Aplikasi Teori Bilangan dalam Pengamanan Transmisi Data pada Aplikasi Perpesanan

Rahmat Rafid Akbar - 13520090[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13520090@itb.ac.id

***Abstract*—Perkembangan teknologi telah mengubah tingkah laku dan kebiasaan hidup manusia. Saat ini, komunikasi dapat dilakukan dengan mudah tanpa batasan ruang maupun waktu. Hal ini dapat dilakukan dengan menggunakan perangkat elektronik yang mumpuni seperti *handphone* atau *computer* yang memanfaatkan fitur-fitur serta aplikasi yang tersedia. Pertukaran informasi dilakukan dengan menggunakan aplikasi perpesanan seperti *WhatsApp, Telegram, Signal,* dan *e-mail*. Namun, hal ini tentu rentan terhadap kebocoran data maupun penyadapan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, dibutuhkan pengamanan pada data sebelum ditransmisikan dengan menggunakan teknik kriptografi yang menerapkan konsep teori bilangan. Salah satu metode kriptografi yang populer digunakan adalah algoritma RSA (Rivest–Shamir–Adleman) yang menggunakan kunci publik dan kunci privat dalam proses enkripsi dan dekripsi data (pesan).**

***Keywords*—Kriptografi, Transmisi, Data, Teori Bilangan, Enkripsi, Dekripsi, Aplikasi Perpesanan, WhatsApp, Telegram, Signal.**

I. Latar Belakang

Komunikasi merupakan salah satu aktivitas yang paling sering dilakukan oleh manusia karena sejatinya manusia sebagai makhluk sosial tidak bisa hidup sendiri dan membutuhkan bantuan serta keberadaan orang lain. Untuk berinteraksi dengan orang lain tentu kita akan melakukan komunikasi baik dalam bentuk visual, lisan maupun tindakan. Komunikasi yang awalnya dilakukan secara primitif seperti menggunakan ukiran pada batu dan kayu perlahan-lahan berubah mengikuti perkembangan zaman, mulai dari menggunakan media cetak yang menggunakan kertas untuk surat-menyurat hingga menggunakan media elektronik yang memanfaatkan jaringan dalam melakukan pertukaran informasi.

Dewasa ini, teknologi yang semakin canggih dapat memudahkan manusia dalam berinteraksi dan berkomunikasi melalui perangkat seluler yang dapat digunakan dimana saja dan kapan saja. Komunikasi dapat dilakukan menggunakan aplikasi perpesanan yang ada seperti *WhatsApp, Telegram, dan Signal* ataupun menggunakan sistem surat-menyurat melalui jaringan komputer secara elektronik yang dinamakan E-mail (*Electronic Mail*). Namun, seiring berkembangnya teknologi, semakin canggih dan cerdik pula para kriminal dalam melakukan tindak kejahatan yang dapat merugikan orang lain, salah satunya kejahatan pada bidang komunikasi dan informasi. Ketika seseorang ingin melakukan pertukaran informasi, tentu dikehendaki bahwa informasi yang dikirimkan dapat sampai kepada penerima dengan aman dan tanpa adanya kebocoran dari informasi tersebut ke pihak lain. Sehingga dibutuhkan cara untuk mengamankan data (informasi) yang akan dikirimkan agar dapat mencegah terjadinya kejadian yang tidak diinginkan.

Oleh karena itu, para cendekiawan dunia selama berabad-abad mencari dan mengembangkan metode yang dapat digunakan dalam pengamanan data pada saat ditransmisikan. Setelah penelitian yang panjang, ditemukanlah metode manipulasi (pengkodean) pada data yang dinamakan dengan teknik Kriptografi. Teknik ini memanfaatkan salah satu cabang matematika yang bernama konsep Teori Bilangan. Pada makalah ini, penulis akan mengulas bagaimana penerapan Teori Bilangan dalam teknik Kriptografi terhadap pengamanan data pada aplikasi perpesanan.

