Memvalidasi Integritas Data dan Mengidentifikasi Pengguna melalui Kombinasi Algoritma RSA dan SHA-256

Marvel Pangondian - 135220751

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

113522075@itb.ac.id

*Abstract*—Kriptografi adalah cabang utama dalam ilmu keamanan komputer yang melibatkan teknik-teknik matematis dan komputasi untuk mengamankan komunikasi dan informasi. Tujuan kriptografi adalah teknik-teknik matematis dan komputasi untuk mengamankan komunikasi dan informasi. Salah satu algoritma yang digunakan untuk enkripsi dan deskripsi teks adalah algoritma RSA, tetapi hanya menggunakan algoritma tersebut dapat menyebabkan berbagai masalah. Salah satunya adalah kunci privat/publik yang tidak sesuai ketika mencoba enkripsi/dekripsi teks, keamanan enkripsi/dekripsi yang tidak terlalu bervariasi, serta integritas data yang tidak dapat dideteksi. Dalam makalah ini, akan dibahas penggunaan algoritma *hashing* yakni algoritma SHA-256 dalam meningkatkan keamanan data dan identifikasi pengguna, serta memeriksa integritas kunci publik dan privat yang digunakan.

*Keywords*—Kriptografi, Algoritma RSA, Algoritma SHA-256

# I. PENDAHULUAN

Kriptografi ilmu yang menggunakan matematika untuk mengenkripsi dan mendekripsi data[1]. Sejarah kriptografi bermula ribuan tahun yang lalu, dan penciptaannya didorong oleh kebutuhan akan komunikasi yang aman dan perlindungan informasi yang sensitif. Salah satu metode enkripsi dan dekripsi yang terkenal pada peradaban kuno adalah Sandi Caesar, dinamai oleh penemunya Julius Caesar. Julius menciptakan Sandi Caesar karena dia tidak percaya kurir yang mengirimkan surat tersebut.

Kriptografi diciptakan karena kebutuhan manusia untuk menjaga kerahasiaan data yang mereka miliki. Salah satu algoritma yang efektif dalam melakukan hal ini adalah algoritma RSA(*Rivest-Shamir-Adleman*). Algoritma ini akan mengenkripsi dan mendekripsi teks menggunakan dua kunci berbeda yakni kunci privat dan kunci publik. Kunci publik merupakan kunci untuk melakukan enkripsi kepada sebuah teks, kunci ini bersifat publik dan dapat disebarkan. Kunci privat adalah kunci untuk dekripsi, kunci ini tidak dapat disebarkan. Kedua kunci tersebut akan mengenkripsi dan mendekripsi sebuah teks menggunakan teori bilangan yang akan dibahas lebih dalam pada bagian dasar teori

Algoritma RSA merupakan algoritma yang kuat, tetapi memiliki beberapa kelemahan. Apa yang terjadi jika pengguna mencoba mengakses *plain text* dengan kunci publik/privat yang tidak sesuai ? Atau apa yang terjadi jika enkripsi data diubah, bagaimana pengguna mengetahui hasil enkripsinya telah diubah oleh pihak ketiga ? Untuk menjaga keamanan dan integritas data, diperlukan konsep dan algoritma lain. Konsep yang akan digunakan untuk menangani adalah konsep *signature* .

*Signature* adalah konsep/cara untuk memverifikasi integritas data, pengguna, dan kunci. Dengan konsep *signature*, dapat dibuat sebuah program untuk mendeteksi integritas sebuah data dan mendeteksi apakah data tersebut sudah diubah sebelumnya atau tidak. *Signature* juga digunakan untuk memverifikasi identitas pengguna

Salah satu cara untuk menerapkan konsep *signature* adalah penerapan *signature* kepada sebuah *encrypted text*. Ketika sebuah teks dienkripsi, hasil enkripsi tersebut dapat diubah oleh pengguna lainnya. Untuk mengetahui integritas dari *encrypted text*, dapat digunakan konsep *signature* yang menyimpan *hash value text* sebelumnya, sehingga *text* dapat dideteksi integeritasnya menggunakan *signature* yang sudah disimpan. Jika hasil *hash text* berbeda dengna *signature*, maka *text* tersebut sudah diubah sebelumnya

Salah satu algoritma yang dapat digunakan untuk konsep *signature* ini adalah algoritma SHA-256 yang dapat mengubah sebuah string menjadi *hash value unique* sebesar 256 bits. Dengan algoritma ini, dapat dibentuknya program untuk mengecek integritas pengguna dan data yang ingin dideskripsi

# II. LANDASAN TEORI

1. *Bilangan Bulat*

Bilangan bulat adalah angka-angka yang tidak memiliki bagian desimal atau pecahan. Bilangan ini dapat berupa angka positif, negatif, atau nol. Bilangan bulat termasuk dalam kategori bilangan cacah (non-negatif) dan bilangan negatif. Bilangan bulat dapat berupa bilangan positif (1, 2, 3, ...), bilangan negatif (-1, -2, -3, …), dan nol (0).

1. *Bilangan Riil*

Bilangan riil adalah bilangan yang mencakup seluruh bilangan yang mencakup seluruh bilangan rasional dan irasional. Bilangan riil terdiri atas bilangan bulat (…,-3, -2, -1, 0, 1, 2, 3,…), bilangan rasional (1/2, -5/4, dll), dan bilangan irasional (√2, π, dll).

1. *Bilangan Prima*

Bilangan prima adalah bilangan bulat yang lebih dari satu dan hanya dapat dibagi oleh 1 dan bilangan tersebut sendiri. Contoh bilangan bulat adalah 7 karena 7 hanya dapat habis dibagi oleh 1 dan 7 saja. Bilangan selain bilangan prima disebut sebagai bilangan komposit

1. *Sifat Pembagian*

Sebuah bilangan bulat *a* habis membagi sebuah bilangan bulat *b* jika dan hanya jika terdapat sebuah bilangan *c* yang merupakan bilangan bulat, sedemikian hingga *ac = b* . Jika tidak ada *c*, maka *a* tidak habis membagi *b.* Berikut adalah notasi sifat pembagian :

1. *Teorema Euclidean*

Teorema Eculidean menyatakan bahwa untuk setiap dua integer, *m* (pembilang) dan *n* (penyebut), di mana n tidak sama dengan nol, terdapat dua integer *q* (hasil bagi)dan *r* (hasil sisah) sedemikian hingga,

1. *Pembagi Bersama Terbesar (gcd)*

Pembagi bersama terbesar (gcd) merupakan bilangan bulat terbesar *c* sedemikian hingga dapat habis membagi dua bilangan bulat *a* dan *b*.

