# TANDA TANGAN DIGITAL DENGAN SISTEM KRIPTOGRAFI ALGORITMA RIVEST, SHAMIR DAN ADLEMAN (RSA)

## *DIGITAL SIGNATURE WITH CRYPTOSYSTEM ALGORITHM RIVEST SHAMIR AND ADLEMAN (RSA)*

Oleh:

Naji Maruf Ilyas[1], Karyati[2]

[1]12305141043@student.uny.ac.id

[2]karyati@uny.ac.id

Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Negeri Yogyakarta

**Abstrak**

Salah satu aplikasi kriptografi asimetrik adalah tanda tangan digital. Salah satu fungsi tanda tangan digital adalah menjaga keotentikan dokumen digital. Beberapa algoritma tanda tangan digital yang telah dikembangkan antara lain El Gamal, kurva eliptik dan RSA. El Gamal mendasarkan keamanannya pada logaritma diskrit, kurva eliptik pada penguraian kurva eliptik, sedangkan RSA pada pemfaktoran bilangan bulat. Tujuan penelitian ini adalah mengetahui skema pembuatan kunci tanda tangan digital algoritma RSA, skema tanda tangan digital algoritma RSA dan mengetahui skema verifikasi tanda tangan digital algoritma RSA. Skema pembuatan kunci diawali dengan memilih dua bilangan prima yang berbeda. Kemudian kedua bilangan tersebut dikalikan, misal $n$. Selanjutnya memilih satu bilangan bulat positif kurang dari $\varphi(n)$, dengan $\varphi(n)$ adalah Totient Euler $n$, dan saling prima dengan $\varphi(n)$, misal $v$. Bilangan $(n, v)$ ini disebut kunci publik. Kemudian kunci privat $s$ diperoleh dengan menyelesaikan $s.v \equiv 1\ (modulo\ \varphi(n))$. Selanjutnya skema tanda tangan digital. Nilai tanda tangan digital diperoleh dengan menghitung $S = D^s (mod\ n)$ dengan $D$ adalah nilai hash pesan digital. Kemudian skema verifikasi. Nilai verifikasi $V$ diperoleh dengan menghitung $V = S^v (mod\ n)$. Apabila $V = D$ berarti dokumen belum berubah, namun apabila $V \neq D$, berarti dokumen sudah berubah.
Kata kunci: kriptografi asimetrik, tanda tangan digital, algoritma RSA, tanda tangan digital algoritma RSA.

**Abstract**

*One of asymmetric cryptographic applicatoin was digital signature. One of digital signature function was authentication. Some developed digital signature algorithms were El Gamal, elliptic curve, and RSA. The security of El Gamal digital signature was based on discrete logarithm, the elliptic curve was on factorisation of elliptic curve, the RSA was on factoring prime number. The purposes of this research were to know the scheme of RSA key creation, RSA signing scheme, and RSA verification scheme. The scheme of RSA key creation was started with choosing two different prime numbers then computes the product of the prime numbers, called n. After that choose a number, less than $\varphi(n)$, with $\varphi(n)$ was Totient Euler of n, and coprime with $\varphi(n)$, called v. The number (n,v) was public key. The private key was yielded by computing solve $s.v \equiv 1\ (modulo\ \varphi(n))$. The value of document digital signature S was obtained by computing $S = D^s (mod\ n)$ with D was hash value of the document. The value of verification V was yielded by computing $V = S^v (mod\ n)$. If $V = D$, it means that document wasn't changed, but if $V \neq D$, it means that the document was changed*

*Keywords: asymmetric cryptography, digital signature, RSA algorithm, digital signature with RSA algorithm.*

## PENDAHULUAN

Kriptografi atau persandian adalah salah satu cabang matematika yang mempelajari cara merahasiakan pesan sehinggga maksud pesan tersebut tidak dapat diketahui. Dalam persandian dikenal dua proses, yakni enkripsi dan dekripsi. Enkripsi

adalah proses menyandikan pesan atau merahasiakan pesan, yakni mengubah teks yang dapat dibaca (teks terang) ke teks yang tidak dapat dibaca (teks sandi). Sedangkan dekripsi adalah proses mengubah teks sandi menjadi teks terang, teks yang dapat dibaca. Kedua proses enkripsi dan dekripsi ini memerlukan kunci. Kunci untuk proses enkripsi disebut kunci enkripsi dan kunci untuk proses dekripsi disebut kunci dekripsi.

Pada zaman kaisar Caesar, orang-orang menggunakan satu kunci untuk enkripsi dan dekripsi. Hal ini disebut sebagai kriptografi kunci simetrik. Selama beberapa waktu kunci simetrik masih digunakan. Tetapi kemudian kunci simetrik mengalami beberapa permasalahan seperti dua orang yang berkomunikasi harus merahasiakan kunci yang mereka gunakan dari orang lain, rumitnya pergantian kunci, banyaknya kunci yang harus disimpan (Spillman, 2005:179).

