**IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA PADA KEAMANAN DATA TRANSKRIP NILAI MAHASISWA UNM JURUSAN MATEMATIKA MENGGUNAKAN BAHASA PEMROGRAMAN PHP**

**Sukarna, Maya Sari Wahyuni, Susilowati1**

Department of Mathematics, Faculty of Mathematics and Natural Sciences,

University of Makassar, Parangtambung, 90244 South Sulawesi Indonesia

**Abstract** :This type of research is the study of the literature by collecting literatures relating to the RSA algorithm.RSA is an asymmetric key cryptography algorithm. Security RSA algorithm lies in the degree of difficulty in factoring non-prime numbers into prime factors. This study begins with the mathematical concepts that underlie the formation of RSA cryptography algorithm, the second stage is the process of encryption, signing, decryption and verification messages, the third stage is the implementation of RSA cryptography using the programming language PHP. The equations used in the RSA cryptography algorithm is the key establishment, selected two prime numbers p and q, and e where ($1 <e <φ (n)).$ n value obtained from $n = p ∙ q$, and the value of d obtained by the equation $e ∙ d mod φ (n) = 1$, obtained public key $(e, n)$ and private key $(d, n)$. The encryption process is done by entering values $m\_{i} $into the equation $c\_{i}=m\_{i}^{e} mod n$, so that the resulting Ciphertext ($ci$). Signing process is done by entering values $m\_{i} $ into the equation $S\_{i}= m\_{i}^{d} mod n$, so that the resulting Digital Signature (Si). Messages sent to the receiver and the signature is then decrypted by the equation $m\_{i}=c\_{i}^{d}mod n$. Messages obtained receiver Digital Signature verified by checking using persamaann $m\_{i}^{'}= S\_{i}^{e} mod n$. The result showed that the security in the process of sending and receiving messages can be enhanced with RSA cryptographic algorithms and digital signatures.

**Keywords**: RSA Cryptography, Encryption, Decryption, ciphertext, plaintext.

**Abstrak** : Jenis penelitian ini merupakan jenis penelitian terapan dengan mengumpulkan literatur-literatur yang berkaitan dengan algoritma RSA. RSA merupakan algoritma kriptografi kunci asimetris. Keamanan Algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor prima. Penelitian ini diawali dengan konsep matematis yang melandasi pembentukan algoritma kriptografi RSA, tahap kedua adalah proses enkripsi, penandatanganan, dekripsi dan verifikasi pesan, tahap ketiga yaitu diterapkannya kriptografi RSA menggunakan bahasa pemrograman PHP. Persamaan yang digunakan dalam algoritma kriptografi RSA adalah pembentukan kunci, dipilih dua bilangan prima p dan q, dan $e$ dimana ($1<e<ϕ(n)).$ Nilai n diperoleh dari$ n=p∙q$, dan nilai d diperoleh dengan persamaan $e ∙d mod ϕ(n)=1$, diperoleh kunci publik $(e,n)$ dan kunci privat $(d,n).$ Proses enkripsi dilakukan dengan memasukkan nilai $m\_{i}$ ke dalam persamaan $c\_{i}=m\_{i}^{e} mod n$, sehingga dihasilkan *Ciphertext* (*ci*). Proses penandatanganan dilakukan dengan memasukkan nilai $m\_{i}$ ke dalam persamaan $S\_{i}= m\_{i}^{d} mod n$ , sehingga dihasilkan Tandatangan Digital $(Si)$. Pesan dan tandatangan dikirim ke penerima kemudian didekripsi dengan persamaan $m\_{i}=c\_{i}^{d}mod n$. Pesan yang diperoleh penerima diverifikasi dengan memeriksa Tandatangan Digital dengan menggunakan persamaann $m\_{i}^{'}= S\_{i}^{e} mod n$. Berdasarkan hasil penelitian diperoleh bahwa keamanan dalam proses pengiriman dan penerimaan pesan dapat ditingkatkan dengan algoritma kriptografi RSA dan tandatangan digital.

**Kata Kunci :** *Kriptografi RSA, Enkripsi, Dekripsi, Ciphertext, Plaintex*

1. **Pendahuluan**

Matematika sebagai ilmu pengetahuan dasar sangat berpengaruh penting dalam perkembangan ilmu pengetahuan lainnya, termasuk perkembangan teknologi informasi.

