Kriptografi Rivest Shamir Adleman (RSA) pada Tanda Tangan Digital

Dwi Puspitasari*, Yurika Permanasari

Prodi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Islam Bandung, Indonesia.

*dwipuspitasari2307@gmail.com, yurikakoe@gmail.com

Abstact. Digital signatures are a verification and authentication tool. Digital signatures contain cryptographic values that depend on the original document and the sender of the message, so it has a different form than the manual / conventional signature. Cryptographic values guarantee security, confidentiality, data integrity, authentication and non-repudiation. A digital signature in a document is a code generated through the message digest encryption process with a hash function. A hash function is a function that maps binary strings with variable length inputs into a binary string with a fixed output length. The cryptographic algorithm used for digital signatures is the RSA asymmetric cryptographic algorithm. The RSA algorithm process is based on euler theorem and its level of security lies in the difficulty of factoring large numbers into prime factors. RSA uses a key pair that is a public key pair for encrypting message digest which produces a digital signature and a private key for decryption. Document is declared valid if the digital signature decryption results are the same as message digest.

Keywords: Digital Signature, Asymmetric Cryptography, RSA Algorithm, Message Digest, Hash Function

Abstrak. Tanda tangan digital merupakan alat verifikasi dan autentifikasi. Tanda tangan digital mengandung nilai kriptografis yang bergantung pada dokumen asli dan pengirim pesan, sehingga memiliki bentuk yang berbeda dari tanda tangan manual/konvensional. Nilai kriptografis menjamin keamanan, kerahasiaan, integritas data, autentifikasi, dan nir-penyangkalan. Tanda tangan digital pada sebuah dokumen berupa sebuah kode yang dihasilkan melalui proses enkripsi *message digest* dengan fungsi *hash*. Fungsi *hash* merupakan fungsi yang memetakan string biner dengan panjang input bervariasi menjadi suatu string biner dengan panjang output tetap. Algoritma kriptografi yang digunakan untuk tanda tangan digital adalah algoritma kriptografi asimetri RSA. Proses algoritma RSA berdasarkan pada teorema euler dan tingkat keamanannya terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. RSA menggunakan pasangan kunci yaitu pasangan kunci public untuk enkripsi *message digest* yang menghasilkan tanda tangan digital dan kunci private untuk dekripsi. Dokumen dinyatakan valid jika hasil dekripsi tanda tangan digital sama dengan *message digest*.

Kata Kunci:Tanda Tangan Digital, Kriptografi Asimetris, Algoritma RSA, Message Digest, Fungsi Hash.

1. Pendahuluan

Kemajuan teknologi meningkat setiap hari dengan begitu cepat. Hal ini berpengaruh terhadap kehidupan manusia. Berkembangnya teknologi diiringi juga oleh perkembangan internet. Semakin hari penggunaan internet di kalangan masyarakat semakin luas, salah satunya sebagai alat verifikasi dan autentikasi yang biasa menggunakan tanda tangan. Di era revolusi industry 4.0 seperti sekarang, tanda tangan dilakukan tidak hanya secara manual (konvensional) tetapi bisa juga secara digital untuk mempermudah dan mempercepat jalannya suatu birokrasi karena tidak adanya batasan jarak. Seperti halnya tanda tangan yang dilakukan secara manual, tanda tangan digital juga dapat digunakan oleh semua orang tanpa memandang status atau jabatan apapun.

Tanda tangan digital bukanlah tanda tangan yang di-digitalisasi dengan alat *scanner* tetapi suatu nilai kriptografis yang bergantung pada dokumen asli dan pengirim pesan. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan.

Mekanisme pembuatan tanda tangan digital yaitu dengan menambahkan sebuah kode yang bertindak sebagai tanda tangan. Kode ini adalah hasil enkripsi (*cipherteks*) dari *message digest* yang dihasilkan dari *generate* isi dokumen yang akan di tanda tangan. Kode yang ditampilkan sebagai tanda tangan digital tidak hanya dalam bentuk *cipherteks*, bisa juga dalam bentuk yang lebih menarik seperti gambar, inisial dan lain-lain, tetapi diperlukan proses tambahan untuk mengubah ke dalam bentuk tersebut.

