Analisis Penggunaan Algoritma RSA dalam Protokol TLS 1.2 pada Sertifikat Digital Website Resmi ITB untuk Menjamin Kemanan Transaksi Data Digital

Keisha Rizka Syofyani - 13524073
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: keishars2111@gmail.com , 13524073@std.stei.itb.ac.id

***Abstrak*—Keamanan komunikasi di era digital sangat krusial, terutama dalam menjaga kerahasiaan dan integritas data yang ditransmisikan melalui internet. Transport Layer Security (TLS), dengan algoritma RSA sebagai bagian dari mekanisme keamanannya, menjadi salah satu protokol kunci. Makalah ini menganalisis implementasi RSA dalam protokol TLS 1.2 pada sertifikat digital situs web resmi Institut Teknologi Bandung. Analisis dilakukan melalui inspeksi langsung struktur sertifikat menggunakan *browser* dan alat bantu seperti SSL Labs. Hasilnya menunjukkan bahwa RSA berfungsi sebagai algoritma kunci publik dan tanda tangan digital, dengan parameter kriptografi yang sesuai standar industri. Temuan ini menegaskan aplikasi konsep matematika diskrit, seperti eksponensial modular dan invers modulo, dalam sistem keamanan digital modern.**

Kata Kunci—RSA, TLS 1.2, Sertifikat Digital, HTTPS, Keamanan Data, Teori Bilangan, Matematika Diskrit

I. PENDAHULUAN

Dewasa ini, website merupakan salah satu platform utama yang digunakan dalam berbagai bidang, mulai dari kebutuhan individu, bisnis, hingga institusi pendidikan. Dalam penggunaannya, website sering kali memproses dan menyimpan data-data sensitif, baik berupa informasi pribadi pengguna maupun data internal milik institusi. Data tersebut merupakan aset penting yang harus dijaga kerahasiaannya, integritasnya, dan keasliannya. Di sisi lain, website juga rentan terhadap berbagai bentuk serangan siber yang dapat menyebabkan kebocoran data dan kerugian besar bagi pengguna maupun pengelola.

Untuk mengatasi ancaman tersebut, diperlukan mekanisme keamanan yang andal guna menjamin keamanan transaksi data yang berlangsung antara pengguna (klien) dan server. Salah satu protokol yang dirancang untuk tujuan ini adalah Transport Layer Security (TLS). TLS merupakan protokol keamanan yang berfungsi untuk mengamankan komunikasi data melalui jaringan internet, khususnya pada website. TLS melindungi data dengan cara mengenkripsi informasi yang dikirimkan antara klien dan server, menjaga integritas agar data tidak diubah selama transmisi, serta melakukan autentikasi guna memastikan bahwa data berasal dari sumber yang sah.

Dalam implementasinya, TLS menggunakan algoritma RSA (Rivest–Shamir–Adleman) sebagai bagian dari proses handshake awal. RSA berperan dalam melakukan pertukaran kunci secara aman antara klien dan server, sehingga memungkinkan keduanya menyepakati kunci sesi untuk enkripsi simetris. Selain itu, RSA juga digunakan dalam proses autentikasi melalui sertifikat digital yang menjamin identitas server. Dengan demikian, RSA menjadi elemen penting dalam menjamin kerahasiaan, integritas, dan keaslian komunikasi data pada protokol TLS.

Salah satu website yang paling sering digunakan oleh mahasiswa adalah website resmi institusi pendidikan, yang berfungsi sebagai pusat akses informasi akademik dan administrasi. Dalam makalah ini, penulis memilih website resmi Institut Teknologi Bandung (https://itb.ac.id) sebagai objek studi karena penulis merupakan mahasiswa aktif ITB yang secara langsung menggunakan layanan digital dari situs tersebut dalam kegiatan akademik sehari-hari. Penulis juga berharap bahwa melalui analisis ini, makalah ini dapat memberikan kontribusi nyata bagi peningkatan kesadaran dan kualitas keamanan digital di lingkungan kampus.

Pemilihan website ITB sebagai studi kasus juga didasari oleh posisinya sebagai institusi pendidikan tinggi ternama di Indonesia yang diharapkan menerapkan standar keamanan digital yang baik. Oleh karena itu, dalam penelitian ini, penulis bertujuan untuk menganalisis penggunaan algoritma RSA dalam protokol TLS 1.2 pada sertifikat digital website ITB, mengevaluasi struktur dan kekuatan kunci yang digunakan, serta menilai sejauh mana implementasi tersebut sesuai dengan standar keamanan informasi modern.

Topik yang diangkat dalam makalah ini juga memiliki keterkaitan erat dengan konsep-konsep dalam Matematika Diskrit. Algoritma RSA dibangun di atas dasar konsep teori bilangan, khususnya menggunakan prinsip bilangan prima besar, operasi modulo, dan invers modulo. Proses enkripsi dan dekripsi dalam RSA melibatkan fungsi eksponensial modular, yang menjadi bagian penting dalam cabang kriptografi berbasis teori bilangan. Selain itu, struktur sertifikat digital yang digunakan dalam protokol TLS 1.2 mengikuti sistem otentikasi yang memanfaatkan pasangan kunci publik dan privat sebuah aplikasi langsung dari logika formal, relasi, dan struktur

matematika yang juga dipelajari dalam Matematika Diskrit. Oleh karena itu, pembahasan dalam makalah ini tidak hanya relevan dalam konteks teknologi keamanan informasi, tetapi juga memperlihatkan penerapan nyata dari teori matematika diskrit dalam dunia siber modern.

Makalah ini bertujuan untuk mengkaji dan menganalisis penggunaan algoritma RSA dalam protokol TLS 1.2 pada website resmi Institut Teknologi Bandung (https://itb.ac.id), sebagai contoh penerapan konsep teori bilangan dalam Matematika Diskrit pada sistem keamanan digital. Penulisan ini difokuskan untuk:

1. Menjelaskan peran algoritma RSA dalam proses handshake dan autentikasi pada protokol TLS 1.2.
2. Menganalisis struktur sertifikat digital yang digunakan pada website itb.ac.id, khususnya dari aspek panjang kunci dan algoritma kriptografi.
3. Mengevaluasi tingkat keamanan penggunaan RSA berdasarkan prinsip-prinsip matematika diskrit, terutama teori bilangan.
4. Memberikan gambaran bagaimana implementasi RSA di dunia nyata mencerminkan penerapan langsung dari konsep-konsep dasar Matematika Diskrit.

