Penerapan Teori Bilangan (Kriptografi) untuk Mengamankan Sebuah Informasi

Jauza Lathifah Annassalafi - 13521030[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13521030@std.stei.itb.ac.id

***Abstrak*— Matematika diskrit memiliki banyak kegunaannya untuk kehidupan manusia, salah satunya adalah teori bilangan yang diterapkan pada kriptografi dengan memanfaatkan aritmetika modulo dan prinsip bilangan prima untuk menjaga keamanan dan kerahasiaan sebuah informasi. Seiring berkembangnya zaman, informasi semakin mudah untuk disampaikan tanpa batasan ruang maupun waktu. Agar informasi tersebut tetap terjaga kerahasiaannya, dapat dilakukan enkripsi-dekripsi informasi agar pihak lain tidak mengetahui isi dari informasi tersebut. Peningkatan keamanan informasi dibuat dengan mengkombinasikan dua algoritma, yaitu algoritma caesar cipher dan algoritma RSA, dengan tujuan menjaga kerahasiaan informasi agar lebih terjamin.**

***Keywords*— Teori Biangan, Kriptografi, Caesar Cipher, RSA.**

I. PENDAHULUAN

Sejatinya manusia adalah makhluk sosial yang artinya manusia hidup dan tumbuh bersama manusia lain dengan bersosialisasi, berkomunikasi, berpesan, dan lain sebagainya. Di saat-saat tertentu, seseorang hanya ingin memberikan suatu pesan atau informasi kepada pihak-pihak tertentu. Untuk menjaga keamanan sebuah informasi yang ingin disampaikan, maka perlu diberi suatu tindakan khusus sehingga informasi tersebut tidak bocor kepada pihak lain, sehingga masalah dalam menjaga keamanan sebuah informasi merupakan aspek yang penting.

Ditambah teknologi di bidang ilmu komputer yang kian hari semakin berkembang, sehingga hal ini dapat memudahkan seseorang untuk melakukan perusakan atau pencurian sebuah informasi terutama yang tersimpan dalam bentuk digital. Keamanan pesan atau informasi merupakan salah satu yang wajib dimiliki karena bisa saja informasi tersebut merupakan informasi yang berbentuk sangat rahasia, misalnya informasi mengenai password atau PIN. Dengan demikian dibutuhkan sebuah tindakan untuk mengatasi hal tersebut, yaitu salah satunya dengan kriptografi.

Kriptografi ada karena adanya situasi berkomunikasi dan saling bertukar informasi atau data secara jarak jauh. Komunikasi dan pertukaran informasi dapat dilakukan antar wilayah, negara, maupun benua, sehingga dibutuhkan keamanan terhadap kerahasiaan informasi yang dipertukarkan tersebut yang semakin meningkat.

Kriptografi merupakan salah satu cara agar sebuah informasi dapat tetap terjaga kerahasiaannya dengan mengenkripsi (proses penyandian pesan asli menjadi pesan tersandi) dan mendekripsi (mengembalikan pesan yang tersandi menjadi pesan asli) sebuah informasi. Setiap proses enkripsi dan dekripsi membutuhkan parameter untuk transformasi yang dinamakan kunci.

Berdasarkan kunci yang digunakan, ada tiga jenis kriptografi, yaitu kriptografi klasik (algoritma simetri), kriptografi kunci publik (algoritma asimetri), dan fungsi hash (hash function). Algoritma simetri disebut dengan kriptografi klasik karena untuk proses enkripsi dan dekripsinya hanya menggunakan satu kunci dan kunci tersebut bersifat rahasia. Jika orang lain mengetahui kuncinya maka orang tersebut dapat melakukan proses enkripsi dan dekripsi. Algoritma asimetri sering disebut dengan kriptografi kunci publik yang dalam proses enkripsi menggunakan kunci publik, sedangkan untuk proses dekripsi menggunakan kunci privat. Yang artinya, pesan yang dienkripsi menggunakan kunci publik hanya dapat didekripsi menggunakan kunci privat. Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sebarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap.