Permasalahan yang ada tersebut, memotivasi beberapa ahli matematika untuk menggunakan dua kunci yang berbeda antara kunci enkripsi dengan kunci dekripsi. Kunci enkripsi dipublikasikan tetapi kunci dekripsi dirahasiakan. Hal ini disebut kriptografi kunci asimetrik. Pada kriptografi kunci asimetrik ini, kunci untuk proses enkripsi disebut kunci publik sedangkan kunci untuk proses dekripsi disebut kunci privat atau kunci rahasia. Spillman (2005:180) memberikan ilustrasi mengenai kunci asimetrik sebagai berikut. Ibarat sebuah lemari yang diletakkan di tempat publik. Lemari tersebut memiliki nama pemilik, lubang kecil untuk memasukkan surat dan sebuah kunci. Setiap orang mengetahui lemari tersebut milik siapa dan dapat mengirimkan surat ke dalamnya melalui lubang kecil yang ada di lemari itu. Tetapi hanya pemilik lemari yang dapat membuka lemari dan membaca surat di dalamnya.

Salah satu aplikasi lain dari kriptografi kunci asimetrik adalah tanda tangan digital. Tanda tangan digital di sini bukanlah tanda tangan yang discan, melainkan suatu bilangan yang diolah secara matematis sedemikian sehingga menghasilkan kesimpulan bahwa suatu dokumen masih asli atau bukan (Isnaeni, 2016:35). Dalam tanda tangan digital, dikenal tiga proses, yakni proses pembuatan kunci, proses menandatangani dokumen digital dan proses verifikasi tanda tangan digital. Proses pembuatan kunci menghasilkan kunci publik dan kunci rahasia. Kemudian kunci privat digunakan untuk menandatangani dokumen digital, sedangkan kunci publik digunakan untuk memverifikasi tanda tangan digital.

Tanda tangan digital dan tanda tangan konvensional memiliki fungsi sama, yaitu otentikasi (menjamin keaslian dokumen). Beberapa algoritma tanda tangan digital yang telah dikembangkan antara lain tanda tangan digital algoritma R. Rivest, A. Shamir dan L. Adleman (RSA), metode ElGamal, dan metode kurva eliptik.

Di antara ketiga metode tanda tangan digital tersebut, yang akan dibahas dalam penelitian ini adalah metode tanda tangan digital sistem R. Rivest, A. Shamir dan L. Adleman (RSA) sebab langkah yang digunakan sederhana.

Wahyuni (2014:31) menggunakan tanda tangan digital dengan sistem kriptografi algoritma RSA untuk melegalisasi ijazah mahasiswa. Sebelumnya Husodo (2010:1) juga menggunakan tanda tangan digital dengan sistem kriptografi algoritma RSA untuk melegalisasi ijazah mahasiswa. Sebelum itu, Munir (2005:31) menggunakan tanda tangan digital dengan sistem kriptografi algoritma RSA untuk menjaga integritas berkas perangkat lunak. Sementara itu Leonardo Refialy, Eko Sediyono dan Adi Setiawan (2015:229), menggunakan tanda tangan digital dengan sistem kriptografi algoritma RSA untuk melegalisasi sertifikat tanah.

## PEMBAHASAN

RSA merupakan singkatan dari nama tiga orang yaitu: Rivest, Shamir, dan Adleman. Ketiga orang inilah yang mengenalkan tanda tangan digital RSA. Tanda tangan digital RSA diperoleh melalui tiga proses yakni proses pembentukan kunci, proses tanda tangan digital, dan proses verifikasi. Ringkasan Hoffstein (2008:441) tentang skema tanda tangan digital RSA ada pada Tabel 1.

Pada Tabel 1, Hoffstein (2008:441) menggunakan nama Saepul dan Vina. Saepul mewakili pihak yang menandatangani dokumen digital, dan Vina mewakili pihak yang akan memverifikasi. Proses pembentukan

kunci dan tanda tangan dilakukan oleh Saepul, proses verifikasi dilakukan oleh Vina.

Tabel 1. Ringkasan Skema Tanda Tangan Digital Algoritma RSA.

| Saepul | Vina |
|---|---|
| **Pembuatan kunci** | |
| Pilih dua bilangan prima $p$ dan $q$.<br>Pilih exponen verifikasi $v$ dengan $\gcd(v,(p-1)(q-1)) = 1$.<br>publikasikan $n = pq\ dan\ v$. | |
| **Proses tanda tangan** | |
| Menghitung $s$ yang memenuhi:<br>$sv \equiv 1(mod(p-1)(q-1))$.<br>Menandatangani dokumen D dengan menghitung:<br>$S \equiv D^s(mod\ n)$. | |
| **Proses Verifikasi** | |
| | Menghitung $S^v\ mod\ n$ dan mencocokan-nya dengan D. |

**Pembentukan Kunci**

Proses ini dilakukan oleh pihak yang akan menandatangani dokumen. Proses ini memerlukan dua bilangan prima berbeda, misal $p$ dan $q$. Untuk mengecek apakah bilangan-bilangan tersebut prima atau bukan digunakan saringan Erastostenes, yakni jika tidak ada bilangan prima yang kurang dari $\sqrt{n}$ dan membagi $n$, maka $n$ bilangan prima. Kedua bilangan prima yang dipilih ini haruslah besar, minimal seratus digit. Tetapi pada karya ini digunakan bilangan prima yang kecil untuk memudahkan perhitungan. Kedua bilangan tersebut adalah $p = 11$ dan $q = 17$.