Perkembangan teknologi informasi mempunyai pengaruh yang sangat signifikan bagi aspek kehidupan, tidak terkecuali aspek komunikasi dan pengiriman pesan maupun pengiriman data.

Data yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai *file* di dalam komputer maupun saat data tersebut dikirim melalui *e-mail*.

Untuk membangun sistem penyimpanan data yang aman dan tidak dapat dibaca oleh orang yang tidak berwenang, diperlukan suatu ilmu tertentu yang fokus mempelajari mengenai teknik-teknik penyandian suatu pesan dengan susunan algoritma-algoritma tertentu yang disebut kriptografi.

Kriptografi umumnya digunakan untuk mengamankan suatu data yang dirahasiakan dengan mengubah data tersebut menjadi kode-kode rahasia yang hanya pengirim dan penerima data yang mengetahuai kode tersebut. Salah satu contoh penggunaan kriptografi adalah pengamanan data transkrip nilai mahasiswa. Data transkrip nilai dianggap sangat penting untuk dijaga kerahasiaannya agar data tersebut tidak dapat diubah dan diakui sebagai milik orang yang tidak berkepentingan.

Menurut Ariyus (Suhan: 2013), jenis kriptografi kunci asimetris diantaranya adalah RSA (*Rivest, Shamir,Adleman*), ElGamal dan algoritma kriptografi berbasis kurva Eliptik. RSA merupakan salah satu algoritma kriptografi asimetris yang dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*) yaitu: Ron **R**ivest, Adi **S**hamir, dan Leonard **A**dleman pada tahun 1976. Proses enkripsi dan dekripsi RSA didasarkan pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Keamanan Algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor prima.

Kontribusi yang paling penting adalah tandatangan digital (*digital Signature*) pada pesan untuk memberikan aspek keamanan autentikasi, integritas data dan pembuktian kesahihan asal informasi yang diperoleh. Tandatangan digital juga bebas sangkal (*non-repudiation*), yang berarti bahwa tandatangan digital mencegah pengirim untuk menyangkal bahwa pengirim tersebut benar-benar tidak mengirim informasi itu sebelumnya.

1. **Kajian Pustaka**
2. **Teori Bilangan**

Teori bilangan (*number theory*) adalah teori yang mendasari dalam memahami kriptografi, baik pada kriptografi simetris maupun pada kriptografi asimetris. Bilangan yang dimaksud adalah bilangan bulat (*integer*). Himpunan semua bilangan bulat yang dinotasikan dengan $Z$ adalah himpunan {…, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, …}, yang berperan sangat penting dalam kriptografi, karena sebagian besar algoritma kriptografi menggunakan sifat-sifat himpunan semua bilangan bulat dalam melakukan prosesnya.

Pada himpunan ini berlaku sifat asosiatif, komutatif dan distributif terhadap operasi penjumlahan dan perkalian, serta identitas, transitif, trikotomi dan hukum pembatalan (*Cancellation Law*).

1. **Kriptografi**

Kriptografi (*Cryptography*) berasal dari Bahasa Yunani, *Cryptos* artinya rahasia (*Secret*), sedangkan *Graphein* yang berarti tulisan (*writing*). Jadi, kriptografi berarti tulisan rahasia (*Secret Writing*) (Munir, 2006: 2).

Kriptografi Ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan pesan asli (*plaintext*) ke dalam bentuk pesan rahasia (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) pesan kepada penerima (*receiver*) pesan. Setelah sampai di penerima, *ciphertext* tersebut ditransformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali. Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*). Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

1. **Tanda tangan Digital**

Tanda tangan digital dibuat dengan menggunakan teknik kriptografi, suatu cabang dari matematika terapan yang menangani tentang pengubahan suatu informasi menjadi bentuk lain yang tidak dapat dimengerti dan dikembalikan seperti semula. Tanda tangan digital menggunakan “*public key cryptography*” (kriptografi kunci publik), dimana algoritmanya menggunakan dua buah kunci, yang pertama adalah kunci untuk membentuk tanda tangan digital atau mengubah data ke bentuk lain yang tidak dapat dimengerti, dan kunci kedua digunakan untuk verifikasi tanda tangan digital ataupun mengembalikan pesan ke bentuk semula.