1. *Algoritma Euclidean*

Algoritma Euclidean adalah algoritma untuk mencari gcd dari dua bilangan bulat. Algoritma ini menyatakan bahwa untuk setiap bilangan bulat non negatif *m* dan *n* di mana *m*  ≥ *n*, maka jika *m = r0*  dan *n = r1*berlaku :

Dengan aturan di atas, maka gcd *m* dan *n* dapat dicari menggunakan Teorema 2,

1. Relatif Prima

Dua bilangan, *m* dan *n*, dikatakan relatif prima jika dan hanya jika,

Relatif prima akan digunakan dalam implementasi enkripsi menggunakan algoritma RSA

1. *Aritmatika Modulo*

Untuk bilangan bulat *m* dan *n* di mana berlaku kombinasi linier sebagai berikut :

maka dapat ditulis ulang sebagai berikut :

notasi di atas dapat diinterpretasikan sebagai “*a* dibagi dengan *m* menghasilkan sisa *r* ”

1. *Kongruen dan Sifat – Sifatnya*

Untuk bilangan bulat *a* dan *b* dikatakan kongruen jika dan hanya jika terdapat modulus *c* yang membagi  *a*  dan *b* dan menghasilkan sisa *r* yang sama

Jika berlaku di atas, maka *a* kongruen dengan *b* dalam modulus *c*. Bilangan *a* dapat dikatakan kongruen dengan b dalam jika dan hanya jika (*a*-*b*) juga habis dibagi dengan *c*.

melalui kongruen, didapat beberapa sifat yakni,

1. Jika *a* ≡ *b* (mod *c*), dan *k* adalah sembarang bilangan bulat, maka berlaku
2. (*a + k*) ≡ (*b + k* ) (mod *c*)
3. *ak* ≡ *bk* (mod *c*)
4. *ak* ≡ *bk* (mod *c*) , *k* bilangan bulat tak-negatif
5. Jika *a* ≡ *b* (mod *c*) dan *k* ≡ *m* (mod *c*), maka
6. (*a + k*) ≡ (*b + m*) (mod *c*)
7. *ak* ≡ *bm* (mod *c*)
8. *Balikan Modulo (Modulo Inverse)*

Untuk mencari inverse dari *a* (mod b), maka harus berlaku gcd(*a, b*) = 1, jika tidak maka *a* (mod b) tidak memiliki inverse. Untuk gcd(*a, b*) = 1, maka berlaku :

melalu implikasi, didapat :

Perhatikan bahwa

maka,

Kekongruenan terakhir ini berarti m merupakan *inverse* dari a (mod b). Cara lain mencari inverse dari *a* (mod *b*) adalah dengan cara berikut :

*x* yang merupakan *inverse* dari *a* (mod *b*) dapat diperoleh dengan mencari nilai *k* sedemikian hingga hasil *x* di atas merupakan bilangan bulat.

1. *Kekongruenan Linier dan Sistem Kekongruenan linier*

Kekongruenan linier secara umum memiliki bentuk sebagai berikut:

solusi ­­*x* dapat dicari dengan mengubah bentuk kongruen di atas menjadi

dengan memilih nilai k sedemikian hingga hasil *x* adalah bilangan bulat. Nilai *k* yang menghasilkan nilai *x* merupakan bilangan bulat.

Sistem kekongruenan linier berarti sistem kongruen dengan lebih dari satu kongruen, sebagai contoh :

Sistem ini dikenal sebagai sistem kekongruenan linier karena setiap persamaan adalah kongruen linier. Untuk memecahkan sistem kekongruenan linier, kita perlu mencari *x* yang memenuhi semua kongruen pada sistem kekongruenen linier. Dalam banyak kasus, sistem kekongruenan linier dapat dipecahkan menggunakan teorema Chinese Remainder Theorem (CRT)

1. *Kriptografi*

Kriptografi adalah seni menyembunyikan data menggunakan ilmu matematika. Kriptografi berasal dari bahasa Yunani "kryptós" yang berarti tersembunyi/rahasia, serta "gráphein" yang berarti menulis. Ketika kedua kata tersebut digabung, didapat kata kriptografi yang berarti studi mempelajari teknik – Teknik untuk menyembunyikan data agar terlindungi dari pihak ketiga. Kriptografi memiliki tujuan yakni menjaga pesan/data agar tidak dapat dibaca oleh pihak ketiga. Kriptografi terdiri atas dua komponen yakni pesan (*plaintext*) yang berisi data/informasi yang ingin disembunyikan, serta *cipherteks* (*ciphertext*) yang berisi hasil setelah pesan disembunyikan. Terdapat dua proses utama dalam kriptografi yakni proses enkripsi dan dekripsi. Proses enkripsi adalah proses mengubah sebuah data, biasanya sebuah pesan, menjadi data yang tidak dapat dibaca oleh orang lain secara umum. Hasil proses enkripsi adalah text/data yang bersifat *unreadable/indecipherable.* Proses berikutnya dalam kriptiografi adalah proses dekripsi. Proses ini melibatkan *ciphertext* dan mengubah kembali menjadi *plain text*. Proses ini hanya dapat dilakukan oleh pengguna yang mengetahui jenis algoritma yang digunakan untuk mengenkripsi *plain text* serta mengetahui kunci – kunci yang digunakan.

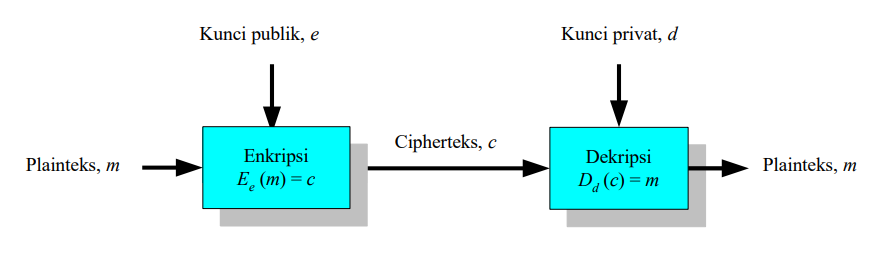
*Gambar 2.1 Alur Kriptografi*

*Sumber :* [*https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf*](https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf)

Kripografi terdiri atas dua tipe, yakni tipe pertama *Symmetric-Key Cryptography* dan tipe kedua *Public-Key Cryptography (Asymmetric Cryptography)*[2]*.* Untuk tipe pertama, kriptografi menggunakan satu kunci saja untuk enkripsi dan dekripsi, sedangkan tipe kedua menggunakan dua kunci yakni kunci publik untuk enkripsi, dan kunci privat untuk dekripsi. Di antara kedua tipe, tipe kedua memiliki keamanan yang lebih ketat dibandingkan tipe pertama. Salah satu algoritma implementasi kriptografi tipe *Asymmetric Cryptography* adalah algoritma RSA (*Rivest-Shamir-Adleman*).