Algoritma yang digunakan untuk mendapatkan kode yang bertindak sebagai tanda tangan tersebut adalah algoritma Rivest Shamir Adleman (RSA). RSA termasuk kedalam algoritma kriptografi asimetris yaitu algoritma yang mempunyai dua buah kunci yaitu kunci public untuk enkripsi dan kunci private untuk dekripsi. Tujuan dari artikel ini adalah untuk mengetahui cara pembuatan tanda tangan digital dengan algoritma RSA.

2. Landasan Teori

Tanda Tangan Digital

Menurut Undang-Undang Nomor 19 Tahun 2016 Pasal 1 ayat 12, Tanda Tangan Elektronik (Digital) adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi [1].

Teknik yang umum digunakan untuk membentuk tanda tangan digital adalah dengan fungsi *hash* dan melibatkan algoritma kriptografi asimetris dengan skema kriptografi kunci publik. Fungsi *hash* adalah fungsi yang memetakan string biner dengan panjang input bervariasi ke suatu string biner dengan panjang output tetap atau disebut juga sebagai *message digest* [2].

Proses pembuatan tanda tangan digital adalah dengan menginputkan dokumen yang akan ditandatangani untuk pembuatan *message digest*. *Message digest* dihasilkan dengan melakukan *generate* isi dokumen yang telah diinputkan pada field pesan, kemudian dokumen tersebut dikenai fungsi *hash*, sehingga menghasilkan *message digest* [3]. *Message digest* yang diperoleh kemudian di enkripsi, dimana enkripsi tersebut merupakan tanda tangan elektonik untuk dokumen yang di-*generate*.

Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (tersembunyi atau rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Sehingga kriptografi artinya ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasian data, keabsahan data, integritas data dan autentikasi data [4].

Secara umum, kriptografi adalah ilmu mengenai teknik enkripsi data yang diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi atau menyembunyikan informasi [5]. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu

algoritma dengan beberapa parameter. Biasanya algoritma tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritma dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter [6]. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (parameter menjadi ekuivalen dengan kunci). [7].

Di dalam kriptografi, terdapat berapa istilah umum yang sering digunakan. Berikut ini diberikan beberapa istilah umum tersebut [8]:

1. *Plaintext* (*message/*dokumen), yaitu pesan atau informasi asli yang akan dikirimkan dan dijaga keamanannya.
2. *Ciphertext*, yaitu pesan atau informasi yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.
3. Enkripsi (*Encryption*), yaitu proses penyandian *plaintext* sehingga menjadi *chipherteks*.
4. Dekripsi (*Decryption*), yaitu proses untuk memperoleh kembali *plaintext* dari *chipherteks*.
5. Kriptosistem, yaitu sistem untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Kriptografi bertujuan memberi layanan keamanan dengan aspek-aspek sebagai berikut [9] :

1. Kerahasiaan (*confidentiality*), yaitu untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak atau pencegahan akan pengaksesan terhadap informasi yang dilakukan oleh pihak yang tidak berhak.
2. Integritas data (*data integrity*), yaitu pesan masih asli atau utuh belum pernah dimanipulasi selama pengiriman atau pencegahan akan modifikasi informasi yang dilakukan oleh pihak-pihak yang tidak berhak.
3. Autentikasi (*authentication*), yaitu mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan.
4. Nir-penyangkalan (non-repudiation), yaitu mencegah entitas yang berkomunikasi melakukan penyangkalan yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

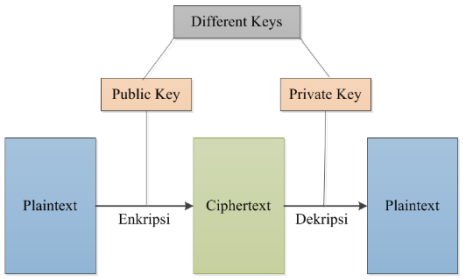
Rivest Shamir Adleman (RSA)

Rivest Shamir Adleman (RSA) diciptakan pada tahun 1978 dan diresmikan pada 1983. RSA ini merupakan singkatan dari nama penciptanya yaitu Ron Rivest, Adi Shamir dan Leonard Adleman dari Masschusetts Institute of Technology. RSA dalam kriptografi adalah algoritma untuk skema enkripsi kunci publik (*public-key encryption*). Kunci dari algoritma ini mempunyai panjang yang bervariasi mulai dari 40 bit hingga 2048 bit. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai atau tanda tangan digital dan untuk enkripsi serta merupakan salah satu penemuan besar pertama dalam kriptografi kunci publik [10].