II. LANDASAN TEORI

A. *Teori Bilangan dalam Kriptografi*

Teori bilangan (dalam bahasa Inggris: Number Theory) adalah cabang matematika murni yang mempelajari bilangan bulat (*integer*) atau fungsi bernilai bilangan bulat dan sifat-sifatnya. Bilangan bulat (*integer*) adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, -34, -1, dan 0. Dalam konteks Matematika Diskrit, teori bilangan memainkan peran penting dalam kriptografi modern, khususnya dalam algoritma RSA. Beberapa konsep penting dari teori bilangan yang digunakan dalam RSA antara lain adalah bilangan prima, operasi modulo, kekongruenan, dan invers modulo.

1) Bilangan Prima

Bilangan prima adalah bilangan bulat positif ppp yang lebih besar dari 1, dan hanya memiliki dua faktor pembagi, yaitu 1 dan ppp itu sendiri. Satu-satunya bilangan prima genap adalah 2, sedangkan bilangan prima lainnya selalu ganjil. Bilangan yang bukan prima disebut sebagai bilangan komposit.

Berdasarkan Teorema Dasar Aritmetika, setiap bilangan bulat positif $n \geq 2$ dapat dinyatakan sebagai hasil perkalian satu atau lebih bilangan prima, dan faktorisasi ini bersifat unik. Dalam algoritma RSA, digunakan dua bilangan prima besar untuk menghasilkan kunci publik dan kunci privat. Bilangan-bilangan ini harus cukup besar agar faktorisasi terhadap hasil perkalian keduanya (modulus n) menjadi sangat sulit, sehingga menjaga keamanan kriptografi.

2) Operasi Modulo dan Kekongruenan

a) Konsep Dasar Modulo

Operasi modulo adalah operasi yang mneyatakan sisa pembagian suatu bilangan a terhadap bilangan m (dengan $m \geq 0$). Dinyatakan sebagai:

$$\boldsymbol{a = mq + r, \qquad 0 \leq r \leq m}$$

Hasil operasi ditulis sebagai $\boldsymbol{a \bmod m = r}$. *Nilai r* disebut sebagai hasil sisa (remainder), dan m disebut modulus.

b) Kekongruenan Modulo

Dua bilangan bulat a dan b dikatakan kongruen modulo m, ditulis:

$$\boldsymbol{a \equiv b \pmod m}$$

jika dan hanya jika $m \mid (a - b)$, atau dengan kata lain, a dan b memiliki sisa pembagian yang sama terhadap m. Jika tidak kongruen, ditulis $\boldsymbol{a \not\equiv b \pmod m}$.

c) Sifat-sifat Kekongruenan Modulo

Jika $a \equiv b \pmod m$ dan $c \equiv d \pmod m$ maka berlaku:

- Penjumlahan: $(a + c) \equiv (b + c) \pmod m$
- Perkalian: $ac \equiv bc \pmod m$
- Perpangkatan: jika $a \equiv b \pmod m$, maka $a^k \equiv b^k \pmod m$ untuk setiap konstanta k.

Sifat-sifat ini sangat berguna dalam menyederhanakan perhitungan kriptografi berbasis modulo.

d) Invers Modulo

Syarat dari suatu bilangan bulat $a \pmod m$ memiliki invers adalah jika a dan m relatif prima dan $m > 1$.

Invers dari $a \pmod m$ adalah bilangan bulat x sedemikian sehingga:

$$xa \equiv 1 \pmod m$$

Invers modulo $\boldsymbol{a^{-1} \bmod m}$ hanya ada jika a dan m relatif prima, yaitu $gcd(a, m) = 1$. Invers ini digunakan dalam RSA untuk menghitung kunci privat dan kunci publik.

3) Teorema Fermat dan Teorema Euler

Dalam konteks kriptografi, dua teorema klasik dari teori bilangan memiliki peran penting dalam menjelaskan kenapa operasi eksponensial modulo dan invers modulo dapat dilakukan, yaitu Teorema Fermat dan Teorema Euler.

Teroema Fermat menyatakan bahwa jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi oleh p, maka:

$$\boldsymbol{a^{p-1} \equiv 1 \pmod p}$$

Teorema ini merupakan dasar dari perhitungan eksponensial modulo dalam kasus modulus prima, dan menjadi kasus khusus dari Teorema Euler.

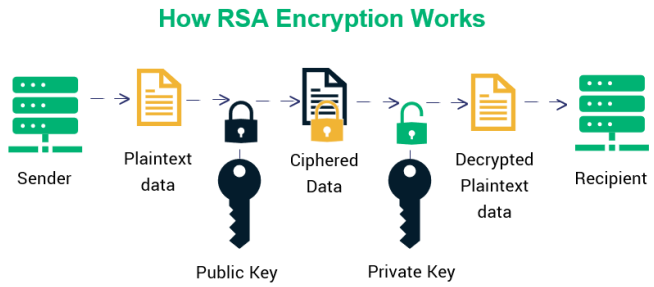
Teorema Euler memperluas prinsip tersebut untuk modulus n yang bukan bilangan prima. Jika a dan n adalah bilangan bulat positif yang relatif prima, maka:

$$\boldsymbol{a^{\varphi(n)} \equiv 1 \pmod n}$$

di mana $\varphi(n)$ adalah fungsi totien Euler, yaitu banyaknya bilangan kurang dari n yang relatif prima dengan n. Kedua

teorema ini menjadi dasar matematis dari keabsahan operasi kriptografi RSA.