1. *Algoritma RSA (Rivest-Shamir-Adleman)*

Algoritma RSA dinamakan berdasarkan penemunya yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Algoritma ini merupakan penerapan jenis kriptografi yakni *Asymmetric Cryptography* yang menggunakan dua kunci[8]. Dua kunci tersebut adalah kunci publik untuk enkripsi dan kunci privat untuk dekrispi.



*Gambar 2.2 Alur Algoritma RSA*

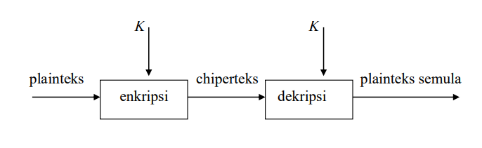
*Sumber :* [*https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf*](https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf)

alur pembuatan kunci algoritma RSA adalah sebagai berikut :

1. Pertama, dipilihnya dua angka, *p* dan *q* yang merupakan angka prima yang *random* dan berbeda.
2. Menhitung *n* = *pq* yang merupakan modulus algoritma RSA (tidak perlu dirahasiakan)
3. Menghitung *ϕ*(*n*) = (*p - 1*) (*q - 1*)(perlu dirahasiakan)
4. Mencari kunci publik (e), kunci tersebut memiliki nilai 1 < *e* < *ϕ*(*n*) dan relatif prima dengan *n* dan *ϕ*(*n*). Kunci ini akan digunakan untuk enkripsi dan dapat disebarkan
5. Mencari kunci privat (*d*) yang memenuhi syarat *de ≡* 1 (mod *ϕ*(*n*)). Kunci privat (*d*) akan digunakan untuk mendekripsi *ciphertext*

alur enkripsi dan dekripsi dengan algoritma RSA:

1. Pertama, akan dibuat kunci publik (*e*) dan kunci privat (*d*). Pembentukan kunci biasanya dilakukan dengan memilih *p* dan *q* yang random
2. Untuk enkripsi, mengubah tiap *character* pada *plain text* menjadi unicode, setelah itu mengubah tiap *value* *character* menjadi *value* lain dengan rumus berkut :

**Setelah itu hasilnya disimpan menjadi *cipher text*

1. Untuk dekripsi, pertama menerima *cipher text* dan mengubah setiap *character* *value* pada *cipher text* kembali menjadi *value* semula dengan rumus berikut :

hasilnya kemudian disimpan menjadi *plain text* yang semula

1. *Fungsi Hash*

Fungsi hash adalah algoritma matematis yang mengubah input data (pesan) menjadi nilai hash dengan panjang tetap digunakan untuk beragam keperluan, termasuk memastikan keutuhan data, memvalidasi kata sandi, dan menyimpan data dalam bentuk struktur data hash. Salah satu fungsi hash yang efektif adalah SHA-256 (*Secure Hash Algorithm 256-bit*)

1. *Fungsi Hash SHA-256 (Secure Hash Algorithm 256-bit)*

SHA-256, yang merupakan singkatan dari Secure Hash Algorithm 256-bit, adalah suatu algoritma hash kriptografis yang termasuk dalam serangkaian algoritma Secure Hash Algorithm (SHA) yang dirancang oleh National Institute of Standards and Technology (NIST) Amerika Serikat. Proses SHA-256 menghasilkan nilai hash yang memiliki panjang tetap sebesar 256 bit, setara dengan 32 byte.

1. *Digital Signature*

*Digital signature* adalah jenis tanda tangan elektronik khusus yang melibatkan penggunaan teknik kriptografi. *Digital signature* menyediakan cara yang aman dan tahan terhadap penyusup untuk mengonfirmasi asal dan otentikasi pesan atau dokumen digital. *Signature* ini bergantung pada kriptografi kunci publik, di mana kunci pribadi digunakan untuk menghasilkan tanda tangan, dan kunci publik yang sesuai digunakan untuk memverifikasinya. *Digital Signature* digunakan untuk memastikan bahwa informasi berasal dari pengguna yang benar dan memvalidasi integritas data[10].

# III. ANALISIS MASALAH

## A. Implementasi Konsep Digital Signature

Salah satu cara untuk memvalidasi integritas data adalah melalui *Digital signature*. *Digital signature* digunakan untuk memastikan data valid/tidak diubah oleh pihak luar. Implementasi *Digital signature* akan menggunakan fungsi hash SHA-256 untuk menghash data berupa *text* menjadi nilai hash yang memiliki panjang tetap sebesar 256 bit, setara dengan 32 byte. Alasan penulis memilih fungsi hash SHA-256 adalah agar memastikan besar *signature* selalu konsisten serta algoritma SHA-256 telah terbukti menghasilkan probabilitas *collision* yang rendah[3] . *Signature* akan dimasukan pada hasil enkripsi (*cipher text*) dan akan diambil kembali ketika ingin memvalidasi integritas data. *Signature* juga akan digunakan untuk mengecek integritas *private key* dan *public key* yang digunakan pengguna untuk enkripsi atau dekripsi.

## B. Validasi Integritas Data

Data akan divalidasi melalui *signature* yang ada dalam data tersebut. Pada proses enkripsi, *text* akan diubah menjadi *hash value* 256 bit menggunakan algoritma SHA-256. *Hash value* tersebut kemudian dijadikan *signature* dengan menggunakan *private key (d)*. Caranya adalah dengan mengenkripsi hash *value* tersebut menggunakan *d* dan *modulus (n)* . *Signature* kemudian dimasukan ke dalam *cipher text*. Ketika ingin validasi integritas data, maka *signature* dalam *cipher text* perlu dipsah dari *cipher text* terlebih dahulu. *Cipher text* perlu di dekripsi, setelah itu hasil dekripsi di hash menggunakan algoritma SHA-256. Signature awal text di ubah menjadi *value* semulanya (*value* sebelum di enkripsi menjadi signature) dengan menggunakan kunci publik (*e*) dan modulus (*n*) . Hasil *hash* semula kemudian di bandingkan dengan hasil hash dekripsi. Jika sama, maka data sama dengan data orijinal, jika beda maka data telah diubah/diedit oleh pihak ketiga (*data is compromised*).

## B. Validasi Pengguna

Ketika mencoba untuk mendekripsi/mengenkripsi data, perlu dipastikan integritas *private key* dan *public key* yang digunakan. Hal tersebut dapat dilakukan dengan melakukan validasi pengguna. Setiap pengguna akan memiliki *username* dan *password* pilihan mereka sendiri, kemudian program akan menggunakan *private key* , *username*, dan *password* untuk membuat *signature* unik yang akan digunakan untuk menvalidasi *publik key* dan *private key ,* *signature* tersebut kemudian disimpan di *database*. Ketika pengguna ingin mengenkripsi/mendekrispsi, program akan meminta *username, password, public key,* dan *private key* pengguna, kemudian program akan memvalidasi integritas *public key,* dan *private key* berdasarkan *signature* yang sudah disimpan di database.