II. Teori Dasar

A. Teori Bilangan

1. Bilangan dan Teori Bilangan

Terdapat berbagai jenis bilangan yang dipelajari di cabang ilmu Matematika. Jenis-jenis bilangan tersebut meliputi :

- Bilangan Asli (N), yaitu bilangan yang dimulai dari 1 ke atas {1, 2, 3, 4, 5, 6, 7, …}.
- Bilangan Cacah, yaitu bilangan asli yang juga meliputi angka 0 : {0, 1, 2, 3, 4, 5, 6, 7, …}.
- Bilangan Bulat (Z), yaitu bilangan cacah yang ditambahkan dengan bilangan negatif : {-4, -3, -2, -1 , 0, 1, 2, 3, 4,…}.
- Bilangan Prima (P), yaitu bilangan bulat yang hanya habis dibagi 1 dan bilangan itu sendiri : {2, 3, 5, 7, 11, 13, 17, …..}.
- Bilangan Pecahan, yaitu bilangan yang dapat dinyatakan dalam bentuk pecahan a/b : {1/2, 3/4, 5/6, 7/8, …}
- Bilangan Rasional, yaitu bilangan yang meliputi bilangan Bulat dan Pecahan.
- Bilangan Irasional, yaitu bilangan yang tidak dapat

dinyatakan dalam bentuk pecahan a/b : {√2, √3, dan bilangan irasional lainnya}

- Bilangan Riil (R), yaitu bilangan yang meliputi bilangan rasional dan irasional
- Bilangan Imajiner, yaitu bilangan yang meliputi i di mana i2 = -1, contoh √−1, √−2
- Bilangan Kompleks, yaitu bilangan yang meliputi bilangan Riil dan Imajiner.

Teori bilangan sendiri adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (integer) beserta dengan fungsi-fungsi yang berkaitan dengan bilangan tersebut.

2. Sifat Pembagian pada Bilangan Bulat

Pembagi atau faktor dari sebuah bilangan bulat adalah bilangan yang memenuhi teorema berikut:

Teorema 1.

Jika terdapat $a, b \in Z$ dan $a \neq 0$, maka dikatakan bahwa a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga : $b = a \,.\, c$. Sifat pembagian a habis membagi b dapat ditulis dalam bentuk $a \mid b$.

Contoh : 2 habis membagi 8 karena terdapat sebuah bilangan $c = 4$ sehingga $8 = 2 \,.\, 4$ atau $2 \mid 8$.

Pada sifat pembagian, hanya bilangan bulat positif yang diperhitungkan sebagai faktor (pembagi) dari sebuah bilangan. Walaupun pada kenyataannya bilangan negatif dapat memenuhi teorema tersebut dan merupakan pembagi.

3. Teorema Euclidean pada Bilangan Bulat

Gambar 2.1. Lukisan Euclides
Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf

Euclides adalah seorang matematikawan yunani yang berasal dari Aleksandria, Mesir. Ia juga dikenal sebagai Bapak Geometri karena beberapa penemuannya. Ia juga mengusungkan Teorema dan Algoritma yang sangat membantu dalam konsep teori bilangan dan dituliskan dalam bukunya, *Element.*

Teorema 2. (Teorema Euclidian 1)

Jika terdapat $m, n \in Z$ dan $n > 0$, maka pembagian m/n akan memberikan hasil bagi q $(quotient)$ dengan sisa r $(remainder)$ sedemikian sehingga

$$m = nq + r$$

dengan syarat,

$$0 \leq r < n.$$

Contoh : $13/7$ dapat disajikan di dalam bentuk,

$$\frac{13}{7} \equiv\gg 13 = 7 \,.\, 1 + 6$$

sehingga dapat terlihat bahwa hasil baginya $(quotient)$ adalah 1 dan sisanya $(remainder)$ adalah 6.

Note :

Pada bilangan negatif, perlu diingat bahwa $0 \leq r < n$, sehingga jika $-13/7$ harus disajikan sebagai

$$-\frac{13}{7} \equiv\gg -13 = 7 \,.\, (-2) + 1$$

yang berarti memberikan hasil baginya adalah -2 dan sisa baginya adalah 1.

4. Pembagi Bersama Terbesar (PPB) / Greatest Common Divisor (gcd)

Teorema 3.

Jika terdapat $a,\ b,\ c \in Z$, maka c dikatakan sebagai pembagi bersama terbesar (gcd) dari a dan b, jika c adalah bilangan bulat terbesar sehingga c habis membagi a dan c habis membagi b atau dapat ditulis,

$$PBB(a, b) = c \quad \text{atau} \quad \gcd(a, b) = c$$

dengan syarat,

$$c \mid a \ \text{ dan } \ c \mid b$$

Contoh, $PBB(8,12) = 4$ karena 4 merupakan bilangan bulat terbesar yang memenuhi 4 | 8 dan 4 | 12.