B. *Algoritma RSA*



Gambar 1. Bagan Alur Kerja Algoritma RSA
(Sumber: Medium, https://sectigostore.com/blog/wp-content/uploads/2020/06/how-rsa-works.png)

Algoritma RSA dikembangkan pada tahun 1977 oleh tiga peneliti dari Massachusetts Institute of Technology, yaitu Ronald Rivest, Adi Shamir, dan Leonard Adleman. RSA merupakan algoritma kriptografi kunci publik yang memungkinkan proses enkripsi dan dekripsi dilakukan dengan pasangan kunci berbeda. Dalam RSA, setiap pengguna memiliki sepasang kunci, yaitu kunci publik dan kunci privat. **Kunci publik (*e*)** bersifat terbuka dan digunakan untuk mengenkripsi pesan, sedangkan **kunci privat (*d*)** bersifat rahasia dan digunakan untuk mendekripsi pesan yang telah dienkripsi.Prosedur Pembentukkan Kunci RSA.

1) *Prosedur Pembentukan Kunci RSA*

Langkah-langkah untuk membentuk pasangan kunci RSA adalah sebagai berikut.

a. Pilih dua bilangan prima, p dan q yang dirahasiakan.

b. Hitung nilai $n = pq$. Nilai ini menjadi bagian dari kunci publik dan tidak perlu dirahasiakan.

c. Hitung fungsi totien Euler yang nilainya dirahasiakan.

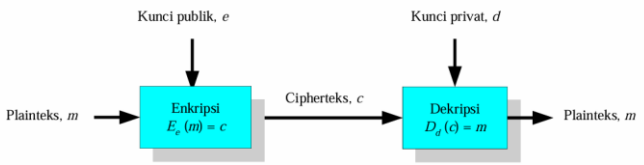
$$\varphi(n) = (p-1)(q-1),$$

d. Pilih sebuah kunci publik e sedemikian sehingga $1 < e < \varphi(n)$ yang relatif prima terhadap m, yaitu $gcd(e, \varphi(n)) = 1$.

e. Hitung nilai kunci dekripsi d melalui kekongruenan.

$$ed \equiv 1 \pmod{\varphi(n)}$$

2) *Prosedur Enkripsi-Dekripsi*



Gambar 2. Bagan Alur Prosedur Enkripsi-Dekripsi
(Sumber: Teori Bilangan (Bagian 3), https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/17-Teori-Bilangan-Bagian3-2024.pdf)

RSA menggunakan eksponensial modular dalam proses enkripsi dan dekripsi. Eksponensial modular adalah operasi perpangkatan dalam sistem modulo, yaitu:

- Enkripsi:

$$p^e \equiv c \pmod{n}$$

di mana p adalah *plaintext*, dan c adalah *ciphertext*.

- Dekripsi:

$$c^d \equiv p \pmod{n}$$

Proses ini mengembalikan pesan asli menggunakan kunci privat d.

3) *Contoh Sederhana RSA*

Misalkan dipilih dua bilangan prima kecil:

$$p = 5, q = 11$$

Maka:

$$n = p \cdot q = 5 \cdot 11 = 55$$

Kemudian hitung fungsi totien Euler:

$$\varphi(n) = (p-1)(q-1) = 4 \cdot 10 = 40$$

Selanjutnya pilih kunci publik e yang relatif prima terhadap 40, misalnya $e = 3$

Hitung nilai kunci privat d sedemikian sehingga:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$3 \cdot d \equiv 1 \pmod{40}$$

Sehingga didapatkan solusi terkecil untuk d yaitu $d = 27$, karena $3 \cdot 27 = 81 \equiv 1 \pmod{40}$

Dari algoritma RSA ini, didapatkan sebuah kunci publik $e = 3$, kunci privat $d = 27$ dengan $n = 55$.

- Proses Enkripsi
  Misal terdapat *plaintext* P = 9 yang akan dikonversikan menjadi *chipertext*, maka:
  $P^e \equiv C \pmod{n}$
  $9^3 \equiv C \pmod{55}$
  $C = 9^3 \bmod 55$
  Sehingga didapatkan *chipertext* C = 14.

- Proses Dekripsi
  $C^d \equiv P \pmod{n}$
  $14^{27} \equiv P \pmod{55}$
  $P = 14^{27} \bmod 55$
  $P = 9$
  Sehingga dekripsi berhasil mengembalikan pesan asli.

4) Keamanan RSA

Keamanan algoritma RSA bergantung pada kesulitan faktorisasi bilangan bulat besar, khususnya bilangan $n = p \cdot q$, di mana p dan q adalah bilangan prima besar. Ketika n sangat besar (misalnya 2048 bit), memfaktorkan n untuk memperoleh p dan q secara efisien dianggap sangat sulit dengan algoritma klasik saat ini sehingga pesan yang dienkripsi menjadi aman dari ancaman kebocoran.

Faktor -faktor yang memengaruhi kemana RSA:

a. Ukuran Modulus n

Semakin besar n, semakin sulit untuk difaktorkan. Saat ini, ukuran yang dianggap aman yaitu sekitar 2048 bit atau lebih.

b. Kerumitan Faktorisasi

Hingga saat ini belum ada algoritma yang dapat melakukan faktorisasi bilangan prima yang besar secara cepat.

c. Relasi dengan Teori Bilangan

Meskipun kunci publik (e, n) diketahui semua orang, kunci privat d hanya bisa dihitung jika $\varphi(n)$ diketahui, dan itu memerlukan p dan q.

Namun, jika di masa depan ditemukan algoritma faktorisasi cepat atau penggunaan komputer kuantum menjadi umum (misalnya dengan algoritma Shor), RSA dapat menjadi rentan. Oleh karena itu, saat ini sedang dikembangkan alternatif seperti *Elliptic Curve Cryptography* (ECC) dan *post-quantum cryptography* untuk mengantisipasi potensi ancaman tersebut.