## C. Implementasi Algoritma RSA

Algoritma enkripsi dan dekripsi yang akan digunakan adalah algoritma RSA (*Rivest-Shamir-Adleman*). Berikut alur enkripsi dalam implementasi RSA menggunakan python :

1. Menerima *message* yang akan dienkripsi
2. Mengubah tiap *character* pada *message* menjadi integer dengan menggunakan *public key* dan modulus ()
3. Tiap integer diuabah menjadi string, dan di padding dengan “0” untuk memastikan tiap representasi *character* memiliki panjang 6 angka
4. Setelah itu, tiap representasi *character* di konkatenasi menjadi satu string yang besar
5. String tersebut kemudian di save di database yakni pada .json file
6. Pada .json file juga disimpan *signature* message yang sudah dibuat dengan menggunakan *private key*

Berikut alur dekripsi dalam implementasi RSA menggunakan python :

1. Pertama, user akan memilih *entry/message* yang ingin didekripsi
2. Program akan mengambil data dari *database* yakni *cipher text*
3. *Cipher text* tersebut kemudian di parser menjadi *block of 6 characters*, kemudian tiap blok tersebut diubah menjadi integer
4. Tiap block merupakan representasi tiap *character* yang perlu didekrispi. Tiap blok didekripsi dengan menggunakan *private key (d)* dan *modulus (n)* dari pengguna (). Setelah tiap blok didekripsi, maka perlu dikonkatenasi menjadi satu *string* yang merupkan *plain text*
5. Sebelum hasil dekripsi dikirim ke pengguna, perlu validasi integritas data terlebih dahulu. *Signature* *data* yang disimpan pada *database* akan digunakan dan dibandingkan dengan *signature* yang dihasilkan menggunakan hasil dekripsi. Jika kedua *signature* berbeda, maka terbukti bahwa *cipher text* telah diubah oleh pihak ketiga.

## D. Database

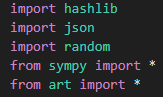
Untuk menyimpan hasil *signature* untuk memvalidasi isi data dan memvalidasi pengguna, diperlukan *database* untuk menyimpan *signature* pengguna serta *cipher text* yang berisi *signature* data. Jenis data yang penulis gunakan untuk menyimpan hal-hal tersebut adalah .json file. Implementasi ini masih sederhana, dalam dunia nyata .json file jarang digunakan sebagai tempat penyimpanan data, tetapi dalam kasus simpel ini pengguna menggunakan .json file untuk memudahkan proses *debugging.* .json file akan berupa list of dictionary, dalam setiap dictionary akan terdiri atas “id”, “username”, “signature”, “data” sebagai keys nya. *Value* “id” berisi id dari dictionary, *value* “username” akan berisi username pengguna yang sudah di hash menggunakan algoritma SHA-256 (untuk menjaga keamanan dan menghemat data, ukuran string dalam python secara default 48 byte (jika string kosong), jauh lebih besar dibandingkan hasil hash SHA-256 yakni 32 byte[9]), *value* “siganature” adalah *signature* pengguna yang akan digunakan untuk validasi pengguna, *value* “data” adalah *cipher text* berserta *signature* data yang sudah disisipkan pada *cipher text* yang akan digunakan untuk memvalidasi integritas data

# IV. IMPLEMENTASI PROGRAM

Penulis berhasil membuat program yang dapat memvalidasi integritas data serta mengidentifikasi pengguna dengan menggunakan bahasa *pyhton*. Program secara garis besar akan membuat *digital signature* menggunakan *private key* dan *text*  yang ingin pengguna enkripsi. *Digital signature* tersebut dibuat dengan menggunakan algoritma SHA-256. Untuk algoritma SHA-256 sendiri, penulis menggunakan library hashlib. Untuk algortima enkripsi serta dekripsi, penulis menggunakan algoritma RSA. Implementasi program mengunakan library serta fungsi sebagai berikut :

1. ***hashlib, json, random, sympy, art***

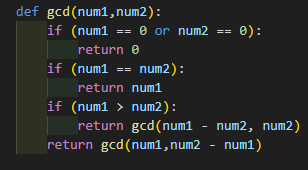
Library yang digunakan berupa library *hashlib* untuk implementasi SHA-256, library *json* untuk implementasi *database,* library *random* yang digunakan saat ingin memilih bilangan prima secara acak serta memilih *public key*, library *sympy* untuk membantu dalam memilih bilangan prima, dan library *art* untuk menu utama



*Gambar 4.1 Library yang digunakan dalam implementasi program*

*Sumber : Dokumentasi pribadi*

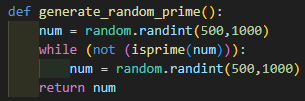
1. **gcd**

Fungsi ini menerima dua angka dan mengembalikan gcd (*greates common divisor*) dari kedua angka tersebut. Penulis menggunakan rekursi dan algoritma euclidean dalam implementasi fungsi ini.

*Gambar 4.2 Fungsi gcd untuk menemukan gcd dua angka*

*Sumber : Dokumentasi pribadi*

1. **generate\_random\_prime**

Fungsi ini akan mengembalikan sebuah bilangan prima secara acak. Fungsi ini menggunakan library *random* dalam memlih angka dan fungsi *isprime* yang merupkan fungsi dari library *sympy* untuk memastikan bilangan merupakan bilangan prima. Penulis membatasi *range* dari angka yang dipilih yakni dari 500 sampai 1000 untuk mempermudah kalkulasi serta menghindari terpilihnya bilangan prima yang terlalu kecil ( < 100).