Setelah itu, kedua bilangan ini dikalikan $pq = n$. Bilangan ini akan digunakan sebagai modulus. Oleh karena itu, pada karya ini, bilangan ini disebut sebagai bilangan modulus. Pada karya ini bilangan modulusnya adalah $n = pq = 11.17 = 187$.

Kemudian dicari nilai phi Euler dari $\varphi(n)$. Sebab n adalah hasil kali bilangan prima, maka $\varphi(n) = (p-1)(q-1)$. Pada karya ini $\varphi(n) = (p-1)(q-1) = 10.16 = 160$. Ketiga bilangan ini, $p, q, \varphi(n)$ tidak boleh dipublikasikan.

Selanjutnya, memilih bilangan bulat antara 1 dan $\varphi(n)$ yang saling prima dengan $\varphi(n)$, misal v. Jadi $1 < v < \varphi(n)$ dan $gcd(v, \varphi(n)) = 1$. Pada karya ini, bilangan ini dinamakan eksponen verifikasi. Untuk mengecek apakah v dan $\varphi(n)$ saling prima, digunakan algoritma Euclid yakni apabila $b = aq + r\ maka\ gcd(b,a) = gcd(a,r)$. Bilangan v dan $\varphi(n)$ harus saling prima untuk menjamin ketunggalan invers v modulo $\varphi(n)$.

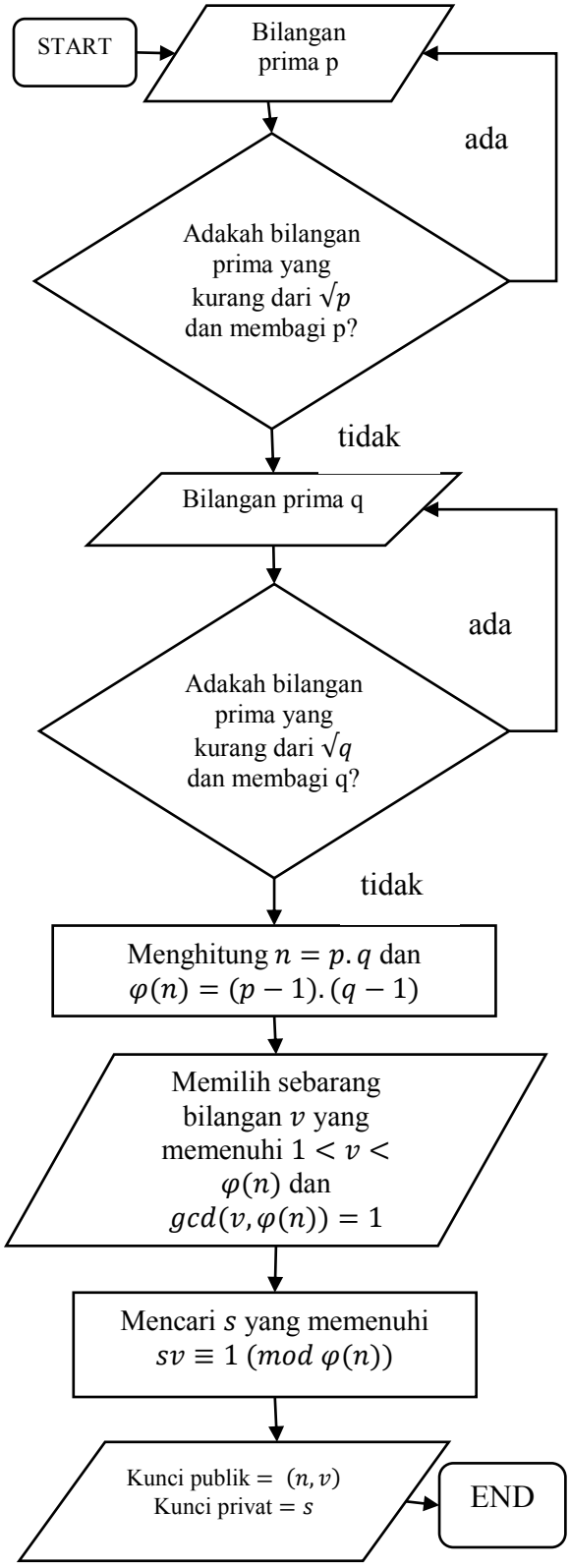
Pada penelitian ini dipilih $v = 53$. Kemudian akan dicek apakah $v = 53$ dan $\varphi(n) = 160$ saling prima sebagai berikut. Diketahui bahwa $160 = 153.3 + 1$ maka $gcd(160,153) = 1$. Ini menunjukkan bahwa $v = 153$ dan $\varphi(n) = 160$ saling prima.