Teorema 4. (Teorema Euclidean 2)

Jika terdapat $m, n \in Z$ dan $n > 0$, sedemikian sehingga

$$m = nq + r$$

dengan,

$$0 \leq r < n$$

maka dapat dipastikan,

$$PBB(m, n) = PBB(n, r)$$

Algoritma Euclidean (Mencari PBB)

Misalkan terdapat $m, n \in Z^+$ dan $m \geq n$ maka pembagi bersama terbesar dari dua bilangan tersebut dapat dicari dengan memanfaatkan **Teorema 2.** dan **Teorema 4.** dengan algoritma berikut :

1. Jika n = 0 maka m adalah PBB(m,n); stop.
   Tetapi, jika n ≠ 0 maka lanjutkan ke langkah 2.

2. Bagilah m dengan n dan menghasilkan sisa r.
3. Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulangi kembali ke langkah 1.

Berikut ilustrasinya, $r_0 = m$ dan $r_1 = n$:

$$\begin{aligned} r_0 &= r_1 . q_1 + r_2 \quad , \quad 0 \le r_2 < r_1 \\ r_1 &= r_2 . q_2 + r_3 \quad , \quad 0 \le r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} . q_{n-1} + r_n \quad , \quad 0 \le r_n < r_{n-1} \\ r_{n-1} &= r_n . q_n + 0 \end{aligned}$$

Didapatkan :

$$\boldsymbol{PBB(m,n)} = PBB(r_0, r_1) = PBB(r_1, r_2) = \cdots$$
$$PBB(r_{n-1}, r_n) = PBB(r_n, 0) = \boldsymbol{r_n}$$

Contoh : Akan dicari $PBB(55,15)$. Berdasarkan algoritma euclidian :

$$55 = 15 . 3 + 10$$
$$15 = 10 . 1 + 5$$
$$10 = 5 . 2 + 0$$

$$\boldsymbol{PBB(55,15)} = PBB(15,10) = PBB(10,5) = PBB(5,0) = \mathbf{5}$$

5. Kombinasi Linier

Teorema 5.
Misal terdapat $a, b \in Z^+$, maka terdapat bilangan bulat x dan y sehingga terpenuhi persamaan

$$PBB(a,b) = x.a + y.b$$

Untuk mencari nilai x dan y, dapat digunakan algoritma euclidean dan proses mundur (*backtrack*).

Contoh : Carilah nilai *x* dan *y* yang memenuhi persamaan

$$55x + 15y = PBB(55,15).$$

- Dilakukan percarian PBB(55,15)

$$55 = 15 . 3 + 10 \ldots(1)$$
$$15 = 10 . 1 + 5 \ldots(2)$$
$$10 = 5 . 2 + 0 \ldots(3)$$
$$PBB(55,15) = 5$$

Proses mundur sebagai berikut :

- Dari (1) dijadikan (4) :
  $10 = 55 . 1 + 15 . (-3) \ldots(4)$
- Sulihkan (4) ke (2) :
  $15 = \big(55 . 1 + 15 . (-3)\big) . 1 + 5 \ldots(5)$
- Dari (5) dijadikan (6) :

$$15 = 55 . 1 + 15 . (-3) + 5$$
$$55 . (-1) + 15 . 4 = 5$$

sehingga didapat x adalah -1 dan y adalah 4.

6. Relatif Prima

Dua bilangan bulat misal a dan b dikatakan relatif prima jika dan hanya jika

$$PBB(a,b) = 1$$
$$atau$$
$$x . a + y . b = 1$$

- 20 dan 7 relatif prima karena $PBB(20,7) = 1$
- 20 dan 18 tidak relatif prima karena $PBB(20,14) = 2 \neq 1$

7. Aritmatika Modulo

Jika terdapat $a, m \in Z$ dan $m > 0$, operansi $\boldsymbol{a \bmod m}$ (dibaca "a modulo m") akan memberikan hasil berupa sisa (*remainder*) dari pembagian a oleh m. Dapat ditulis sebagai:

$$a \bmod m = r$$

sedemikian sehingga,

$$a = m . q + r$$

dengan,

$$0 \le r < m.$$

Di sini, m disebut sebagai modulo dan hasil dari a mod m akan berada dalam rentang 0 dan $m - 1$.