RSA merupakan salah satu contoh dari algoritma asimetri yang digunakan untuk mengamankan sebuah informasi. Nama RSA didapat dari singkatan huruf depan tiap nama para penemunya yaitu Rivest, Shamir, dan Adleman. RSA dianggap algoritma paling aman karena menggunakan algoritma pemfaktoran bilangan yang sangat besar, tetapi RSA lambat dalam proses enkripsi dan dekripsi dibandingkan dengan algoritma simetri. Selanjutnya, algoritma caesar cipher yang merupakan salah satu contoh dari algoritma simetri. cara kerjanya adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Kelemahan caesar cipher adalah pesan asli dapat diperoleh dengan metode brute force dan presentasi frekuensi huruf yang paling sering muncul dalam suatu kalimat. Algoritma simetri juga memiliki sistem keamanan yang lemah karena kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk dekripsi. Untuk menutup kekurangan tersebut, penggabungan kedua algoritma caesar cipher dan algoritma RSA memungkinkan keamanan pada informasi yang berbentuk pesan sangat efektif untuk mengunci informasi menjadi lebih baik lagi.

II. LANDASAN TEORI

2.1 Teori Bilangan

Teori bilangan adalah ilmu atau cabang matematika murni yang mempelajari bilangan bulat (integer) atau fungsi bernilai bilangan bulat.

2.1.1 Bilangan

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

1. Bilangan Asli (N), yaitu bilangan yang dimulai dari 1 ke atas {1, 2, 3, 4, 5, 6, 7, …}. Berdasarkan bentuknya, bilangan asli bisa dibagi lagi jadi empat macam, yaitu:
   - Bilangan genap {2, 4, 6, 8, 10, …}.
   - Bilangan ganjil {1, 3, 5, 7, 9, …}.
   - Bilangan prima yang merupakan bilangan asli yang cuma punya dua faktor, yaitu satu dan bilangan itu sendiri {2, 3, 5, 7, 11, …}.
   - Bilangan komposit yang punya lebih dari dua faktor atau bisa dibagi dengan bilangan lain selain satu dan dirinya sendiri {4, 6, 8, 9, 10, …}.
2. Bilangan Cacah, yaitu bilangan asli yang juga meliputi angka 0 : {0, 1, 2, 3, 4, 5, 6, 7, …}.
3. Bilangan Bulat (Z), yaitu bilangan cacah yang ditambahkan dengan bilangan negatif : {-4, -3, -2, -1 , 0, 1, 2, 3, 4,…}.
4. Bilangan Pecahan, yaitu bilangan yang dapat dinyatakan dalam bentuk pecahan a/b : {1/2, 3/4, 5/6, 7/8, …}.
5. Bilangan Rasional, yaitu bilangan yang meliputi bilangan Bulat dan Pecahan.
6. Bilangan Irasional, yaitu bilangan yang tidak dapat dinyatakan dalam bentuk pecahan a/b : {√2, √3, dan bilangan irasional lainnya}.
7. Bilangan Riil (R), yaitu bilangan yang meliputi bilangan rasional dan irasional.
8. Bilangan Imajiner, yaitu bilangan yang meliputi i di mana i2 = -1, contoh √−1, √−2 .
9. Bilangan Kompleks, yaitu bilangan yang meliputi bilangan Riil dan Imajiner.

2.1.2 Bilangan Bulat

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal, misalnya 8, 21, 8765, -34, 0. Kebalikan dari bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02.

Sifat Pembagian pada Bilangan Bulat

Jika terdapat a dan b yang merupakan dua buah bilangan bulat dengan syarat $a \neq 0$. Dikatakan bahwa a habis membagi b (a divides b) jika terdapat bilangan bulat c sedemikian sehingga $b = ac$.

Notasinya adalah $a \mid b$ jika $b = ac$, $c \in Z$ dan $a \neq 0$. Pernyataan "a habis membagi b" dapat ditulis juga "b kelipatan a".

Contoh : 5 habis membagi 20 karena terdapat sebuah bilangan $c = 4$ sehingga $5 \mid 20$ karena $20 \div 5 = 4$ (bilangan bulat) atau $20 = 5 \times 4$.