Sampai langkah ini sebenarnya kita sudah mendapatkan bilangan modulus dan eksponen verifikasi. Kedua bilangan ini adalah kunci publik. Keduanya dipublikasikan secara berurutan, bilangan modulus kemudian eksponen verifikasi $(n, v)$. Pada penelitian ini, kunci publiknya adalah $(n, v) = (187,53)$.

Langkah selanjutnya adalah membentuk kunci privat. Pada karya ini kunci privat disimbolkan dengan s. Bilangan s ini didapatkan dengan mencari invers v modulo $\varphi(n)$. Jadi bilangan s memenuhi $sv \equiv 1\ (mod\ \varphi(n))$. Karena v dan $\varphi(n)$ saling prima maka banyaknya bilangan s adalah tunggal. Selanjutnya bilangan ini selain disebut sebagai kunci privat, juga disebut sebagai eksponen tanda tangan. Pada karya ini bilangan $s = 157$. Sebab $157.53 = 8321 \equiv 1(mod\ 160)$. Sampai sini semua kunci sudah ditemukan.

Jadi pada karya ini, kunci publiknya adalah $(n, v) = (187,53)$ dan kunci privatnya adalah $s = 157$. Bilangan yang dipublikasikan adalah $(n, v) = (187,53)$ sedangkan bilangan $s = 157$ dirahasiakan. Begitu juga dengan bilangan $p, q$ dan $\varphi(n)$ harus dirahasiakan.

Diagram alir pembentukan kunci tanda tangan digital terangkum dalam Gambar 1.




Gambar 1. Diagram Alir Pembentukan Kunci Tanda Tangan Digital RSA.

Berikut disertakan pula algoritma pembuatan kunci tanda tangan digital:

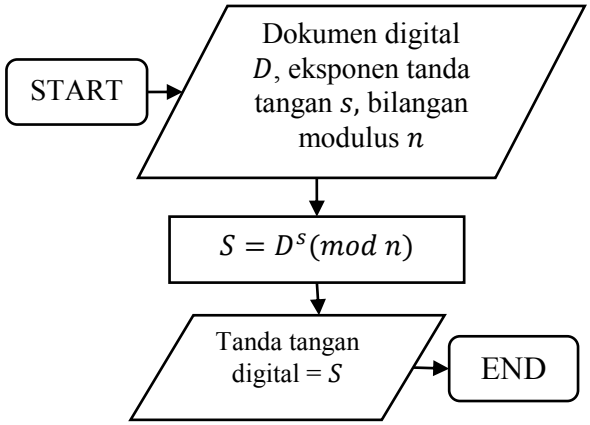
1. Pilih bilangan prima pertama, misal p.
2. Cek, apakah ada bilangan prima yang kurang dari $\sqrt{p}$ dan membagi habis p.
3. Jika ada, maka cari bilangan yang lain. Jika tidak ada maka langkah selanjutnya adalah cari bilangan prima kedua, misal q.
4. Cek, apakah ada bilangan prima lain yang kurang $\sqrt{q}$ dan membagi habis q.
5. Jika ada, maka cari bilangan yang lain. Jika tidak ada maka langkah selanjutnya adalah kalikan kedua bilangan tersebut, $n = p.q$.
6. Hitung fungsi phi Euler dari n, $\varphi(n) = (p-1)(q-1)$.
7. Pilih bilangan bulat antara 1 dan $\varphi(n)$ yang saling prima dengan $\varphi(n)$, misal $v$.
8. Cek, apakah bilangan tersebut saling prima dengan $\varphi(n)$ menggunakan algoritma Euclides. $Jika\ b = aq + r\ maka\ gcd(b,a) = gcd(a,r)$.
9. Jika saling prima, maka selanjutnya adalah mencari $s = v^{-1}\ modulo\ \varphi(n)$. Jika tidak maka cari bilangan yang lain.
10. Mempublikasikan kunci publik $(n, v)$.
11. Merahasiakan kunci privat $s$, dan juga bilangan $p, q, \varphi(n)$.

**Skema Penandatanganan**

Proses ini dilakukan oleh orang yang akan menandatangani dokumen digital. Pada proses ini dibutuhkan dokumen digital dan eksponen tanda tangan $s$. Sebelum dokumen digital ditandatangani, terlebih dahulu dokumen tersebut direduksi menggunakan fungsi hash. Sebab akan jadi repot jika dokumen terebut tidak direduksi.

Pada karya ini, hasil fungsi hash dari dokumen tersebut disimbolkan dengan D. Langkah selanjutnya adalah memangkatkan D dengan eksponen tanda tangan $s\ modulo\ n$. Jadi $S = D^s (mod\ n)$ adalah tanda tangan digital dari dokumen

tersebut. Tanda tangan ini bisa dilampirkan bersama dokumen atau dipisahkan dari dokumen. Diagram alir proses tanda tangan digital diberikan dalam Gambar 2.




