi bisnis suatu negara. Dia bahkan telah disarankan bahwa miskin atau tidak ada enkripsi tenda akan mengarah pada eko-internasional perang nomic, perhatian penting untuk keamanan nasional. (Ada spekulasi bahwa ini terjadi dengan pembelian biji-bijian Rusia yang besar dari beberapa tahun yang lalu.) Ada tradeoff antara ini dan lainnya pertimbangan keamanan nasional yang perlu diselesaikan, tetapi penanganan data nasional standar enkripsi menunjukkan bahwa diskusi publik dan resolusi tradeoff tidak mungkin kecuali individu membuat

keprihatinan mereka diketahui di tingkat teknis dan politis.

DAFTAR PUSTAKA

A. Sadikin, Rifki. 2012."Kriptografi untuk Keamanan Jaringan". Yogyakarta : Andi.355-400

C, Febrian. Wahyu, Rahagiar, A. P., & Fretes, F. (2012)."Penerapan Algoritma Gabungan Rc4 dan Base64 Pada Sistem Keamanan E-Commerce". Seminar Nasional Aplikasi Teknologi Informasi. 47-52.

Halim Dermawan, D.A., 2014."Penerapan Algoritma RC4 untuk Enkripsi dan Dekripsi SMS Berbasis Android 1,2". Seminar Perkembangan dan Hasil penelitian ilmu komputer (SPHP-ILKOM), pp.79–87.

Menezes, A.J., Oorschot, P.C. Van & Vanstone, S. a, 1996."Handbook of Applied Cryptography". Stanford University, Electrical Engineering.

Munir, Rinaldi. 2006."Diktat Kuliah Kriptografi, Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika". Insitut Teknologi Bandung, Bandung.

Sarangih Sholihah U, (2017). "Implementasi enkripsi dan dekripsi dengan Metode Rc4 untuk Pengamanan Data Sistem Informasi". Universitas Bandar Lampung.13(1)1-92