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma secara khusus, maka selama itu pula keamanan algoritma RSA tetap terjamin [11].

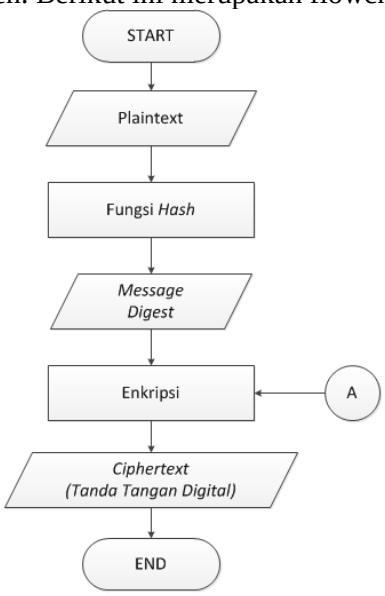
3. Pembahasan

Algoritma asimetris (*asymmetric algorithm*) muncul sekitar pertengahan tahun 1970an. Algoritma ini memiliki dua buah kunci dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Kedua kunci tersebut adalah kunci publik yang digunakan untuk enkripsi serta disebarkan secara umum dan kunci privat untuk dekripsi yang disimpan dengan rahasia oleh pengguna [12]. Gambar 1 merupakan skema algoritma asimetris:



Gambar 1. Skema Algoritma Asimetris

Algoritma RSA adalah salah satu algoritma kriptografi asimetris yang dapat digunakan untuk menandai sebuah dokumen. Berikut ini merupakan flowchart tanda tangan digital:

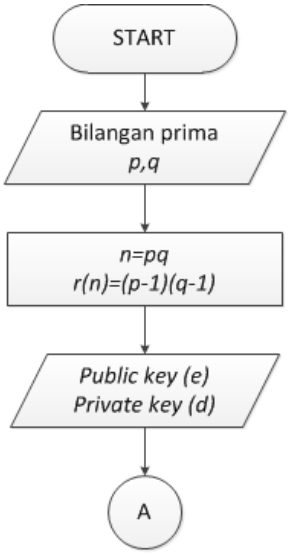


Gambar 2. Flowchart Tanda Tangan Digital dengan RSA

Algoritma RSA untuk enkripsi dan dekripsi didasarkan pada teorema Euler, sehingga menghasilkan rumus enkripsi dan dekripsi algoritma RSA sebagai berikut:

$$E_e(M) = C \equiv M^e \pmod{n}$$
$$D_d(C) = M \equiv C^d \pmod{n}$$
$$\equiv (M^e)^d \pmod{n}$$

Sedangkan proses pembangkitan kunci mengikuti flowchart berikut :



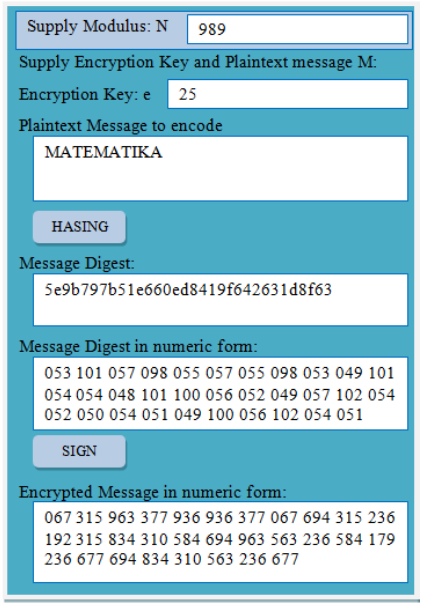
Gambar 3. Flowchart pembangkitan kunci RSA

Bilangan *p* dan *q* dipilih adalah bilangan prima yang nilainya cukup besar.

Pembuatan Tandatangan digital

Tanda tangan digital digunakan untuk menjamin autentikasi dan nir-penyangkalan dokumen. Hal ini menunjukkan bahwa dokumen yang dikirim bersama tanda tangan digital berasal dari sumber yang benar dan mencegah pengirim melakukan penyangkalan pengiriman atau penerima menyangkal telah menerima dokumen.