*Gambar 4.3 Fungsi untuk mencari bilangan prima secara acak*

*Sumber : Dokumentasi pribadi*

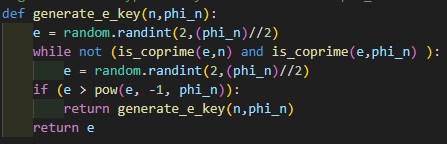
1. **is\_coprime**

Fungsi ini menerima dua angka dan mengembalikan *true* jika kedua angka tersebut adalah relatif prima

*Gambar 4.4 Fungsi untuk memastikan dua angka relatif prima*

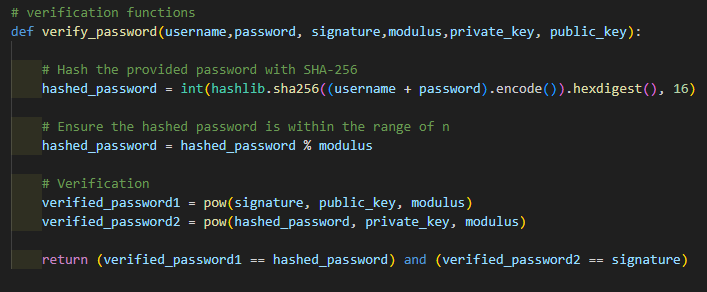
*Sumber : Dokumentasi pribadi*

1. **generate\_e\_key**

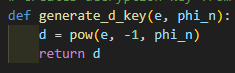
Fungsi ini akan menghasilkan *public key* yang sesuai dengan modulus dan hasil *phi function­ (φ(n)).* Pemilihan *public key* dilakukan secara acak, yakni dengan menggunakan library *random.* Untuk *range* dari *public key,* penulis membatasinya supaya mengurangi waktu pencarian yang dibutuhkan

*Gambar 4.5 Fungsi untuk membuat public key*

*Sumber : Dokumentasi pribadi*

1. **generate\_d\_key**

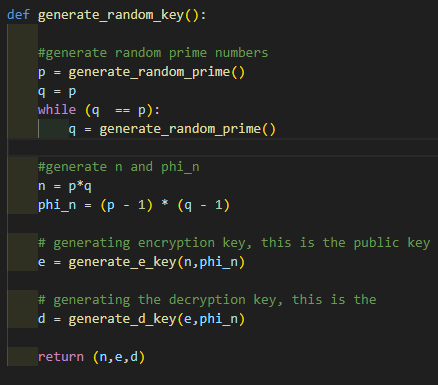
Fungsi ini akan menghasilkan *private key* sesuai dengan *public key* dan hasil *phi function* yang sudah dibuat sebelumnya



*Gambar 4.6 Fungsi untuk membuat private key*

*Sumber : Dokumentasi pribadi*

1. **generate\_random\_key**

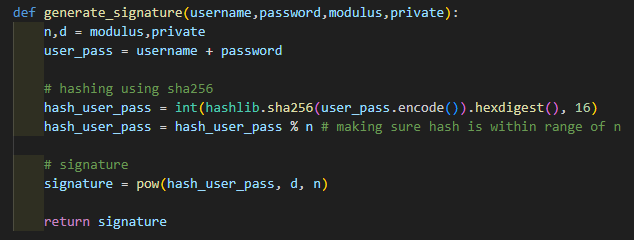
Fungsi ini akan membuat dan mengembalikan *modulus, public key,* dan *private key*.

*Gambar 4.7 Fungsi untuk membuat modulus, private key, dan public key*

*Sumber : Dokumentasi pribadi*

1. **generate\_signature**

Fungsi in akan membuat *Digital signature* dari *username*, *password*, *modulus*, dan *private key* pengguna. *Digital signature* ini akan dipakai ketika ingin identifikasi pengguna serta memvalidasi *private key* dan *public key* pengguna. Fungsi akan menggabungkan *username* dan *password* pengguna menjadi satu string yang kemudian akan di hash menggunakan algoritma SHA-256. Hasil hash akan dijadikan *Digital signature* dengan mengenkripsi hasil hash menggunakan *private key.*



*Gambar 4.8 Fungsi untuk membuat digital signature pengguna*

*Sumber : Dokumentasi pribadi*

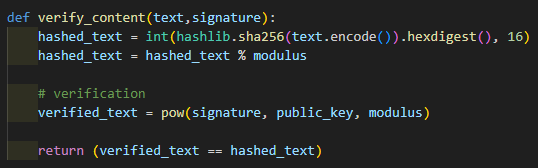
1. **verify\_password**

Fungsi ini akan memvalidasi *username, password, private key,* dan *public key* yang akan digunakan oleh pengguna. Cara kerja fungsi secara garis besar sama dengan yang sudah dijelaskan pada bagian *Validasi Pengguna* bab III laporan.

*Gambar 4.9 Fungsi untuk memvalidasi pengguna*

*Sumber : Dokumentasi pribadi*

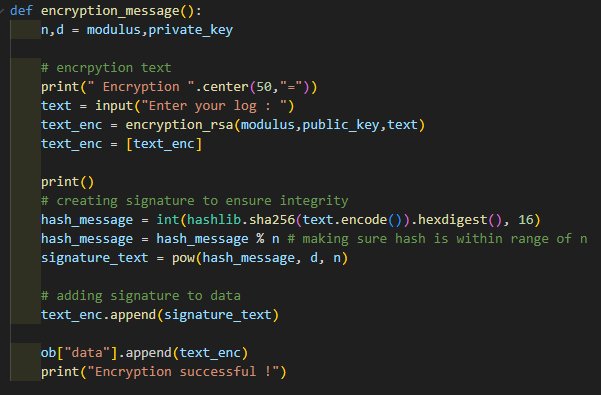
1. **verify\_content**

Fungsi ini akan memvalidasi integritas data *cipher text* yang sudah disimpan di *databse*. Cara kerja fungsi secara garis besar sama dengan yang sudah dijelaskan pada bagian *Validasi Integritas Data* bab III laporan.

*Gambar 4.10 Fungsi untuk memvalidasi integritas data*

*Sumber : Dokumentasi pribadi*

1. **encryption\_message**

Fungsi untuk mengenkripsi pesan pengguna (dengan memanggil fungsi *encryption\_rsa*) serta membuat *signature* pesan tersebut.

*Gambar 4.11 Fungsi untuk mengenkripsi dan membuat signature pesan*

*Sumber : Dokumentasi pribadi*

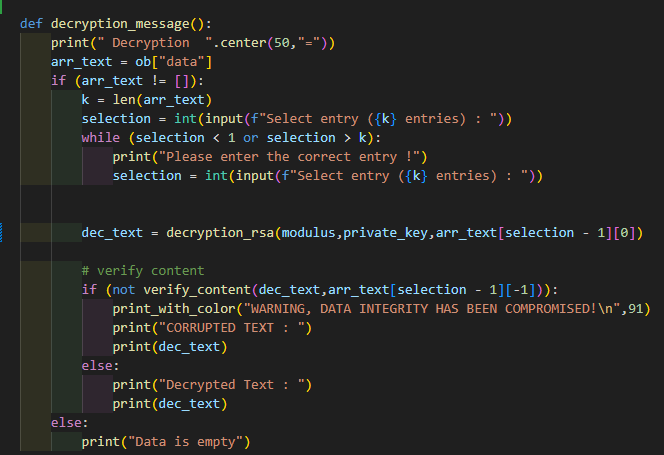
1. **encryption\_rsa**

Fungsi untuk mengenkripsi pesan menggunakan algoritma RSA. Fungsi in mengembalikan *cipher text* yang merupakan *string integer* yang merupakan representasi integer hasil enkripsi dalam bentuk *string* yang sudah dipadding dengan angka 0. Alasan dipaddign adalah supaya setiap blok string yang merepresentasikan karakter itu konsisten panjangnya, yakni 6 *character integer.*