Gambar 2. Diagram Alir Skema Penandatanganan

Berikut adalah algoritma proses tanda tangan digital:

1. Mencari dokumen digital.
2. Mencari nilai hash dari dokumen tersebut, misal D.
3. Mencari kunci publik $(n, v)$ dan kunci privat $s$.
4. Memangkatkan dokumen tersebut dengan kunci privat $s\ modulo\ n$. Jadi $S = D^s(mod\ n)$.
5. Bilangan $S$ adalah tanda tangan digital dari dokumen tersebut.

Misal diketahui suatu dokumen digital memiliki nilai hash $D = 30721(mod\ 187) = 53$ dan akan ditandatangani menggunakan eksponen tanda tangan $s = 157$. Maka tanda tangan digital dokumen tersebut adalah $S = D^s = 53^{157}(mod\ 187) = 15$.

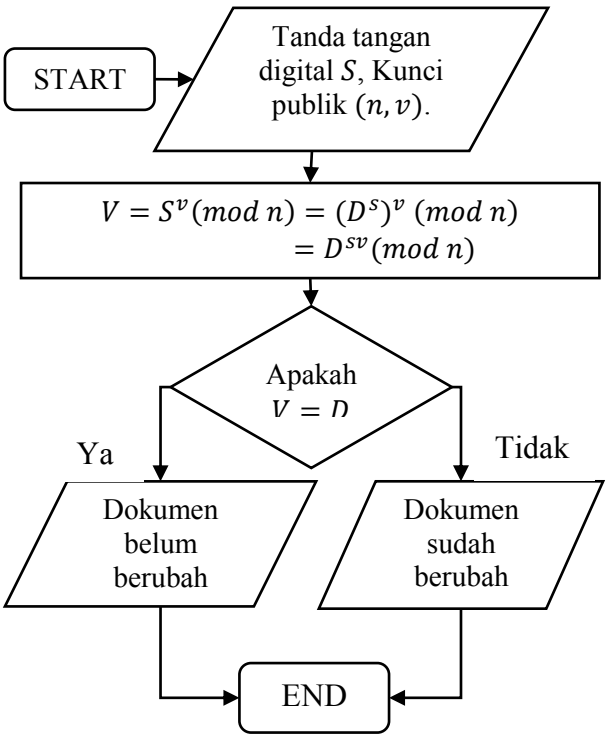
**Proses Verifikasi**

Proses ini bisa dilakukan oleh banyak pihak seperti kepolisian, publik, dan lain-lain sebab yang dibutuhkan dalam proses ini telah dipublikasikan, yaitu tanda tangan digital dan kunci publik. Langkah pertama yang dilakukan adalah memangkatkan tanda tangan digital $S$ dengan eksponen verifikasi $v\ modulo\ n$.

Pada karya ini hasil verifikasi disimbolkan dengan V. Jadi $V = S^v(mod\ n) = (D^s)^v(mod\ n) = D^{sv}(mod\ n)$. Apabila $V = D$ maka disimpulkan bahwa dokumen tersebut masih otentik. Jika tidak berarti dokumen tersebut telah berubah.

Misal ditemukan tanda tangan digital $S = 15$ dengan kunci publik $(n, v) = (187,53)$ pada proses sebelumnya. Selanjutnya tanda tangan tersebut akan diverifikasi. Apakah pesannya masih otentik atau sudah berubah. Hasil proses verifikasinya adalah $V = S^v(mod\ n) = 15^{157}(mod\ 187) = 53 = D$.

Jadi jika hasil proses verifikasi adalah $V = D$. Ini menunjukkan bahwa dokumen tersebut masih otentik atau belum berubah. Diagram alir proses verifikasi tanda tangan digital disajikan dalam Gambar 3.




Gambar 3. Diagram Alir Skema Verifikasi Tanda Tangan Digital.

Berikut adalah algoritma verifikasi tanda tangan digital.

1. Cari tanda tangan digital $S$.
2. Cari kunci publik $(n, v)$.
3. Pangkatkan tanda tangan $S$ dengan $v\ modulo\ n$. Jadi $V = S^v(mod\ n) = (D^s)^v(mod\ n) = D^{sv}(mod\ n)$.
4. Jika $V = D$ berarti dokumen masih otentik, jika tidak berarti dokumen sudah berubah.

Berikut diberikan contoh penggunaan tanda tangan digital pada dokumen berupa ijazah. Pada kehidupan nyata bilangan prima yang dipilih haruslah besar, minimal 100 digit. Selain itu fungsi hash yang digunakan cukup rumit. Tujuannya adalah agar tidak mudah dibobol. Berbeda dengan karya ini, dipilih bilangan prima yang kecil dan fungsi hash yang sederhana untuk memudahkan perhitungan. Berikut contohnya.