Note :
Apabila $a \in Z^-$ dan $|a| \bmod m = r', maka$

$$a \bmod m = m - r'$$

Contoh :

- 23 mod 5 = 3
- 4 mod 7 = 4
- 0 mod 3 = 0
- -1 mod 4 = 4 – 1 = 3

8. Invers Modulo

Di dalam aritmetika bilangan riil, balikan sebuah bilangan yang tidak-nol adalah bentuk pecahannya sedemikian sehingga hasil perkalian keduanya sama dengan 1. Jika a adalah sebuah bilangan tidak-nol, maka balikannya adalah $\frac{1}{a}$ sedemikian sehingga $a . \frac{1}{a} = 1$.
Contoh: Balikan 4 adalah ¼ , sebab $4 . \frac{1}{4} = 1$.

Balikan a dilambangkan dengan a^{-1}. Di dalam aritmetika modulo, balikan modulo sebuah bilangan bulat lebih sulit untuk dihitung.

Balikan modulo hanya bisa dicari jika persamaannya memenuhi syarat, yaitu untuk sebuah bilangan bulat a dan modulus m dengan $m > 1$ relatif prima atau $gcd(a,m) = 1$, maka balikan (invers) dari $a \ (mod\ m)$ ada.

Balikan dari $a \ (mod\ m)$ adalah bilangan bulat x sedemikian sehingga :

$$x . a \equiv 1 \ (mod\ m)$$

atau dengan notasi :

$$x = a^{-1} \ (mod\ m)$$

yang nantinya inverse dari modulo (a^{-1}) merupakan kongruensi x dalam modulus m, atau ditulis :

$$a^{-1} \equiv x \ (mod\ m)$$

Pembuktiannya :

Terdapat dua buah bilangan bulat, a dan m, yang relatif prima $(PBB(a,m) = 1)$ dan terdapat bilangan bulat x dan y sedemikian sehingga :

$$x \,.\, a + y \,.\, m = 1$$

yang mengimplikasikan bahwa

$$x \,.\, a + y \,.\, m = 1 \,(mod\ m)$$

karena $y \,.\, m = 0 \,(mod\ m)$, maka

$$x \,.\, a + 0 = 1 \,(mod\ m)$$

$$x \,.\, a = 1 \,(mod\ m)$$

Kekongruenan yang terakhir ini berarti bahwa x adalah balikan dari bilangan bulat a dalam modulus m atau $a \,(mod\ m)$.

9. Kongruensi

Jika terdapat a, b dan m yang memenuhi $a \ mod\ m = c$ dan $b \ mod\ m = c$, maka dapat dikatakan bahwa a kongruen dengan b dalam modulus m, atau ditulis :

$$a \equiv b \,(mod\ m)$$

Untuk m > 0, maka juga berlaku :

$$m \mid (a - b)$$

Teorema 6. (Kongruensi Bilangan)

a) Jika $a \equiv b \,(mod\ m)$ dan c sembarang bilangan bulat, maka berlaku :
   - $(a + c) \equiv (b + c) \,(mod\ m)$
   - $a \,.\, c \equiv b \,.\, c \,(mod\ m)$
   - $a^p \equiv b^p \,(mod\ m)$

b) b) Jika $a \equiv b \,(mod\ m)$ dan $c \equiv d \,(mod\ m)$, maka berlaku:
   - $(a + c) \equiv (b + d) \,(mod\ m)$
   - $a \,.\, c \equiv b \,.\, d \,(mod\ m)$

B. Kriptografi

1. Definisi dan Istilah Penting Kriptografi

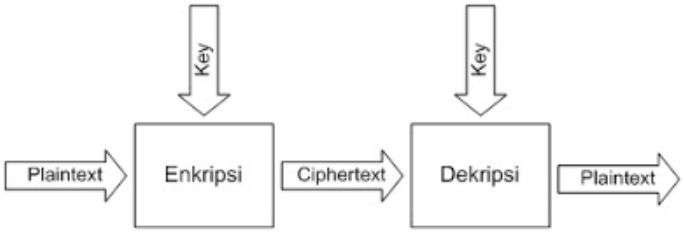
Definisi

Kriptografi berasal dari Bahasa Yunani yaitu "krypatos" yang artinya tersembunyi, disembunyikan, dirahasiakan dan "grafia" yang artinya tulisan, berita, data. Maka secara etimologi, kriptografi dapat diartikan sebagai "secret writing" atau "tulisan rahasia".