Sistem kriptografi ini menggunakan kunci privat, yang hanya diketahui oleh penandatangan dan digunakan untuk membentuk tanda tangan digital, serta kunci publik, yang digunakan untuk verifikasi tanda tangan digital. Jika beberapa orang ingin memverifikasi suatu tanda tangan digital yang dikeluarkan oleh seseorang, maka kunci publik tersebut harus disebarkan ke orang-orang tersebut. Kunci privat dan kunci publik ini sesungguhnya secara matematis berhubungan, walaupun demikian kunci privat tidak dapat ditemukan menggunakan informasi yang didapat dari kunci publik.

1. **Bahasa Pemrograman PHP**

PHP adalah bahasa pemrograman script yang paling banyak dipakai saat ini. PHP banyak dipakai untuk memrogram situs web dinamis, walaupun tidak tertutup kemungkinan digunakan untuk pemakaian lain. Contoh terkenal dari aplikasi PHP adalah forum (phpBB) dan MediaWiki (software di belakang Wikipedia). PHP juga dapat dilihat sebagai pilihan lain dari ASP.NET/C#/VB.NET Microsoft, ColdFusion Macromedia, JSP/Java Sun Microsystems, dan CGI/Perl. Contoh aplikasi lain yang lebih kompleks berupa CMS yang dibangun menggunakan PHP adalah Mambo, Joomla, Postnuke, Xaraya, dan lain-lain.

Simulasi algoritma kriptogragi RSA dilakukan dengan menggunakan bahasa pemrograman PHP. Simulasi ini dilakukan dengan membuat sebuah program, yang dapat melakukan enkripsi, deskripsi, tanda tangan digital dan verifikasi tanda tangan digital.

1. **Metode Penelitian**
2. **Jenis Penelitian**

Jenis penelitian pada tulisan ini adalah jenis penelitian terapan, sehingga metode yang digunakan dalam penelitian adalah kajian kepustakaan dengan mengambil beberapa definisi, teorema, serta sifat-sifat yang berkaitan dengan Algoritma Kriptografi RSA dan penerapannya pada Bahasa Pemrograman PHP.

1. **Sumber Pustaka Penelitian**

Sumber pustaka yang digunakan dalam penelitian ini berasal dari literatur-literatur, baik yang ada di perpustakaan Jurusan Matematika FMIPA UNM maupun perpustakaan lain. Selain itu, literatur juga diperoleh dari *website* berupa jurnal ilmiah dan referensi-referensi lainnya yang berkaitan dengan penelitian.

1. **Prosedur Penelitian**

Proses Pembangkitan Kunci

1. Dipilih dua buah bilangan prima acak dan dirahasiakan, misalkan kedua bilangan prima tersebut $p$ dan $q.$
2. Dihitung modulus RSA yaitu $n$ yang diperoleh dengan mengalikan kedua bilangan prima yang telah ditentukan pada langkah sebelumnya. Secara matematis, $n=p ∙q$
3. Dihitung $ϕ(n)$ yang merupakan hasil perkalian dari $p-1 $dengan $q-1$. Secara matematis $ϕ(n)=\left(p-1\right)\left(q-1\right)$
4. Dipilih sembarang bilangan acak $e$, dimana ($1<e<ϕ(n))$ dengan syarat $e$ harus relative prima terhadap $m$. Secara matematis $\left(e, ϕ(n)\right)=1$
5. Dihitung nilai $d$ menggunkan persamaan $e ∙d mod ϕ(n)=1$ atau $e∙d ≡1 mod ϕ\left(n\right) $ sehingga $d=\frac{1+k∙ϕ(n)}{e}$
6. **Hasil dan Pembahasan**
7. **Enkripsi Plaintext**

*Plaintext* dipotong menjadi blok-blok karakter sehingga satu blok memuat satu karakter. Blok-blok karakter kemudian dikonversi ke kode ASCII. Setiap blok dienkripsi menjadi ciphertext dengan menggunakan rumus $c\_{i}=m\_{i}^{e"} mod n^{"}$. Sebagai masukan pada proses enkripsi adalah judul halaman dan kunci publik milik mahasiswa. Proses Enkripsi dengan menggunakan bahasa pemrograman PHP dapat dilihat pada gambar di bawah ini :



dan hasil proses Enkripsi dapat dilihat pada gambar berikut

1. **Pembuatan Tanda tangan Digital**

Setiap blok dienkripsi menjadi tanda tangan digital menggunakan rumus $S\_{i}= m\_{i}^{d^{'}} mod n'$. Sebagai masukan pada proses enkripsi adalah pesan dan kunci privat milik pengirim pesan atau pihak Admin.