*Gambar 4.12 Fungsi untuk mengenkripsi string menggunakan algoritma rsa*

*Sumber : Dokumentasi pribadi*

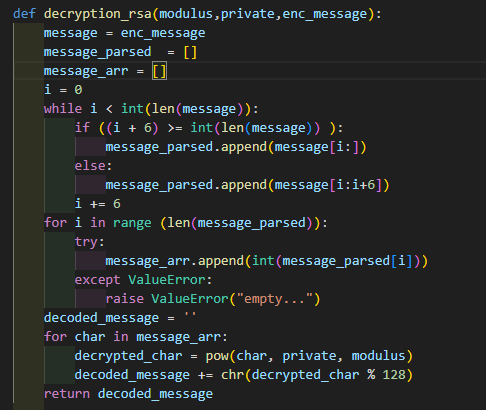
1. **decryption\_message**

Fungsi ini akan mendekripsi *cipher text* yang dipilih pengguna. Setiap pengguna memiliki *entry* masing – masing, yakni *cipher text* yang sudah disimpan di database. Setiap pengguna dapat memiliki lebih dari satu *entry* sehingga pengguna harus memilih dulu *entry* yang ingin didekripsi. Setelah itu, fungsi ini akan mencoba mendekripsi *entry* yang sudah dipilih pengguna dengan memanggil fungsi *decryption\_rsa*. Hasil dekripsi tersebut akan divalidasi integritasnya dengan menggunakan fungsi *verify\_content*

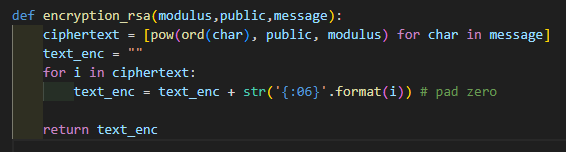
*Gambar 4.13 Fungsi untuk mendekripsi dan memvalidasi cipher text*

*Sumber : Dokumentasi pribadi*

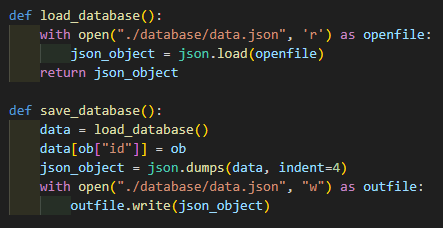
1. **decryption\_rsa**

Fungsi ini akan menerima *modulus, private key,* dan *cipher text* untuk mengembalikan hasil dekripsi *cipher text.* *Cipher text* akan diparse mejadi *block of 6 characters*. Setelah diparse, setiap blok akan diubah kembali menjadi integer dan kemudian didekripsi menggunakan algoritma RSA

*Gambar 4.14 Fungsi untuk mendekripsi cipher text*

*****Sumber : Dokumentasi pribadi*

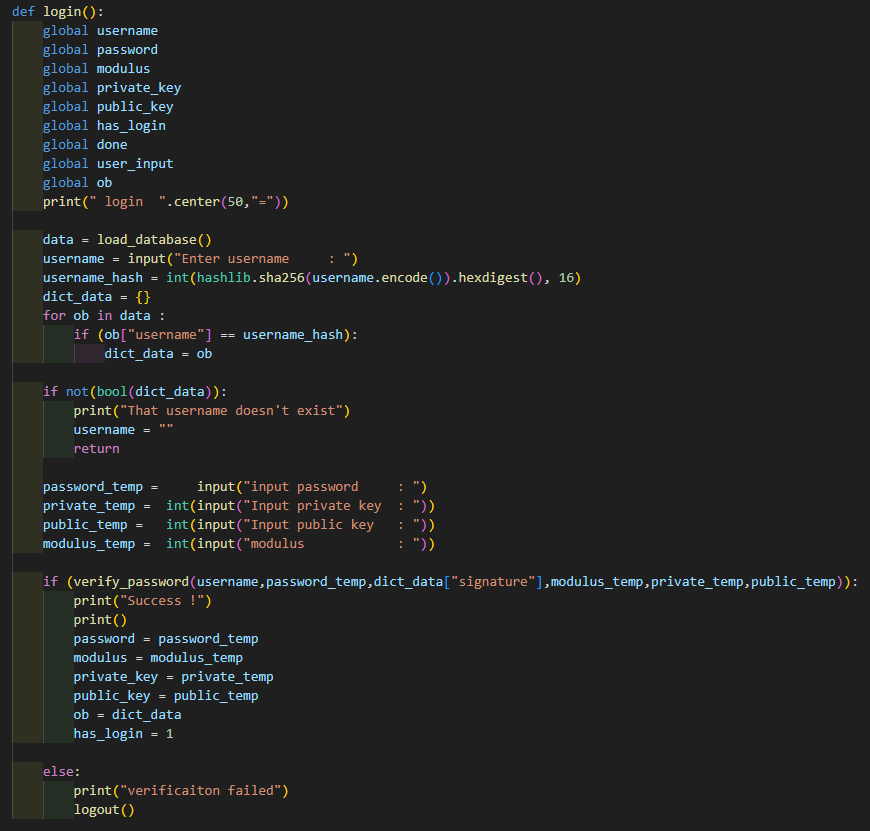
1. **load\_database dan save\_database**

Fungsi *load\_database* akan membuka dan *load* data yang ada pada *database*. Fungsi *save\_databse* akan menyimpan data ke *database*

*Gambar 4.15 Fungsi – fungsi yang mengatur database*

*Sumber : Dokumentasi pribadi*

1. **login**

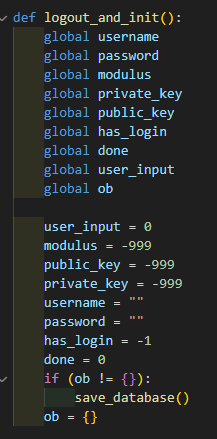
Fungsi ini akan memvalidasi *username, password, private key,* dan *public key* serta mengidentifikasi pengguna.