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan atau data dengan cara menyandikannya menjadi bentuk lain yang tidak bermakna. Tujuan dari penerapan ilmu kriptografi ini sendiri adalah agar pesan atau data yang bersifat rahasia tidak dapat dibaca oleh orang yang tidak berhak.

Komponen Kriptografi

- *PlainText* (Teks Biasa) : pesan yang dapat dibaca oleh manusia secara naluriah.
- *CipherText* (Kode Sandi) : pesan yang telah disandikan dengan menggunakan metode tertentu menjadi pesan acak dan tidak bermakna
- *Key* (Kunci) : Formula, rumus, atau pola yang digunakan dalam proses pengubahan bentuk pesan antara *PlainText* dan *CipherText*
- *Algoritma* (Metode) : Langkah-langkah teratur dalam proses pengkodean pesan berupa enkripsi dan dekripsi.
  - *Encryption* : Proses mengubah *PlainText* menjadi *CipherText*
  - *Decryption* : Proses mengubah *CipherText* menjadi *PlainText*



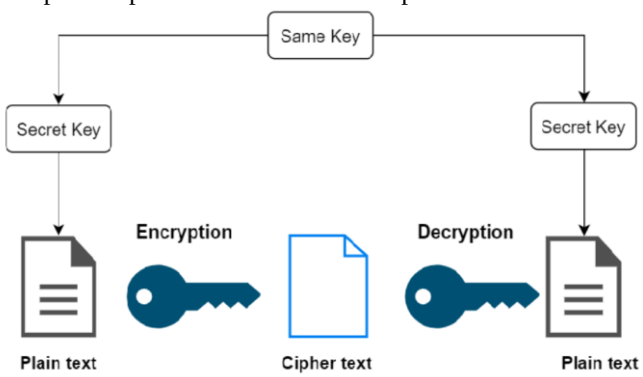
Gambar 2.2. Prinsip Kriptografi Secara Umum
Sumber : http://offrevan.blogspot.com/2018/05/enkripsi.html

2. Algoritma Kriptografi

Ada banyak algoritma kriptografi yang dapat digunakan, namun secara umum algoritma kriptografi dapat dibagi menjadi 3 kategori, yakni : *symmetric key cryptography*, *public key cryptography*, dan fungsi hash. Masing-masing memiliki perannya sendiri dalam ilmu kriptografi.

➢ **Symmetric Key Cryptography**

Kriptografi simetrik atau disebut juga kriptografi rahasia adalah kriptografi di mana kunci untuk melakukan enkripsi dan kunci untuk melakukan dekripsi adalah sama. Kunci yang dipakai saat enkripsi lah yang dipakai lagi saat dekripsi pesan. Apabila pertukaran informasi dilakukan, pesan tidak bisa disertai dengan pengiriman key karena berkemungkinan untuk dipecahkan. Algoritma kriptografi ini lebih baik digunakan apabila pertukaran informasi dalam kurun wilayah tertentu dan key yang dipakai dipahami oleh kedua belah pihak.



Gambar 2.3. Prinsip Kriptografi Kunci Simetris
Sumber : https://www.elprocus.com/cryptography-and-its-concepts/

Symmetic key cryptography biasanya digunakan untuk menjaga kerahasiaan data. Ini bisa sangat berguna untuk menjaga hard drive lokal pribadi karena pengguna yang sama umumnya mengenkripsi dan mendekripsi data yang dilindungi berbagi key dan diketahui oleh sistem lokal. Pendekatan yang diterapkan melalui jenis ini pun dianggap lebih efisien dan lebih cepat dibanding metode lainnya sehingga cocok untuk diterapkan pada mesin lokal yang membutuhkan efisiensi waktu.