Suatu universitas memiliki kebijakan baru yang dirasa dapat membantu mahasiswa dalam masalah birokrasi saat melamar kerja. Kebijakan tersebut adalah mengeluarkan ijazah digital. Dengan demikian setiap mahasiswa yang lulus akan mendapatkan ijazah asli dan ijazah digital. Pihak universitas menyatakan bahwa ijazah digital sama dengan ijazah asli. Namun untuk mengantisipasi hal-hal yang tidak diinginkan, misal mengubah nama, nilai dan lain-lain, mereka menambahkan tanda tangan digital. Oleh karena itu, mereka mengeluarkan kunci publik, yaitu $(n, v) = (187,53)$, sedangkan kunci privatnya adalah $s = 157$. Berikut ditunjukkan proses pembentukan kuncinya.

Diketahui bahwa bilangan modulus $n = 187$ adalah perkalian dari 11 dan 17 yang keduanya adalah bilangan prima. Kemudian akan dicari $\varphi(n)$. Diketahui bahwa $\varphi(n) = (11-1)(17-1) = 10.16 = 160$. Setelah itu, memilih bilangan bulat, misal $v$, antara $1\ dan\ 160$ yang saling prima dengan 160. Dipilihlah bilangan tersebut $v = 53$. Kemudian dicek, apakah $\varphi(n) = 160$ dan $v = 53$ saling prima. Diketahui bahwa $160 = 53 * 3 + 1$. Ini berarti bahwa $gcd(160,53) = gcd(53,1) = 1$. Sehingga $\varphi(n) = 160\ dan\ v = 53$ saling prima. Pada langkah ini didapat kunci publik yaitu $(n, v) = (187,53)$.

Setelah itu, mencari kunci privat,misal s. Bilangan ini harus memenuhi $sv \equiv 1(mod\ 160)$. Kekongruenan ini berarti $sv - 1$ adalah kelipatan 160. Dengan perhitungan biasa didapat b

Bahwa $s = 157$. Jadi didapatkan kunci privatnya adalah $s = 157$.

Ijazah tersebut berisi sebuah pernyataan yang mencakup pernyataan kelulusan, nama mahasiswa, tempat dan tanggal lahir mahasiswa, IPK mahasiswa, tanggal pembuatan, pihak yang mengeluarkan ijazah. Hal ini mengakibatkan antar ijazah mahasiswa memiliki tanda tangan digital yang berbeda, tetapi masih bisa diverifikasi dengan kunci publik yang sama.

Misal diketahui seorang mahasiswa beranama Faqih sudah lulus. Dia memiliki ijazah digital. dalam ijazah tersebut terdapat tulisan sebagai berikut: "Dengan ini saya, Naji Maruf Ilyas selaku Kaprodi Matematika Universitas Bani Yazit, menyatakan bahwa mahasiswa kami dengan nama: Muhammad Oemar Faqih, tempat tanggal lahir: Gresik 12 September 1994, NIM: 12305141043 telah menyelesaikan program studi Matematika yang kami berikan dengan IPK = 3.12 dan predikat Cumlaude pada tanggal 24 Februari 2018." Setelah dihitung, nilai hash ijazahnya adalah 30721. Kemudian pihak universitas menandatangani ijazah tersebut, didapatkan hasil $S = 30721^{157}(mod\ 187) = 15$. Setelah itu perusahaan yang dilamar oleh Nabil mencoba memverifikasinya dengan kunci publik dan tanda tangan digital yang diketahui. Perusahan tersebut menemukan bahwa $V = S^v(mod\ 187) = 15^{53}(mod\ 187) = 53 = D$. Jadi $V = D$. Sehingga dapat disimpulkan bahwa ijazah tersebut masih otentik.

Contoh ini merupakan fungsi tanda tangan digital yang menjamin otentikasi pesan. Contoh berikutnya menunjukkan bahwa tanda tangan digital tidak dapat disangkal. Berikut adalah contohnya.

Sebuah perusahaan telekomunikasi terkenal telah dibobol. Setelah diadakan olah TKP, pihak kepolisian menemukan petunjuk, sebuah kertas bertuliskan 'FIND ME' dan sebuah tanda tangan digital $S = 83$.

Setelah itu pihak kepolisian mengumpulkan daftar hacker di kota itu beserta kunci publik yang dimiliki masing-masing. Mereka mendapatkan 15 hacker beserta kunci publiknya. Daftar nama dan kunci publik disajikan dalam Tabel 2.

Kemudian tanda tangan yang ditemukan itu akan diverifikasi. Verifikasi yang benar menunjukkan bahwa dia adalah pelaku pembobolan yang dicari. Berikut adalah proses pencarian pelaku.

Tabel 2. Daftar Nama dan Kunci Publik

| Nama | Kunci Publik (n,v) | Nama | Kunci Publik (n,v) |
|---|---|---|---|
| Doctor | (1763,101) | Zulfa | (33,13) |
| Nabil | (187,53) | Hamam | (155,29) |
| Barok | (85,47) | Zidni | (55,19) |
| Epep | (899,89) | Faat | (93,23) |
| Defri | (143,29) | Adlan | (62,19) |
| Taufik | (209,31) | Farouq | (77,13) |
| Fadhil | (319,43) | Ajisaka | (217,37) |
| Aghna | (22,7) | | |

Pertama mencari nilai hash dokumen tersebut. Diketahui bahwa nilai hash dokumen tersebut adalah 467. Kemudian memverifikasi tanda tangan dengan kunci publik dari masing-masing orang di atas. Jika hasil verifikasi V=nilai hash, maka dialah orangnya.