Berikut akan ditunjukkan proses pengiriman dokumen yang sudah diberi tanda tangan digital.



Gambar 4. Proses Pembuatan Tanda Tangan Digital

Tanda tangan digital dibangkitkan berdasarkan teks dokumen asli. Proses pembuatan tanda tangan digital dimulai dengan pengubahan teks dokumen menjadi *message digest*. *Message digest* kemudian dienkripsi menggunakan algoritma RSA untuk menjamin kerahasiaan

dan integritas data. Hal ini menunjukkan bahwa tanda tangan digital tidak dapat dibaca atau ditiru oleh pihak-pihak yang tidak berwenang dan tanda tangan digital masih asli atau belum pernah dimanipulasi selama pengiriman.

Teks dokumen yang akan dibuat tanda tangan digital terletak pada kotak *plaintext* yang kemudian di-*hashing* menjadi *message digest* dengan menekan tombol hashing. *Message digest* dikonversi menjadi *numeric number* yang dibagi menjadi blok-blok *cipher* (3 digit per blok), kemudian di enkripsi untuk mendapatkan tanda tangan digital dengan menekan tombol sign. Tanda tangan digital disertakan dengan dokumen yang akan dikirim untuk menjaga aspek keamanan dokumen yang dikirimkan.

Gambar 5. Proses pengiriman Dokumen dengan tanda tangan digital

Penerima memvalidasi teks dokumen yang dikirim dengan melakukan dekripsi pada tandatangan digital dengan menekan tombol verify. Jika hasil dekripsi sama dengan *message digest* maka tanda tangan digital valid.

4. Kesimpulan

Keamanan tanda tangan digital dipengaruhi oleh pemilihan dua bilangan prima untuk pembangkitan kunci. Semakin besar nilai yang diambil maka tanda tangan digital semakin sulit diretas, sehingga keamannya semakin terjamin.

Pembuatan tanda tangan digital dengan menggunakan algoritma RSA memenuhi 4 aspek keamanan yaitu tidak dapat dibaca atau ditiru oleh pihak-pihak yang tidak berwenang, masih asli atau belum pernah dimanipulasi selama pengiriman, berasal dari sumber yang benar dan mencegah pengirim melakukan penyangkalan pengiriman atau penerima menyangkal telah menerima dokumen.

Daftar Pustaka

[1] "Undang-Undang Nomor 11 Tahun 2008," www.hukumonline.com, Jakarta, 2008.

[2] W. Stallings, Cryptography and Network Security Principles and Practice, United States of America: Alan R. Apt, 2003.

[3] Y. Anshori, A. Y. E. Dodu and D. M. P. Wedananta, "Implementasi Algoritma Kriptografi Rivest Shamir," Techno.COM, vol. 18, pp. 110-121, 2019.

[4] A. J. Menezes, P. C. Van Oorschot and S. , Handbook of Applied Cryptography, New

York: Taylor & Francis Group, 2001.

[5] A. R. Tulloh, Y. Permanasari and E. Harahap, "Kriptografi Advanced Encryption Standard (AES) untuk Penyandian File Dokumen," in Spesia Unisba, Bandung, 2016.

[6] Y. Permanasari and E. Harahap, "Kriptografi Polyalphabetic," Matematika, vol. 17, no. 1, pp. 31-34, 2018.

[7] S. Kromodimoeljo, Teori dan Aplikasi Kriptografi, SPK IT Consulting, 2009.

[8] H. Y. Fay, Penerapan Kriptografi Algoritma RSA untuk Keamanan Database (Studi Kasus pada Sistem Informasi Toko Buku), Bandung, 2008.

[9] V. Lusiana and W. Hadikurniawati, "Kriptografi Kunci Publik (Public Key Cryptography)," Dinamika Informatika, vol. II, 2010.

[10] Z. Arifin, "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman," Jurnal Informatika Mulawarman, vol. 4, p. 3, 2009.

[11] R. Munir, Kriptografi Edisi Kedua, Bandung: Informatika, 2019.

[12] Y. Permanasari and E. Harahap, "Algoritma Data Encryption Standard (DES) pada Electronic Code Book (ECB)," Matematika, vol. 6, no. 1, pp. 77-84, 2006.

[13] K. Y. Tung, Memahami Teori Bilangan dengan Mudah dan Menarik, Jakarta: PT Grasindo, 2008.