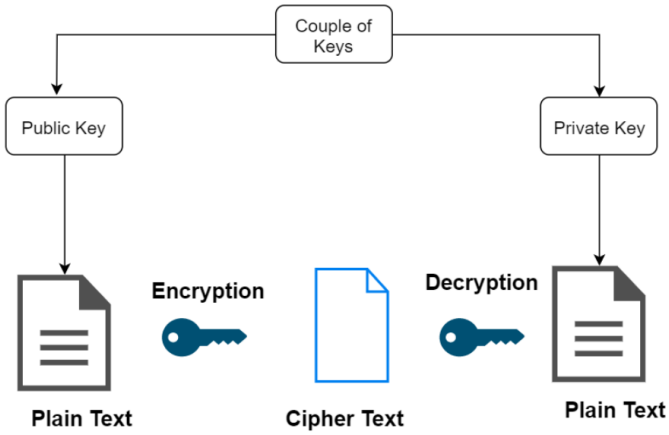
Symmetric key cryptography juga dapat digunakan untuk menjaga kerahasiaan pesan yang dikirimkan melalui internet. Namun, agar berhasil mewujudkannya, kita perlu menerapkan bentuk kriptografi berikutnya bersama-sama dengan jenis kriptografi ini.

Beberapa Algoritma Kriptografi yang termasuk kedalam jenis ini adalah:

- AES
- Block
- Pass Blocking
- DES (*Data Encryption System*)
- RC2
- IDEA
- Blowfish
- Stream cipher

➢ **Public Key Cryptography**

Dalam public key cryptography terdapat dua key. Satu bersifat publik, dan dikirimkan kepada siapa pun yang ingin diajak berkomunikasi. Itulah key yang digunakan untuk mengenkripsi pesan. Tetapi key lainnya bersifat pribadi, hanya dimiliki oleh siapa pun yang berhak untuk mendekripsi pesan-pesan itu.



Gambar 2.3. Prinsip Kriptografi Kunci Publik
Sumber : https://www.elprocus.com/cryptography-and-its-concepts/

Prinsip inti dari kriptografi jenis ini adalah kedua key sebenarnya terkait satu sama lain secara matematis sehingga mudah untuk mendapatkan key publik dari key privat tetapi tidak sebaliknya. Misalnya, key privat dapat berupa dua bilangan prima yang sangat besar yang harus dikalikan bersama untuk mendapatkan key publik.

Kompleksitas dari algoritma kriptografi jenis ini memang lebih rumit sehingga lebih aman dan lebih baik daripada jenis kunci simetris. Namun, kekurangannya adalah kurangnya efisiensi waktu dalam proses enkripsi dan dekripsi kunci sehingga tidak secepat kunci simetri. Algoritma tipe ini cocok digunakan untuk transmisi data secara terbuka dan diaplikasikan di aplikasi perpesanan seperti WhatsApp, Telegram, dan Signal.

Beberapa Algoritma Kriptografi yang termasuk kedalam jenis ini adalah:

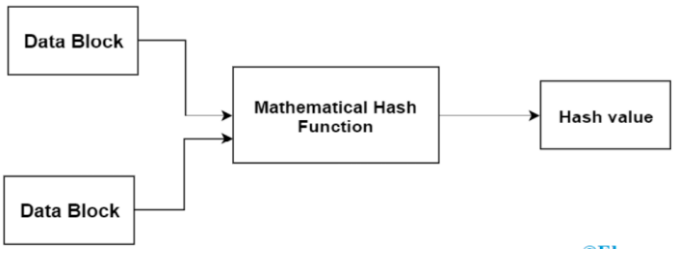
- RSA
- DSA
- PKCs
- Ecliptic curve techniques
- Diffie-Hellman key exchange

➢ **Funsi Hash**

Jenis kriptografi ini mengandalkan persamaan matematika alih-alih menggunakan kunci, di mana algoritma akan mengambil nilai numerik sebagai input dan menghasilkan pesan yang akan diringkas oleh *hash.*

Apabila pada dua metode sebelumnya dilakukan pengubahan plaintext menjadi ciphertext dan kemudian kembali menjadi plaintext. Sebaliknya, fungsi hash adalah algoritma enkripsi satu arah dan tidak memerlukan kunci apapun. Setelah kita mengenkripsi plaintext, kita tidak dapat memulihkannya dari ciphertext yang dihasilkan (disebut sebagai hash). Ini mungkin membuat fungsi hash tampak tidak berguna. Tetapi kegunaan sebenarnya dari fungsi ini adalah untuk fungsi hash apa pun, tidak ada dua plaintext yang akan menghasilkan hash yang sama (Secara matematis ini tidak sepenuhnya benar, tetapi untuk fungsi hash apa pun kemungkinan terjadinya hal itu umumnya semakin kecil dan dapat diabaikan).