Orang yang pertama diteliti bernama Dokter dengan kunci publik $(n, v) = (1763,101)$. Kemudian tanda tangan S=83 dipangkatkan dengan v=101. Diperoleh bahwa $V = S^v(mod\ 1763) = 83^{101}(mod\ 1763) = 1436$. Jadi $V = 1436\ (mod\ 1763) \neq 83(mod\ 1763)$. Ini menunjukkan bahwa Dokter bukanlah pelaku yang diceri.

Orang kedua yang diteliti bernama Nabil dengan kunci publik $(n, v) = (187,53)$. Kemudian tanda tangan S dipangkatkan dengan $v = 53$. Diperoleh bahwa $V = S^v(mod\ 187) = 169^{53}(mod\ 187) = 172$. Jadi $V = 172\ (mod\ 187) \neq 83(mod\ 187)$. Ini menunjukkan bahwa Nabil bukanlah pelaku yang dicari.

Orang ketiga yang diteliti bernama Barok dengan kunci publik $(n, v) = (85,47)$. Kemudian tanda tangan S dipangkatkan dengan v=47. Diperoleh bahwa $V = S^v(mod\ 85) = 83^{47}(mod\ 85) = 83$. Karena $169(mod\ 85) = 83 = V$ berarti bahwa Barok adalah pelaku yang dicari.

Tampilan program GUI matlab yang dapat memudahkan perhitungan proses tanda tangan digital dan verifikasi tanda tangan digital ada dalam Gambar 4.

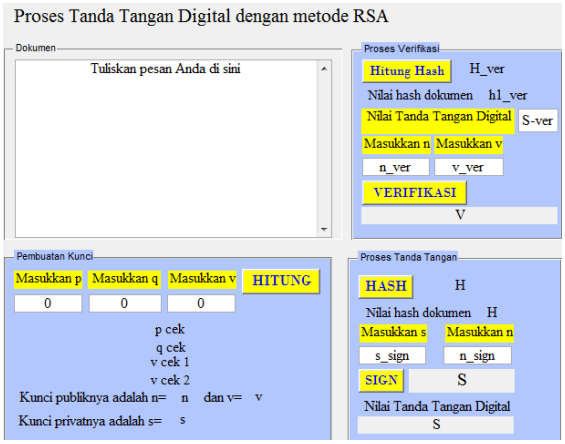
Dalam program tersebut ada empat bagian yaitu dokumen, pembuatan kunci, proses tanda tangan dan proses verifikasi. Dalam bagian dokumen berisi pesan yang ingin ditandatangani. Secara default, pesan tersebut adalah 'Tuliskan pesan Anda di sini' dengan nilai hash $D = 2518$.

Bagian pembuatan kunci berisi bilangan prima p, bilangan prima q, bilangan v, cek p, cek q, v cek 1, v cek 2, kunci publik n dan v, serta kunci privat s. Masukkan bilangan prima $p$ pada kotak putih $p$. Apabila bilangan yang dimasukkan bukan bilangan prima, maka akan muncul tulisan berwarna merah 'bilangan tersebut bukan prima, masukkan bilangan yang lain' pada cek p. Serupa dengan bilangan prima $p$, masukkan bilangan prima $q$ pada kotak putih $q$. Apabila bilangan tersebut bukan prima maka akan muncul tulisan berwarna merah 'bilangan tersebut bukan prima, masukkan bilangan yang lain' pada cek q. Kemudian pada kotak putih $v$, masukkan bilangan $v$ dengan syarat $1 < v < (p-1) * (q-1)$ dan $v$ prima relatif terhadap $(p-1) * (q-1)$. Kotak $v\ cek\ 1$ akan mengecek apakah $1 < v < (p-1) * (q-1)$, apabila $v$ negatif atau lebih dari $(p-1) * (q-1)$, akan muncul tulisan berwarna merah 'Masukkan bilangan positif yang kurang dari $(p-1)(q-1)$'. Sedangkan kotak $v\ cek\ 2$ akan mengecek apakah $v$ dan $(p-1) * (q-1)$ saling prima, apabila v dan $(p-1) * (q-1)$ tidak saling prima, maka akan muncul tulisan 'Masukkan bilangan yang saling prima dengan $(p-1) * (q-1)$'.

Setelah semuanya benar, didapat kunci publik $n$ dan $v$ serta kunci privat $s$. Pada kotak n beriisi bilangan modulo yakni $p * q$. Pada kotak v berisi bilangan v itu sendiri. Kedua bilangan n dan v ini adalah kunci publik tanda tangan digital. Pada kotak $s$ berisi kunci privat $s$ yang akan digunakan untuk menandatangani dokumen digital.