C. Transport Layer Security (TLS) 1.2

1) Definisi dan Peran TLS

Transport Layer Security (TLS) adalah protokol keamanan kriptografi yang dirancang untuk melindungi data yang dikirimkan melalui jaringan, khususnya internet. TLS memastikan kerahasiaan, integritas, dan autentikasi data selama transmisi antara klien dan server. TLS merupakan penerus dari SSL (Secure Sockets Layer) dengan peningkatan fitur keamanan dan telah menjadi standar utama untuk mengamankan komunikasi di internet, terutama pada protokol HTTPS. TLS 1.2 merupakan versi TLS yang membawa banyak peningkatan dari versi sebelumnya yang lebih aman.

Fungsi utama TLS meliputi:

- Enkripsi, yaitu mengubah data menjadi bentuk terenkripsi yang tidak dapat dibaca oleh pihak yang tidak berwenang.
- Integritas data, dengan memastikan data tidak diubah atau dirusak selama proses pengiriman.
- Autentikasi, untuk memverifikasi identitas pihak yang berkomunikasi.

TLS berperan sebagai lapisan keamanan pada komunikasi web, terutama dalam protokol HTTPS. Dengan TLS, data yang dikirimkan antara browser dan web server dienkripsi sehingga menjaga privasi dan keamanan informasi sensitif seperti kredensial login, nomor kartu kredit, dan data pribadi lainnya. TLS juga menyediakan mekanisme handshake yang memungkinkan negosiasi algoritma enkripsi dan pertukaran kunci secara aman sebelum data aplikasi dikirimkan.

2) Arsitektur Umum TLS

Arsitektur TLS terdiri dari dua sub-protokol utama:

a) Handshake Protocol

Subprotokol ini bertugas membangun koneksi yang aman dengan melakukan negosiasi versi TLS, algoritma kriptografi, autentikasi server, dan pertukaran kunci sesi.

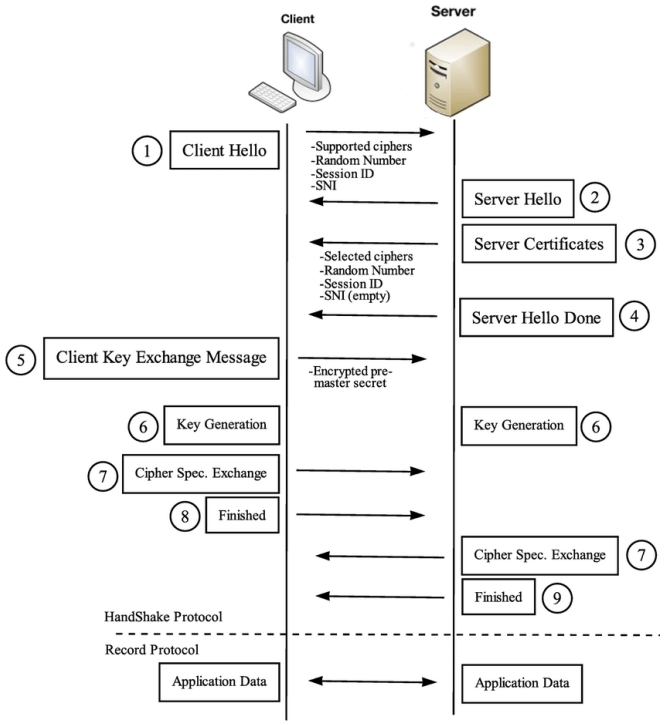
b) Record Protocol

Setelah koneksi aman terbentuk, subprotokol ini mengamankan data aplikasi dengan mengenkripsi dan memverifikasi integritas data menggunakan kunci sesi yang telah disepakati.

TLS juga menggunakan sertifikat digital yang diterbitkan oleh otoritas sertifikat (Certificate Authority/CA) untuk memverifikasi identitas server dan menjamin keaslian komunikasi.

3) Proses Handshake TLS 1.2

Proses handshake TLS 1.2 adalah serangkaian langkah yang dilakukan antara klien dan server untuk membangun koneksi aman. Proses ini memastikan bahwa data yang dikirimkan setelah handshake terlindungi dari penyadapan dan modifikasi oleh pihak ketiga. Berikut adalah tahapan utama dalam handshake TLS 1.2.



Gambar 3. Diagram Handshake TLS 1.2

(Sumber: ResearchGate, https://images.app.goo.gl/pcaLh7PGksz8NydMA)

1. **Client Hello**: Klien mengirim pesan awal yang berisi versi TLS yang didukung, daftar algoritma kriptografi yang didukung, metode kompresi, dan bilangan acak (client random).
2. **Server Hello**: Server membalas dengan versi TLS yang dipilih, algoritma kriptografi yang disetujui, server random, dan sertifikat digital yang berisi kunci publik.
3. **Authentication**: Klien memverifikasi sertifikat digital server dengan otoritas sertifikat untuk memastikan keasliannya.
4. **Premaster Secret**: Klien menghasilkan premaster secret, sebuah nilai acak yang dienkripsi menggunakan kunci publik RSA milik server, lalu dikirim ke server.
5. **Decrypt Premaster**: Server mendekripsi premaster secret menggunakan kunci privat RSA miliknya.
6. **Generate Session Key**: Baik klien maupun server menggunakan premaster secret, client random, dan server random untuk menghasilkan kunci sesi simetris.
7. **Client Finished**: Klien mengirim pesan "finished" yang dienkripsi dengan kunci sesi sebagai bukti bahwa handshake selesai.
8. **Server Finished**: Server mengirim pesan "finished" yang juga dienkripsi dengan kunci sesi.
9. **Secure Connection Established**: Setelah verifikasi berhasil, koneksi aman terbentuk, dan semua komunikasi berikutnya akan dienkripsi dengan kunci sesi tersebut.

D. Sertifikat Digital dan Struktur X.509

1) Definisi dan Fungsi Sertifikat Digital

Sertifikat digital adalah dokumen elektronik yang mengikat identitas pemilik (individu, organisasi, atau perangkat) dengan kunci publik melalui tanda tangan digital dari otoritas sertifikat (CA). Sertifikat ini menjamin bahwa kunci publik memang dimiliki oleh entitas yang tercantum dalam sertifikat.

Fungsi utama sertifikat digital:

- Melakukan autentikasi terhadap identitas pemilik.
- Menyediakan kunci publik untuk proses enkripsi data.
- Menjamin integritas dan nonrepudiasi pesan digital.