1. **Deskripsi Pesan**

Setelah mahasiswa menerima *ciphertext* beserta tanda tangan digital dari admin, selanjutnya mahasiswa mendekripsikan *ciphertext* menjadi *plaintext* menggunakan kunci privat milik mahasiswa dengan rumus $m\_{i}=c\_{i}^{d"}mod n"$*.* Sebagai masukan pada proses dekripsi adalah *ciphertext* dan kunci privat milik penerima pesan yaitu mahasiswa. Proses Dekripsi pesan dapat dilihat pada gambar berikut



dan hasil pros Dekripsi dapat dilihat pada gambar berikut



1. **Verifikasi Tanda tangan Digital**

Proses selanjutnya yaitu memverifikasi tanda tangan digital dengan rumus $m\_{i}^{'}= S\_{i}^{e'} mod n'$. Sebagai masukan pada proses dekripsi adalah tanda tangan digital dan kunci publik milik pihak admin.

1. **Kesimpulan**

Berdasarkan hasil penelitian, maka diperoleh kesimpulan sebagai berikut :

1. Konsep matematis yang melandasi terbentuknya algoritma kriptografi RSA adalah Teorema Euler.
2. Proses Enkripsi dan Proses Dekripsi
3. Proses enkripsi algoritma kriptografi RSA pada pengiriman pesan rahasia yaitu , *plaintext* dipotong menjadi blok-blok karakter, konversi ke Kode ASCII, gunakan rumus enkripsi untuk menghasilkan *ciphertext.*
4. Proses dekripsi algoritma kriptografi RSA pada pengiriman pesan rahasia yaitu,gunakan rumus dekripsi untuk menghasilkan *plaintext*, konversi kembali ke kode ASCII, gabungkan *plaintext.*
5. Proses pembuatan tanda tangan digital menggunakan algoritma kriptografi RSA pada pengiriman pesan rahasia yaitu, *plaintex* dipotong menjadi blok-blok karakter, konversi ke Kode ASCII, gunakan rumus enkripsi dengan kunci privat untuk menghasilkan tanda tangan digital (*digital signature*).

**DAFTAR PUSTAKA**

Feoh, G. (2013). *Sistem Bilangan Dan Konversi Bilangan.* http://lulu mawadah.staff.gunadarma.ac.id/Downloads/files/41709/sistem\_bilangan dan konversi\_bilangan1.pdf, diakses pada tanggal 24 Januari 2016 pukul 16.50 WITA.

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

Munir, R. 2012. *Matematika Diskrit (Edisi Revisi Kelima)*. Bandung: Informatika Bandung.

Nurfadillah,S. 2013. *Penerapan Algoritma Kriptografi RSA pada Pengiriman Pesan Rahasia*. *Skripsi.* Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Makassar. Makassar.

Nurfajrin.2014. *Algoritma Kriptografi Elgamal dan Penerapannya pada Pengiriman Pesan*. *Skripsi.* Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Makassar. Makassar.

Rahajoeningroem dan Aria. 2011. *Studi dan Implementasi Algoritma RSA untuk Pengamanan data Transkrip Akademik Mahasiswa. Majalah Ilmiah UNIKOM. Vol 8. Nomor 1.* <http://jurnal.unikom.ac.id/_s/data/jurnal/v08-n01/volume-81-artikel-9.pdf/pdf/volume-81-artikel-9.pdf>,diakses pada tanggal 11 Desember 2015 pukul 20.45 WITA.

 Ronald,dkk.2012. *Otentikasi Dokumen Elektronik Menggunakan Tandatangan Digital*.<http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Makalah/Makalah12.pdf>*,* diakses pada tanggal20 Januari 2016 pukul 09.21 WITA.

Tiro, M.A, dkk. 2008. Pengenalan Teori Bilangan. Makassar:Andira Publisher.