Selain itu, meringkas informasi dan mengirimkan penjelasannya yang telah dirangkum adalah keguanaan sistem kerja dari metode kriptografi *hash function*.



Gambar 2.5. Prinsip Kriptografi Fungsi Hash
Sumber : https://www.elprocus.com/cryptography-and-its-concepts/

Beberapa fungsi Hash yang umum digunakan adalah:

- MD5
- SHA-1,SHA-2,SHA-3
- MAC

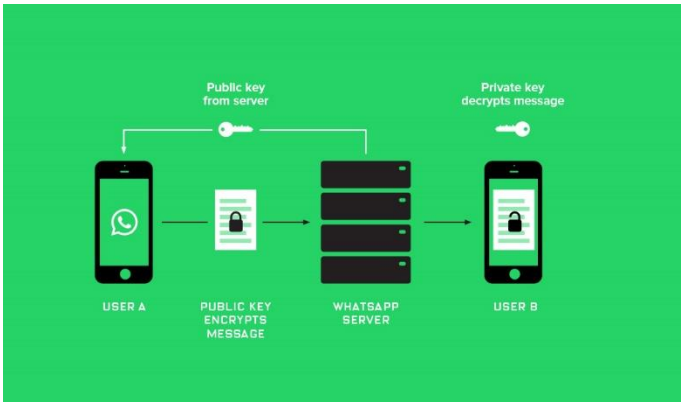
III. Implementasi Kriptografi pada Aplikasi Perpesanan

Banyaknya kasus kebocoran data oleh suatu situs maupun aplikasi tentu membuat penggunanya menjadi risih dan gelisah terhadap keamanan data mereka. Sehingga diperlukan pengamanan terhadap data pengguna. Untungnya apalikasi perpesanan saat ini telah dilindungi dengan fitur keamanan enkripsi end-to-end (E2EE) untuk menjaga data penggunanya agar tetap aman dari kebocoran.

Gambar 2.6 Prinsip Kriptografi pada Aplikasi Perpesanan
Sumber : http://www.jogjatronik.com/v3/2017/07/amankah-enkripsi-end-to-end-pada-whatsapp-telegram/

Memang, jalur komunikasi pesan terenkripsi didukung oleh Transport Layer Security (TLS) yang menghubungkan antara web client dan software web server. Namun, enkripsi biasa saja tidak cukup. Itu sebabnya client software melapisi pesan dengan enkripsi end-to-end sebelum dikirim ke web client. Pesan hanya bisa didekripsi atau dibuka oleh penerima.

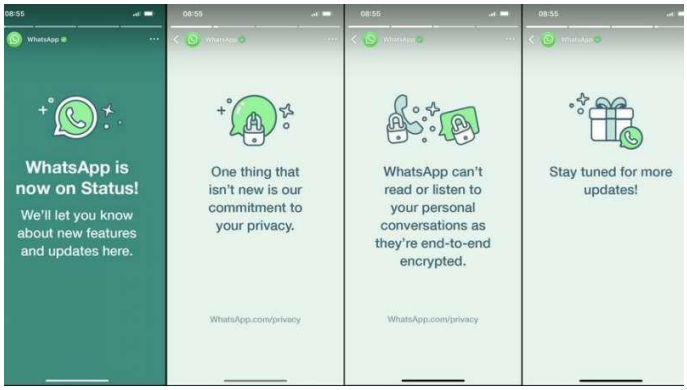
Salah satu aplikasi perpesanan terpopuler di dunia, WhatsApp, melindungi seluruh percakapan yang ada di akun personal penggunanya dengan menggunakan Signal Protocol yang dikembangkan oleh Open Whisper System. Protokol yang sama juga digunakan oleh pesaing WhatsApp, Signal untuk melindungi percakapan di aplikasinya.