Kemudian pada bagian proses tanda tangan ada tombol hash dan tombol sign, ada kotak putih n dan kotak putih s. Untuk menghitung tanda tangan digital pertama ditekan tombol hash. Bilangan yang muncul adalah nilai hash dari dokumen digital. setelah itu masukkan nilai n pada kotak putih n dan masukkan s pada kotak putih s. Kemudian tekan tombol sign. Bilangan yang muncul adalah nilai tanda tangan digital yang dicari.

Dalam bagian proses verifikasi, terdapat tombol hitung hash dan verifikasi serta kotak putih n, kotak putih v, dan kotak putih S. Untuk memverifikasi tanda tangan digital, terlebih dahulu masukkan pesan yang sudah ditandatangani. Hal ini untuk mengetahui apakah pesan masih asli atau sudah berubah. Kemudian tekan tombol hitung hash. Bilangan yang muncul adalah nilai hash dari pesan tersebut. Kemudian masukkan nilai n pada kotak putih n. Masukkan nilai v pada kotak putih v. Dan masukkan nilai tanda tangan digital pada kotak putih S. Setelah itu tekan tombol verifikasi. Apabila $S^v(mod\ n) = D(mod\ n)$ akan muncul tulisan 'dokumen belum berubah'. Apabila $S^v(mod\ n) \neq D\ (mod\ n)$ akan muncul tulisan 'dokumen sudah berubah'.




Gambar 4. Tampilan GUI matlab proses tanda tangan digital RSA

## SIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan pembahasan yang telah dilakukan, diperoleh kesimpulan sebagai berikut:

1. Pembentukan kunci publik dan kunci privat diawali dengan memilih dua bilangan prima yang berbeda, misal $p\ dan\ q$. Kemudian mengalikan keduanya misal $n = p.q$. Setelah itu memilih bilangan positif, misal $v$, yang kurang dari $\varphi(n)$ dan saling prima dengan $\varphi(n)$. Langkah selanjutnya adalah mencari $s$ yang memenuhi $sv \equiv 1(mod\ \varphi(n))$. Kunci publiknya adalah $(n, v)$ sedangkan kunci privatnya adalah $s$.

2. Proses tanda tangan digital RSA diawali dengan menghitung nilai hash dokumen digital D. Setelah itu menghitung $S = D^s(mod\ n)$. Nilai S ini yang disebut dengan tanda tangan digital.

3. Proses verifikasi tanda tangan digital diawali dengan menghitung fungsi hash dokumen yang telah ditandatangani. Kemudian menghitung $V = S^v(mod\ n)$. Apabila $V = D$ berarti dokumen masih belum berubah, namun bila $V \neq D$ berarti dokumen sudah berubah.

### Saran

Berdasarkan pembahasan dan kesimpulan yang telah didapatkan, berikut beberapa saran yang dapat diberikan:

1. Meskipun tanda tangan digital metode RSA bisa dikatakan aman, namun keamanan yang paling utama tetap pada kerahasiaan kunci privat.

2. Perhitungan nilai hash pada penelitian ini masih menggunakan metode sederhana. Hal ini menagkibatkan adanya kemungkinan terjadi *collision resistance,* yakni diberikan input pesan berbeda tetapi memiliki nilai hash yang sama. Berdasarkan beberapa penelitian, pembuatan tanda tangan digital RSA menggunakan MD5 maupun SHA lebih aman.

## DAFTAR PUSTAKA

Hoffstein, Jeffrey & Jil Phiper & Joseph H Silverman. (2014). *An introduction to mathematical cryptography.* USA: Springer.

Husodo, A. Y. (2010). Penerapan metode digital signature dalam legsalisasi ijazah dan transkrip nilai mahasiswa. *Makalah, Seminar Kriptografi, yang diselenggarakan oleh STEI Institut Teknologi Bandung, tanggal 17 Mei 2010. Bandung: Institut Teknologi Bandung.*

Isnaini, Herdita F. (2016). Penerapan tanda tangan schnorr pada pembuatan tanda tangan digital. *Skripsi.* Fakultas

Matematika dan Ilmu Pengetahuan Alam Universitasa Negeri Yogyakarta.

Leonardo Refialy, Eko Sediyono & Adi Setiawan. (2015). Pengamanan sertifikat tanah menggunakan digital signature SHA-512 dan RSA. *Jurnal Teknik Informatika dan Sistem Informatika, 1(3), 229-234.*

Munir, Rinaldi. (Juni 2005). Penggunaan tanda tangan digital untuk menjaga integritas berkas perangkat lunak. *Prosiding, Seminar Nasional Aplikasi Teknologi Informasi di Yogyakarta yang diselenggarakan oleh Fakultas Teknologi Industri tanggal 18 Juni 2005. Yogyakarta: Universitas Islam Indonesia.*

Spillman, Richard J. (2005). *Classical and contemporary cryptography.* USA: Prentice Hall.

Wahyuni, Sri. (2014). Penerapan digital signature dengan algoritma SHA-1 pada surat legalisasi ijazah dan transkrip nilai mahasiswa. *Jurnal Pelita Informatika Budi Darma*, 7(2), 31-38.