*Gambar 4.16 Fungsi untuk mengidentifikasi pengguna*

*Sumber : Dokumentasi pribadi*

1. **logout\_and\_init**

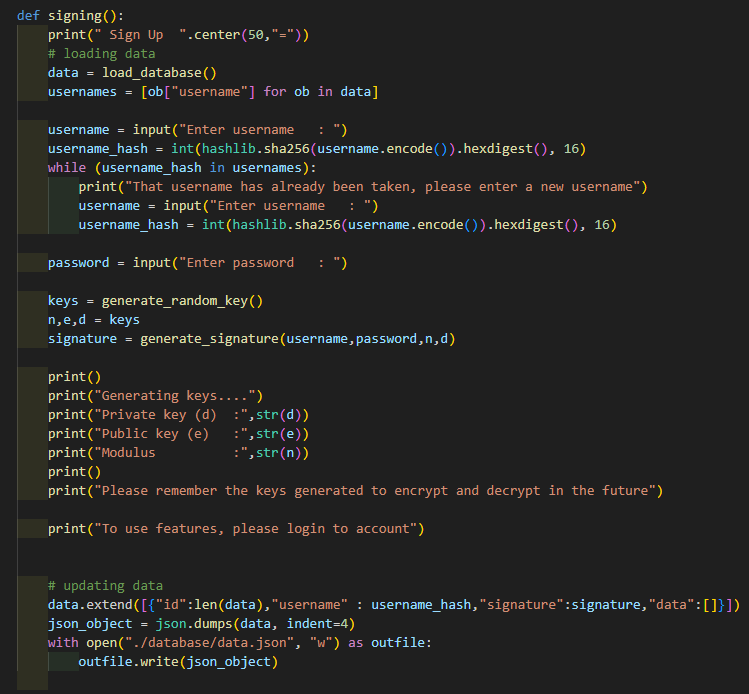
Fungsi ini digunakan pada saat pengguna ingin ”logout” , yakni ketika pengguna mungkin ingin menggunakan *public key* dan *private key* yang berbeda, atau pengguna ingin *signing* baru. Fungsi ini akan me-*reset* variabel global yang ada pada program.



*Gambar 4.17 Fungsi untuk logout*

*Sumber : Dokumentasi pribadi*

1. **signing**

Fungsi ini akan dipanggil ketika pengguna ingin membuat *digital signature* yang baru yang akan digunakan untuk identifikasi pengguna. Fungsi ini akan meminta *username* dan *password* yang unik dari pengguna untuk digunakan dalam pembuatan *digital signature*. Kemudian, fungsi akan memberikan *private key, public key,* dan *modulus* yang pengguna harus simpan. Fungsi ini ibaratnya membuat “akun” baru bagi pengguna yang pengguna dapat gunakan untuk enkripsi dan dekripsi pesan.

*Gambar 4.18 Fungsi untuk signing*

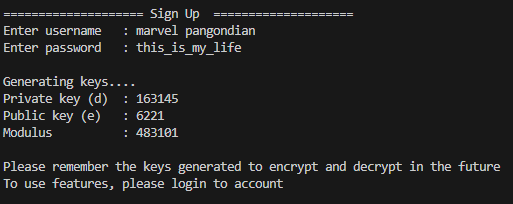
*Sumber : Dokumentasi pribadi*

# V. HASIL UJI COBA

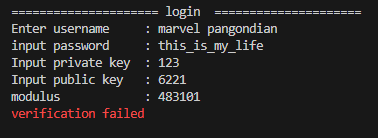
Penulis akan mencoba program dengan petama membuat *signing* baru dan mencoba mengenkripsi dan mendekripsi sebuah pesan. Setelah selesai, penulis akan mencoba mengubah data yang tersimpan pada *database*. Penulis melakukan hal ini dengan tujuan mengetes program dalam hal pengecekan validasi integritas data. Berikut hasil uji coba yang dilakukan penulis :

1. **membuat signing baru dan mencoba identifikasi pengguna**

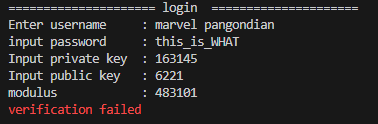
Pertama, penulis akan mencoba untuk membuat signing baru dan mengetes kemampuan identifikasi pengguna pada program. Berikut hasilnya:



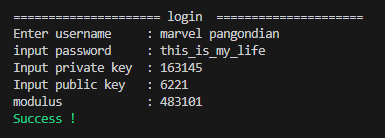
*Gambar 5.1 Signing*

*Sumber : Dokumentasi pribadi*

*Gambar 5.2 Gagal verifikasi, private key salah*

*Sumber : Dokumentasi pribadi*

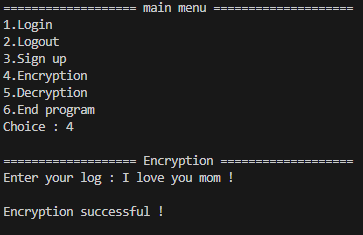
*Gambar 5.3 Gagal verifikasi, password salah*

*Sumber : Dokumentasi pribadi*

*Gambar 5.4 Verifikasi berhasil*

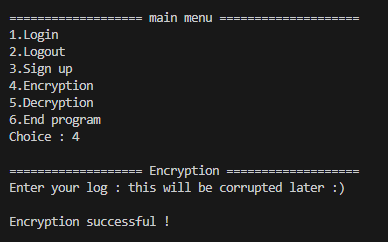
*Sumber : Dokumentasi pribadi*

1. **percobaan enkripsi dan dekripsi**

Setelah berhasil identifikasi pengguna, penulis mencoba berbagai tes mengenai enkripsi dan dekripsi. Pada salah satu tes, penulis mengubah data yang terdapat di dalam database.