2) Struktur Sertifikat X.509

Sertifikat X.509 adalah standar internasional untuk format sertifikat digital yang banyak digunakan pada protokol keamanan seperti SSL/TLS. Struktur utama X.509 meliputi:

- **Versi**: Menunjukkan versi dari format sertifikat.
- **Seri**: Nomor unik sebagai identitas sertifikat.
- **Algoritma Tanda Tangan**: Algoritma yang digunakan untuk menandatangani sertifikat (contoh: SHA256withRSA).
- **Issuer**: Identitas otoritas penerbit (Certificate Authority).
- **Validity**: Periode berlakunya sertifikat.
- **Subject**: Identitas entitas pemilik sertifikat (misalnya domain website).
- **Subject Public Key Info**: Informasi mengenai kunci publik milik pemilik sertifikat.
- **Signature**: Tanda tangan digital dari penerbit, yang digunakan untuk memverifikasi keabsahan sertifikat.

3) Algoritma Tanda Tangan Digital

Algoritma tanda tangan digital digunakan untuk menjamin autentikasi dan integritas dokumen digital. Tanda tangan digital juga mencegah pengirim menyangkal telah mengirimkan pesan (nonrepudiasi). Algoritma yang umum digunakan meliputi RSA, DSA, dan ECDSA.

Proses tanda tangan digital:

1. Pesan di-hash menggunakan fungsi hash kriptografi (misal: SHA-256).
2. Hash tersebut dienkripsi dengan kunci privat pengirim, menghasilkan tanda tangan digital.
3. Penerima mendekripsi tanda tangan dengan kunci publik pengirim dan membandingkannya dengan hash pesan yang diterimanya.
4. Jika hasilnya sama, pesan dianggap autentik dan tidak dimodifikasi.

4) Hubungan RSA dengan Sertifikat

RSA digunakan secara langsung dalam sertifikat digital untuk dua tujuan utama:

a. RSA digunakan sebagai algoritma tanda tangan digital, yaitu oleh Certificate Authority (CA) untuk menandatangani sertifikat X.509.
b. RSA juga digunakan dalam proses autentikasi dan pengiriman premaster secret pada protokol TLS 1.2, dengan cara mengenkripsi nilai tersebut menggunakan kunci publik RSA yang terdapat di dalam sertifikat digital server.

Dengan demikian, RSA berperan penting dalam menjamin keamanan komunikasi antara klien dan server melalui validasi identitas dan penyandian data awal.

III. IMPLEMETASI

A. Tujuan Implementasi

Adapun tujuan dari implementasi yang dilakukan adalah untuk menganalisis penerapan RSA dalam protokol TLS 1.2 pada sertifikat website resmi Institut Teknologi Bandung (https://itb.ac.id) guna mengkaji prinsip yang digunakan sebagai penerapan teori bilangan.

B. Metode Pengumpulan Data

Untuk memperoleh data mengenai penerapan algoritma RSA dalam protokol TLS 1.2 pada website resmi Institut Teknologi Bandung (https://itb.ac.id), penulis melakukan inspeksi terhadap sertifikat digital yang digunakan oleh situs tersebut. Pengumpulan data dilakukan melalui dua metode utama, yakni:

1) Fitur Browser

Penulis menggunakan fitur inspeksi sertifikat yang tersedia pada browser Google Chrome. Dengan mengakses situs https://itb.ac.id, kemudian mengeklik ikon gembok di address bar, penulis membuka informasi detail sertifikat digital yang ditampilkan oleh browser. Informasi yang diamati mencakup algoritma kunci publik, panjang kunci, algoritma tanda tangan digital, serta periode validitas sertifikat.

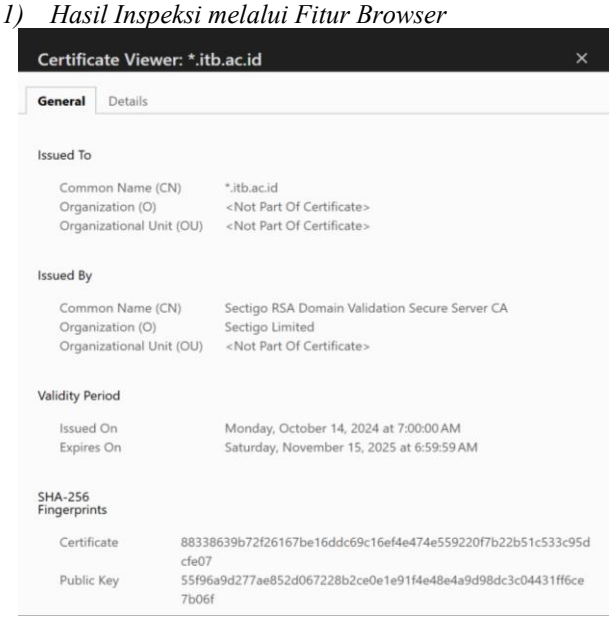
2) Tools

Selain melalui browser, penulis juga memverifikasi informasi sertifikat menggunakan layanan SSL Labs Server Test dari Qualys (https://www.ssllabs.com/ssltest/). Dengan memasukkan domain itb.ac.id, layanan ini menyajikan laporan detail mengenai konfigurasi keamanan TLS pada server, termasuk versi protokol, algoritma kriptografi yang digunakan, dan struktur sertifikat digital.

Data yang diperoleh dari kedua metode ini digunakan untuk dianalisis berdasarkan teori bilangan dan prinsip kriptografi yang telah dijelaskan pada bagian sebelumnya.