Gambar 2.7 Prinsip Enkripsi End-to-end pada WhatsApp
Sumber : http://www.jogjatronik.com/v3/2017/07/amankah-enkripsi-end-to-end-pada-whatsapp-telegram/

Algoritma enkripsi end-to-end pada WhatsApp memanfaatkan algoritma RSA dan sistem TLS dengan cara kerja sebagai berikut :

1. Ketika pengguna pertama kali membuka WhatsApp, dua kunci berbeda dibuat. Proses enkripsi berlangsung di telepon itu sendiri.
2. Kunci pribadi harus tetap bersama pengguna, sedangkan kunci publik ditransfer ke penerima melalui server WhatsApp yang terpusat.
3. Kunci publik mengenkripsi pesan pengirim di telepon, bahkan sebelum mencapai server yang terpusat.
4. Server hanya digunakan untuk mengirimkan pesan terenkripsi. Pesan hanya dapat dibuka oleh kunci pribadi penerima. Tidak ada pihak ketiga, termasuk WhatsApp tidak dapat mencegat dan membaca pesan.
5. Jika seorang hacker mencoba meretas dan membaca pesan, mereka akan gagal karena enkripsi.



Gambar 2.8 Komitmen WhatsApp terhadap Keamanan data
Sumber : https://ryanphd.id/blog/apa-itu-enkripsi-end-to-end-kriptografi-ala-whatsapp

V. CONCLUSION

Teori bilangan merupakan cabang matematika murni yang mempelajari secara khusus mengenai bilangan bulat atau integer. Di dalam cabang tersebut dipelajari mengenai pembagian dan sisa pembagian, faktor pembagi bersama terbesar, relatif prima, aritmetika modulo, kombinasi linier, dan kongruensi.

Teori bilangan memiliki banyak aplikasi di dalam kehidupan nyata, salah satunya di dalam kriptografi. Kriptografi merupakan ilmu untuk mengubah bentuk pesan dari yang dapat dimengerti maknanya ke pesan yang tidak dapat dimengerti dan sebaliknya. Salah satu penggunaan kriptografi adalah pada sekuritas dan pengamanan data dalam transmisi pesan pada aplikasi perpesanan. Kriptografi pada pengamanan transmisi pesan aplikasi perpesanan pada umumnya menggunakan enkripsi end-to-end yang memanfaatkan algoritma RSA yaitu salah satu jenis algoritma kriptografi asimetrik di mana terdapat kunci yang berbeda untuk enkripsi dan dekripsi, dan sistem TLS dalam penerapannya.

IV. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih sebesar-besarnya kepada beberapa pihak yang telah berperan besar dalam penyelesaian makalah ini :

1. Tuhan Yang Maha Esa karena berkat dan rahmat-Nya, makalah ini dapat terselesaikan dengan baik tanpa kurang satu bagian pun.
2. Dra. Harlili, M.Sc. sebagai dosen kelas K2 karena telah membimbing penulis selama pembelajaran matematika diskrit. Makalah IF2120 Matematika Diskrit – Sem. I Tahun 2021/2022
3. Dr. Ir. Rinaldi, M.T. dan seluruh tim dosen matematika diskrit yang telah berperan juga dalam kegiatan perkuliahan secara daring.
4. Teman-teman seangkatan karena telah memberikan dukungan selama perkuliahan sehingga penulis dapat menulis makalah ini dengan baik.

REFERENCES

[1] http://sdp.ditjenpas.go.id/manual/3.6.1/SuratElektronicEmail.html (Diakses pada 12 Desember 2021)

[2] https://www.temukanpengertian.com/2013/01/pengertian-cryptographi-kriptografi.html (Diakses pada 12 Desember 2021)

[3] H. Rochajat Harun, Ir, M.Ed, Ph.D, dkk, *Komunikasi Pembangunan Perubahan Sosial*, (Jakarta; Rajgrafindo Persada, cet.i, 2011),hlm. 39.

[4] https://glints.com/id/lowongan/kriptografi-adalah/#.Ybi4sL1BzSE. (Diakses pada 12 Desember 2021)

[5] https://www.elprocus.com/cryptography-and-its-concepts/ (Diakses pada 12 Desember 2021)

[6] Rinaldi Munir, Diktat Kuliah IF2120 : Matematika Diskrit, Bandung : Program Studi Teknik Informatika Sekolah teknik Elektro dan informatika Institut Teknologi Bandung. https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf (Diakses pada 12 Desember 2021)

[7] http://offrevan.blogspot.com/2018/05/enkripsi.html (Diakses pada 12 Desember 2021)

[8] https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=id (Diakses pada 12 Desember 2021)

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, 13 Desember 2021

Rahmat Rafid Akbar−13520090