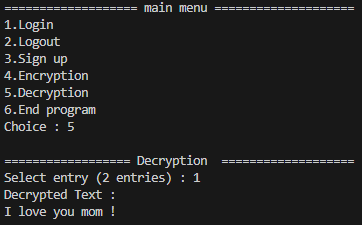
*Gambar 5.5 Enkripsi pesan pertama*

*Sumber : Dokumentasi pribadi*



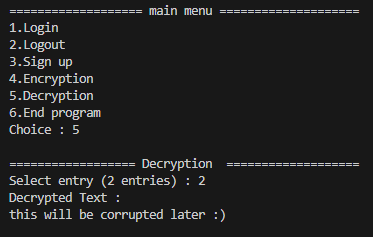
*Gambar 5.6 Enkripsi pesan kedua*

*Sumber : Dokumentasi pribadi*

**

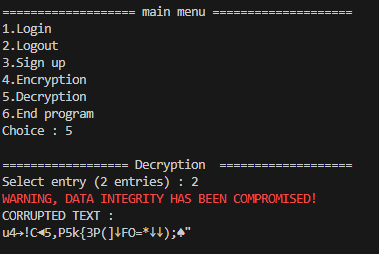
*Gambar 5.7 Dekripsi pesan pertama*

*Sumber : Dokumentasi pribadi*

**

*Gambar 5.8 Dekripsi pesan kedua*

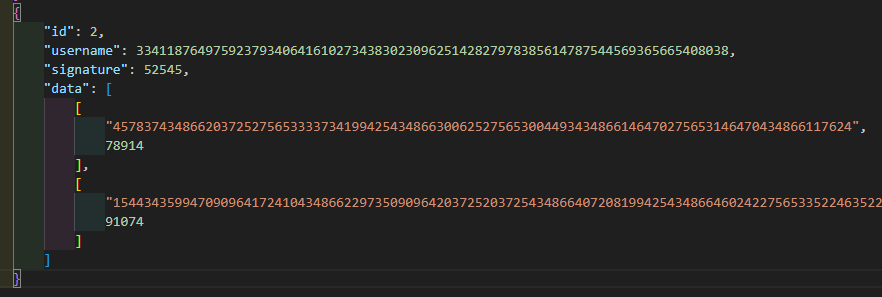
*Sumber : Dokumentasi pribadi*

**

*Gambar 5.9 Dekripsi pesan kedua setelah diubah isi datanya*

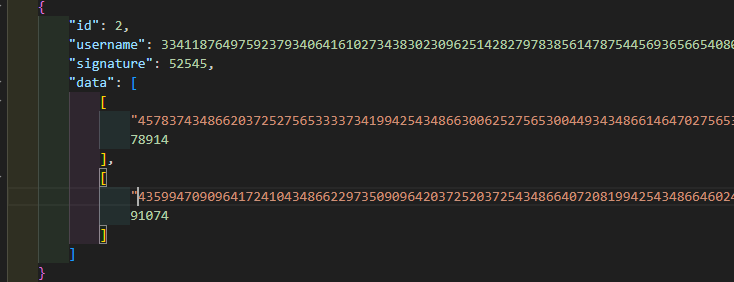
*Sumber : Dokumentasi pribadi*

Pada gambar 5.9, penulis menggantikan is dari *cipher text* pada *database*. Penulis menghapus 5 angka pertama pada *cipher text* sehingga membuat *cipher text* terkorupsi. Berikut sebelum dan sesudah data diubah pada *database* :



*Gambar 5.10 Data sebelum diubah*

*Sumber : Dokumentasi pribadi*



*Gambar 5.11 Data setelah diubah*

*Sumber : Dokumentasi pribadi*

Melalui uji coba ini, dapat terlihat bahwa metode menggunakan *digital signature* merupakan metode yang efektif dalam memvalidasi integritas data serta identifikasi pengguna. Implementasi *digital signature* menggunakan kombinasi algoritma SHA-256 dan RSA merupakan implementasi yang efektif karena dapat menghasilkan *signature* yang unik, rentan *collision*, serta efektif dalam memvalidasi integritas data.

# VI. KESIMPULAN

Data pribadi merupakan aset yang memerlukan perlindungan optimal. Salah satu pendekatan untuk menjaga keamanannya adalah melalui kriptografi yang merupakan metode mengubah data, biasanya teks biasa, menjadi teks sandi yang tidak dapat dibaca. Meskipun demikian, risiko perubahan oleh pihak ketiga masih dapat terjadi terhadap teks sandi tersebut. Untuk menanggulangi risiko ini, penggunaan tanda tangan digital muncul sebagai solusi efektif. Penerapan tanda tangan digital, terutama dengan menggunakan kombinasi algoritma SHA-256 dan RSA, membentuk suatu metode yang mampu memvalidasi integritas data (teks sandi) yang telah disimpan. Melalui mekanisme ini, kita dapat dengan cepat mendeteksi apakah data telah mengalami perubahan oleh pihak yang tidak sah. Dengan demikian, penggunaan tanda tangan digital tidak hanya meningkatkan integritas data, tetapi juga memperkuat keamanan secara keseluruhan.Top of Form

# VII. UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan pada Tuhan Yang Maha Esa atas rahmatnya yang berlimpah sehingga penulis dapat menyelesaikan karya tulis ilmiah yang berjudul “Memvalidasi Integritas Data dan Mengidentifikasi Pengguna melalui Kombinasi Algoritma RSA dan SHA-256”. Karya tulis ini bertujuan memenuhi salah satu tugas pada mata kuliah Matematika Diskrit semester ganjil Tahun 2023/2024 Jurusan Teknik Informatika, Institut Teknologi Bandung. Penulis juga mengucapkan terima kasih kepada dosen mata kuliah IF2120 Matematika Diskrit penulis yaitu Dr. Fariska Zakhralativa Ruskanda, S.T., M.T. yang telah membimbing penulis dalam menulis karya ilmiah ini. Penulis juga mengucapkan terima kasih kepada orang tua dan teman-teman penulis yang sudah mendukung penulis dalam menyelesaikan karya ilimiah ini.

# References

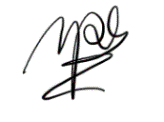
1. Dale Liu, Caceres, M., Robichaux, T., Forte, D. v., Seagren, E. S., Ganger, D. L., Smith, B., Jayawickrama, W., Stokes, C., & Jan Kanclirz, Jr. (2009). Chapter 3 - An Introduction To Cryptography. In Next Generation SSH2 Implementation.
2. <https://www.shiksha.com/online-courses/articles/types-of-cryptography/> diakses pada 10 desember 2023
3. H Mendel, F., Pramstaller, N., Rechberger, C., Rijmen, V. (2006). Analysis of Step-Reduced SHA-256. In: Robshaw, M. (eds) Fast Software Encryption. FSE 2006. Lecture Notes in Computer Science, vol 4047. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/11799313_9>
4. <https://informatika.stei.itb.ac.id/~rinaldi.munir//Matdis/2023-2024/14-Teori-Bilangan-Bagian1-2023.pdf> , diakses pada 10 Desember 2023
5. <https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/15-Teori-Bilangan-Bagian2-2023.pdf> , diakses pada 10 Desember 2023
6. <https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian3-2023.pdf> , diakses pada 10 Desember 2023
7. Ikbal, J. (2007). *An introduction to cryptography*. *Information Security Management Handbook, Sixth Edition*. <https://doi.org/10.2307/2695435>’
8. <https://www.encryptionconsulting.com/education-center/what-is-rsa/>
9. <https://stackoverflow.com/questions/53899931/why-does-an-empty-string-in-python-sometimes-take-up-49-bytes-and-sometimes-51> , diakses pada 10 Desember 2023
10. <https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=overview-digital-signature> , diakses pada 11 Desember 2023

# PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

`

Bandung, 11 Desember 2023



Marvel Pangondian, 13522075

# LAMPIRAN

Untuk uji coba dan pengembangan lebih lanjut, berikut adalah laman *github* penulis :