C. Hasil Inspeksi Sertifikat Website ITB

1) Hasil Inspeksi melalui Fitur Browser



Gambar 3. Tampilan Layar Hasil Inspeksi Website ITB melalui Browser

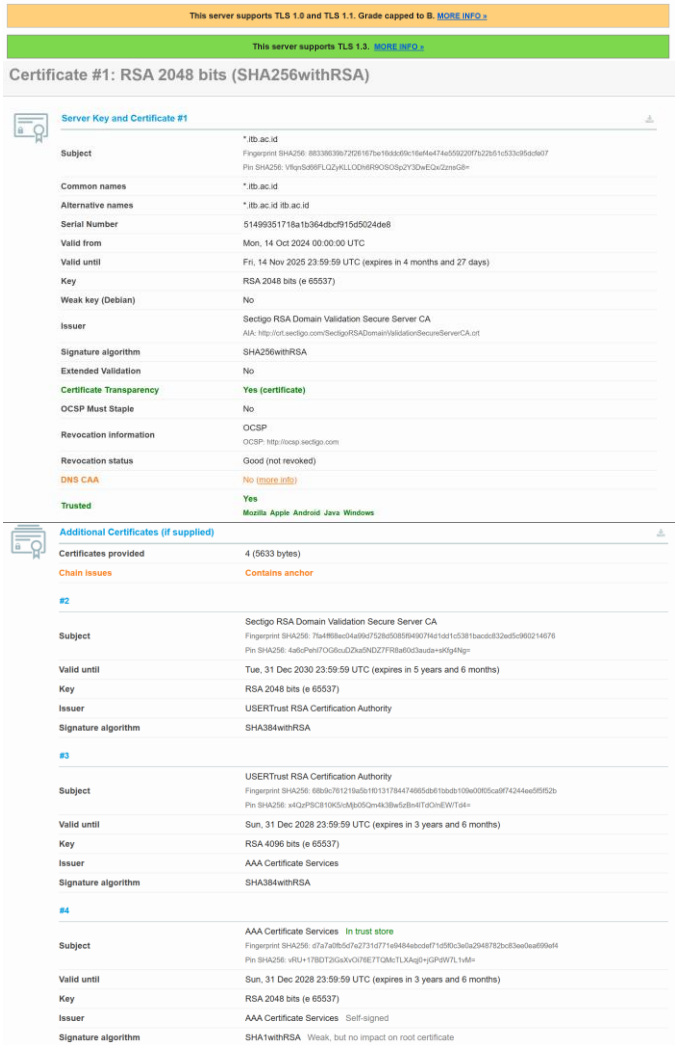
Tabel 1. Informasi Sertifikat Digital Website itb.ac.id (Hasil Inspeksi Browser)

No.	Elemen Sertifikat	Nilai
1	Domain	itb.ac.id
2	Issued By	Sectigo RSA Domain Validation Secure Server CA
3	Valid From-To	14 Okt 2024 – 15 Nov 2025
4	Public Key Algorithm	RSA
5	Key Size	2048 bit
6	Public Exponent	65537 (01 00 01)
7	Signature Algorithm	SHA256withRSA

Berdasarkan inspeksi menggunakan fitur bawaan pada browser Google Chrome terhadap situs https://itb.ac.id, diperoleh informasi sebagai berikut.

1. Sertifikat digital dikeluarkan untuk domain itb.ac.id oleh Certificate Authority (CA) bernama Sectigo RSA Domain Validation Secure Server CA.
2. Masa berlaku sertifikat dimulai pada tanggal 14 Oktober 2024 pukul 07.00 dan berakhir pada 15 November 2025 pukul 06.59.
3. Algoritma kunci publik yang digunakan adalah RSA dengan ukuran modulus sebesar 2048 bit, serta eksponen publik bernilai 65537 (ditampilkan dalam bentuk heksadesimal sebagai 01 00 01), yang merupakan nilai umum dalam implementasi RSA.
4. Algoritma tanda tangan digital yang digunakan adalah SHA-256 with RSA Encryption (PKCS #1 v1.5). Kombinasi informasi ini menunjukkan bahwa server menggunakan RSA sebagai skema kriptografi asimetris baik untuk menyediakan kunci publik kepada klien, maupun untuk memverifikasi keabsahan sertifikat digital yang ditandatangani oleh CA.

2) Hasil Inspeksi melalui Tools SSL Labs



Gambar 4. Tampilan Layar Hasil Inspeksi Website ITB menggunakan SSL Labs

Tabel 2. Informasi Keamanan TLS Website itb.ac.id (Hasil Inspeksi SSL Labs)

No.	Elemen Sertifikat	Nilai
1	TLS Version Supported	TLS 1.0, 1.1, 1.3 (indikasi TLS 1.2 masih digunakan)
2	Key Exchange	RSA
3	Chiper Suite	SHA256withRSA
4	Issuer	USERTrust RSA Certification Authority
5	Signature Algorithm	SHA384withRSA
6	Key Size	2048 bit
7	Trust Status	Trusted

Selain melalui browser, verifikasi tambahan dilakukan menggunakan layanan *SSL Labs Server Test* oleh Qualys. Informasi yang diperoleh dari hasil inspeksi tambahan ini adalah sebagai berikut:

1. Meskipun pada laporan awal tidak secara eksplisit disebutkan dukungan terhadap TLS 1.2, hasil analisis menunjukkan bahwa server itb.ac.id mendukung beberapa versi TLS, termasuk TLS 1.0, 1.1, dan 1.3. Namun, berdasarkan keberadaan RSA key exchange dan algoritma tanda tangan SHA256withRSA, dapat disimpulkan bahwa server masih mengimplementasikan TLS versi 1.2, yang merupakan fokus utama dalam analisis ini.
2. Proses pertukaran kunci dilakukan menggunakan algoritma RSA, dengan dukungan cipher suite SHA256withRSA.
3. Informasi sertifikat tambahan menunjukkan bahwa sertifikat diterbitkan oleh USERTrust RSA Certification Authority, menggunakan algoritma tanda tangan SHA384withRSA, dan ukuran kunci publik sebesar 2048 bit.
4. Hasil uji juga menunjukkan bahwa sertifikat tersebut diakui sebagai valid dan terpercaya oleh mayoritas browser modern.