Teorema 1

Jika $m, n \in Z$ dan $n > 0$, m dibagi dengan n maka terdapat dua buah bilangan unik q (quotient) dan r (remainder), sedemikian sehingga

$$m = n \,.\, q + r$$

dengan

$$0 \leq r < n$$

Contoh : 1987 dibagi dengan 97 memberikan hasil bagi 20 dan sisa 47:

$$1987 = 97 \,.\, 20 + 47$$

2.1.3 Pembagian Bersama Terbesar (PBB)

Teorema 2

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

$$PBB(a, b) = c$$

dengan syarat,

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

Contoh : $PBB(36, 45) = 9$ karena 9 merupakan bilangan bulat terbesar yang memenuhi $9 \mid 36$ dan $9 \mid 45$.

Teorema 3

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

$$m = nq + r$$

dengan,

$$0 \leq r < n$$

maka dapat dipastikan, $PBB(m, n) = PBB(n, r)$

Algoritma Euclidean

Tujuannya adalah untuk mencari PBB dari dua buah bilangan bulat yang ditemukan oleh Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, Element.

Jika $m, n \in Z^+$ dan $m \geq n$ maka pembagi bersama terbesar dari dua bilangan tersebut dapat dicari dengan memanfaatkan Teorema 1. dan Teorema 3. dengan algoritma berikut:

1. Jika n = 0 maka m adalah PBB(m,n);
   stop.
   Tetapi, jika n ≠ 0 maka lanjutkan ke langkah 2.
2. Bagi m dengan n dan menghasilkan sisa r.
3. Ubah nilai m menjadi nilai n dan nilai n menjadi nilai r.
4. Ulang Kembali ke Langkah 1.

Berikut ilustrasinya, $PBB(m, n)$ dengan,

$$m \geq n, r_0 = m \text{ dan } r_1 = n :$$

$$r_0 = r_1 \,.\, q + r_2, \qquad 0 \leq r_2 < r_1$$
$$r_0 = r_1 \,.\, q + r_2, \qquad 0 \leq r_3 < r_2$$
$$\vdots$$
$$\vdots$$
$$r_{n-2} = r_{n-1} \,.\, q_{n-1} + r_n, \qquad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n \,.\, q_n + 0$$

Sehingga,

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

Contoh : PBB(80, 12)

$$80 = 12 \,.\, 6 + 8$$
$$12 = 8 \,.\, 1 + 4$$
$$8 = 4 \,.\, 2 + 0$$
$$PBB(80, 12) = PBB(12, 8) = PBB(8, 4) = PBB(4,0) = 4$$

2.1.4 Relatif Prima

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

$$PBB(a, b) = 1$$

atau

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

Contoh : 20 dan 11 relatif prima karena $PBB(20,11) = 1$. Namun, 20 dan 10 tidak relatif prima karena $PBB(20,10) = 10 \neq 1$.

Jika a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$ma + nb = 1$$

Contoh : Bilangan 20 dan 3 adalah relatif prima karena $PBB(20, 3) = 1$, atau dapat ditulis $2 \,.\, 20 + (-13) \,.\, 3 = 1$ dengan $m = 2$ dan $n = -13$. Tetapi 20 dan 5 tidak relatif prima karena $PBB(20, 5) = 5 \neq 1$ sehingga 20 dan 5 tidak dapat dinyatakan dalam $m \,.\, 20 + n \,.\, 5 = 1$.

2.1.5 Aritmetika Modulo

Jika a, $m \in Z$ dan $m > 0$, operansi $a \bmod m$ (dibaca "a modulo m") memberikan sisa (remainder) dari pembagian a dibagi dengan m.

Notasi : $a \bmod m = r$ sedemikian sehingga,

$$a = m \,.\, q + r$$

dengan,

$$0 \leq r < m$$

Catatan : Apabila $a \in A^-$ – dan $|a| \bmod m = r'$, maka $a \bmod m = m - r'$.