D. Analisis Implementasi RSA Berdasarkan Sertifikat Website ITB

Berdasarkan hasil inspeksi yang telah dilakukan sebelumnya terhadap sertifikat digital website https://itb.ac.id, dapat dilihat bahwa algoritma RSA digunakan secara langsung dalam struktur sertifikat tersebut. Hal ini terlihat dari penggunaan RSA sebagai algoritma kunci publik, di mana nilai modulus sepanjang 2048 bit dan eksponen publik sebesar 65537 (dalam heksadesimal: 01 00 01) digunakan. Konfigurasi ini adalah konfigurasi umum dalam implementasi RSA karena memberikan keamanan yang cukup kuat sekaligus efisiensi dalam proses enkripsi.

RSA juga muncul sebagai algoritma tanda tangan digital (signature algorithm) yang digunakan untuk memverifikasi keabsahan sertifikat, yaitu SHA256withRSA atau SHA384withRSA. Dalam hal ini, otoritas sertifikat (Certificate Authority/CA) menandatangani sertifikat dengan menggunakan kunci privat RSA-nya, lalu klien (misalnya browser) akan melakukan verifikasi menggunakan kunci publik dari CA tersebut. Proses ini memastikan bahwa sertifikat memang diterbitkan oleh lembaga yang sah dan tidak dimodifikasi.

Secara matematis, RSA menggunakan konsep dasar eksponensial modular, yaitu operasi seperti $C = M^e \bmod n$ untuk proses enkripsi dan $M = C^d \bmod n$ untuk dekripsi. Nilai-nilai seperti bilangan prima besar, modulus n, dan eksponen e serta d semuanya berakar dari konsep teori bilangan. Dengan demikian, struktur sertifikat digital ini bisa menjadi contoh nyata dari bagaimana teori matematika diskrit digunakan secara langsung dalam sistem keamanan digital.

E. Analisis Fungsi RSA dalam Protokol TLS 1.2

Dalam protokol *Transport Layer Security* (TLS) versi 1.2, algoritma *RSA* tidak hanya digunakan dalam struktur sertifikat, tapi juga berperan penting dalam proses yang disebut sebagai *handshake*. Proses *handshake* ini terjadi di awal ketika klien (misalnya browser) dan server (dalam hal ini website *itb.ac.id*) ingin membangun koneksi yang aman. Pada tahap ini, dibutuhkan cara agar kedua pihak bisa menyepakati kunci rahasia bersama tanpa harus mengirimkan kunci itu secara langsung dalam bentuk terbuka.

Di sinilah *RSA* digunakan. Klien akan membuat nilai acak yang disebut *premaster secret*, lalu mengenkripsinya menggunakan kunci publik RSA yang diperoleh dari sertifikat digital server. Setelah itu, *premaster secret* yang sudah terenkripsi dikirimkan ke server. Karena hanya server yang memiliki kunci privat RSA yang sesuai, maka hanya server yang dapat mendekripsi nilai tersebut dan mengetahui *premaster secret* yang asli.

Selanjutnya, baik klien maupun server akan menggunakan *premaster secret* tersebut untuk menghasilkan *session key*—kunci sesi simetris yang digunakan untuk mengenkripsi seluruh komunikasi selama koneksi berlangsung. Artinya, *RSA* dalam TLS 1.2 dipakai khusus di awal untuk pertukaran kunci secara aman, sementara enkripsi data setelahnya dilakukan dengan algoritma simetris yang lebih efisien secara komputasi.

Proses ini memperlihatkan bagaimana *RSA* menjadi bagian penting dalam menjamin bahwa proses pertukaran kunci tidak bisa disadap oleh pihak ketiga. Di sinilah teori *eksponensial modular* dari matematika diskrit benar-benar digunakan dalam praktik dunia nyata.

F. Evaluasi Keamanan RSA pada Website ITB

Dari hasil inspeksi dan analisis yang telah dilakukan, dapat disimpulkan bahwa penggunaan algoritma *RSA* pada website resmi *Institut Teknologi Bandung* telah sesuai dengan standar keamanan digital modern. Kunci RSA yang digunakan memiliki panjang *modulus* sebesar 2048 bit, yang saat ini masih dianggap cukup kuat untuk melindungi data dari serangan faktorisasi dengan komputer konvensional. Selain itu, nilai *eksponen publik* 65537 merupakan nilai standar yang banyak digunakan karena seimbang antara keamanan dan efisiensi.

Penggunaan algoritma tanda tangan digital seperti *SHA256withRSA* dan *SHA384withRSA* juga memperkuat

integritas dan keaslian sertifikat yang digunakan oleh website ITB. Sertifikat ini diterbitkan oleh *Certificate Authority* yang terpercaya dan masih berada dalam masa berlaku, sehingga komunikasi yang dilakukan melalui situs tersebut dapat dianggap aman oleh mayoritas peramban.

Namun, penting juga untuk menyadari bahwa keamanan algoritma *RSA* sangat bergantung pada kesulitan faktorisasi bilangan bulat besar. Jika suatu saat ditemukan algoritma faktorisasi yang jauh lebih cepat—terutama oleh komputer kuantum—maka kekuatan RSA bisa melemah. Untuk itu, banyak pengembang sistem keamanan mulai mempertimbangkan migrasi ke algoritma yang disebut sebagai *post-quantum cryptography*.

Meski demikian, hingga saat ini *RSA* masih menjadi salah satu algoritma kriptografi yang paling banyak digunakan dan terbukti andal. Implementasi yang ditemukan di website ITB menunjukkan bahwa prinsip-prinsip dalam matematika diskrit, khususnya teori bilangan, telah diterapkan secara nyata untuk menjamin keamanan data di dunia digital.

IV. KESIMPULAN

Melalui penulisan makalah ini, penulis mencoba melihat lebih dekat bagaimana konsep-konsep dalam matematika diskrit, khususnya teori bilangan, digunakan secara nyata dalam sistem keamanan digital modern. Salah satu contohnya adalah algoritma *RSA*, yang menjadi bagian penting dalam protokol *Transport Layer Security* (TLS) 1.2 yang digunakan untuk mengamankan komunikasi di website https://itb.ac.id.

Berdasarkan hasil inspeksi sertifikat digital dan analisis yang dilakukan, terbukti bahwa algoritma *RSA* digunakan pada dua bagian penting, yaitu sebagai algoritma kunci publik dalam sertifikat digital dan sebagai metode pertukaran kunci pada saat proses *handshake* TLS berlangsung. Kunci RSA dengan panjang 2048 bit dan eksponen publik standar sebesar 65537 menunjukkan bahwa sistem ini telah mengikuti standar keamanan yang umum digunakan. Selain itu, algoritma tanda tangan digital yang digunakan juga memperkuat integritas dan keaslian dari sertifikat tersebut.

Keseluruhan proses ini melibatkan prinsip-prinsip penting dalam teori bilangan seperti bilangan prima, *modulus*, *invers modulo*, serta *eksponensial modular*, yang menjadi dasar dari sistem kriptografi RSA. Hal ini menunjukkan bahwa teori-teori matematika yang dipelajari di bangku kuliah bukan hanya bersifat abstrak, tetapi benar-benar diterapkan dalam kehidupan sehari-hari, terutama dalam hal perlindungan data dan komunikasi digital.

Dengan memilih website ITB sebagai studi kasus, penulis berharap makalah ini dapat memberikan kontribusi kecil dalam meningkatkan kesadaran akan pentingnya keamanan data digital, sekaligus menunjukkan bagaimana teori matematika diskrit dapat diaplikasikan secara konkret dalam bidang teknologi informasi.

LAMPIRAN DIGITAL

Berikut adalah tautan yang berkaitan dengan makalah ini, berupa video penjelasan di YouTube serta salinan file presentasi dalam format PPT.

- Video YouTube: https://youtu.be/kH0MxHNO4Co
- File PPT Presentasi: https://www.canva.com/design/DAGqw8WNuwI/nZzOr2JyecBOGOm4TLwMlg/edit?utm_content=DAGqw8WNuwI&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, sehingga makalah yang berjudul “Analisis Penggunaan Algoritma RSA dalam Protokol TLS 1.2 pada Website Resmi Institut Teknologi Bandung untuk Menjamin Keamanan Transaksi Data Digital” dapat terselesaikan dengan baik.

Penulis mengucapkan terima kasih sebesar-besarnya kepada Bapak Dr. Ir. Rinaldi Munir, M.T., selaku dosen pengampu mata kuliah Matematika Diskrit kelas K-1, atas bimbingan dan materi perkuliahan yang telah diberikan. Materi tersebut sangat membantu penulis dalam memahami konsep-konsep penting yang menjadi dasar penulisan makalah ini sebagai salah satu bentuk penerapan dari pemahaman yang telah diperoleh selama perkuliahan.

Ucapan terima kasih juga penulis sampaikan kepada teman-teman kelas K-1 IF yang telah menjadi rekan belajar dan tempat berdiskusi selama menjalani semester ini. Tak lupa, penulis berterima kasih kepada para penulis buku, jurnal, dan makalah yang telah menjadi referensi utama dalam penyusunan makalah ini.

REFERENSI

[1] W. A, Gunawan dan M. Idris, “Kajian Fungsi Totient Euler,” dalam *Prosiding Seminar Nasional Matematika, Statistika, dan Aplikasinya 2023*, Samarinda, Indonesia, Agustus 2023, hal. 68-79.

[2] R. A. Putra, “Simulasi TLS Handshake dengan Menggunakan Algoritma RSA,” makalah tidak diterbitkan, Institut Teknologi Bandung, 2021.

[3] A. H. Suliman, “Analisis Keamanan Protokol Kriptografi SSL/TLS dengan Algoritma ECC pada Layanan Transaksi Online pada E-Commerce, ” makalah tidak diterbitkan, Institut Teknologi Bandung, 2023.

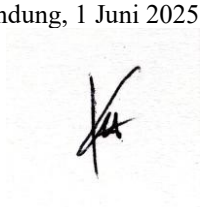
[4] N. G. Subrata, “Application of RSA Cryptosystem and Linear Congruential Generator to Enhance Security in JSON Web Tokens for Storing User's Credentials,” makalah tidak diterbitkan, Institut Teknologi Bandung, 2025.

[5] A. G. A. Ghifari, “Inovasi Keuangan Digital dengan Teori Bilangan dan Kriptografi, ” makalah tidak diterbitkan, Institut Teknologi Bandung, 2025.
[6] D. H. P. Dewa, “Analisis Mekanisme Keamanan antara TLS/SSL dan Crypto pada Komunikasi IOT Middleware dengan Subscriber Berbasis Protokol HTTP,” Skripsi, Universitas Brawijaya, Malang, 2018.
[7] M. Rinaldi, “Teori Bilangan (Bagian 1),” https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/15-Teori-Bilangan-Bagian1-2024.pdf, 2025, diakses pada 17 Juni 2025.
[8] M. Rinaldi, “Teori Bilangan (Bagian 2),” https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/16-Teori-Bilangan-Bagian2-2024.pdf, 2025, diakses pada 17 Juni 2025.
[9] M. Rinaldi, “Teori Bilangan (Bagian 3),” https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2024-2025/17-Teori-Bilangan-Bagian3-2024.pdf, 2025, diakses pada 17 Juni 2025.
[10] P. Rahmadiyanto, “Mengenal Algoritma RSA secara Sederhana, ” Medium, Diakses pada 18 Juni 2025. [Online]. Tersedia: https://medium.com/@puji.rahmadiyanto/mengenal-algoritma-rsa-secara-sederhana-40fdb96e0acc
[11] “GnuTLS Manual,” GnuTLS.org, Diakses pada 18 Juni 2025. [Online]. Tersedia: https://www.gnutls.org/manual/html_node/index.html#SEC_Contents
[12] A. J. Menezes, P. C. van Oorschot, dan S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. [Online]. Tersedia: https://cacr.uwaterloo.ca/hac/
[13] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, dan W. Polk, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” RFC 5280, Internet Engineering Task Force (IETF), May 2008. [Online]. Tersedia: https://datatracker.ietf.org/doc/html/rfc5280

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, 1 Juni 2025



Keisha Rizka Syofyani - 13524073