Contoh :

(i) $6 \bmod 8 = 6$ $\quad (6 = 8 \times 0 + 6)$

(ii) $0 \bmod 12 = 0$ $\quad (0 = 12 \times 0 + 0)$

(iii) $-41 \bmod 9 = 4$ $\quad (-41 = 9(-5) + 4)$

Kongruen

Jika a, b dan $m > 0$ yang memenuhi $a \bmod m = c$ dan $b \bmod m = c$, maka dapat dikatakan bahwa a kongruen dengan b dalam modulus m, atau ditulis sebagai:

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

Kekongruenan $a \equiv b \,(mod\, m)$ juga dapat dituliskan dalam hubungan

$$a = b + km$$

k adalah bilangan bulat.

Teorema 4

Misalkan $m > 0$,

1. Jika $a \equiv b \,(mod\, m)$ dan c sembarang bilangan bulat, maka:
   (i) $(a + c) \equiv (b + c) \,(mod\, m)$
   (ii) $a \,.\, c \equiv b \,.\, c \,(mod\, m)$
   (iii) $a^p \equiv b^p \,(mod\, m)$ untuk bilangan bualat tidak negative p.
2. Jika $a \equiv b \,(mod\, m)$ dan $c \equiv d \,(mod\, m)$, maka
   (i) $(a + c) \equiv (b + d) \,(mod\, m)$
   (ii) $a \,.\, c \equiv b \,.\, d \,(mod\, m)$

Teorema 4. tidak terdapat operasi pembagian pada aritmetika modulo karena jika kedua ruas dibagi dengan bilangan bulat, maka kekongruenan tidak selalu dipenuhi.

Misalnya: $14 \equiv 8 \,(mod\, 6)$ tidak dapat dibagi dengan 2, karena $14 \div 2 = 7$ dan $8 \div 2 = 4$, tetapi $7 \equiv ! \, 4 \,(mod\, 6)$.

Balikan modulo (modulo invers)

Jika a dan m relatif prima dan $m > 1$, maka dapt ditemukan balikan (invers) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat x sedemikian sehingga

$$a \,.\, b \equiv 1 \,(mod\, m)$$

atau dengan notasi :

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

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

$$a - 1 \equiv x \,(mod\, m)$$

Bukti :

Dua buah bilangan bulat, a dan m, yang relatif prima ($PBB(a, m) = 1$) dan terdapat bilangan bulat p dan q sedemikian sehingga :

$$p \,.\, a + q \,.\, m = 1$$

yang mengimplikasikan bahwa

$$p \,.\, a + q \,.\, m = 1 \,(mod\, m)$$

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

$$p \,.\, a \equiv 1 \,(mod\, m)$$

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

Kekongruenan lanjar

Kekongruenan lanjar adalah kongruen yang berbentuk

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

dengan $m > 0$, $a, b \in Z$, dan x adalah peubah bilangan bulat yang dapat dicari sebagai berikut:

$$ax = b + km$$

yang dapat disusun menjadi

$$x = \frac{b + km}{a}$$

Dengan k adalah sembarang bilangan bulat. Uji untuk k = 0, 1, 2, … dan k = -1, -2, … yang menghasilkan x sebagai bilangan bulat.

Chinese remaider problem

Pada abad pertama, seorang matematikawan China yang bernama Sun Tse mengajukan pertanyaan "Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7". Pertanyaan Sun Tse dapat dirumuskan kedalam sistem kongruen lanjar:

$$x \equiv 3 \,(mod\, 5)$$
$$x \equiv 5 \,(mod\, 7)$$
$$x \equiv 7 \,(mod\, 11)$$

Teorema 5. (Chinese Remainder Theorem)

Misalkan $m_1, m_2, \ldots, m_n$ adalah bilangan bulat positif sedemikian sehingga $PBB(m_i, m_j) = 1$ untuk $i \neq j$. Maka sistem kekongruenan linier

$$x \equiv a_1 (mod\, m_1)$$
$$x \equiv a_2 \,(mod\, m_2)$$
$$\vdots$$
$$\vdots$$
$$x \equiv a_n (mod\, m_n)$$

memiliki solusi unik dalam modulus $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$. (adanya solusi x dengan $0 \leq x < m$ dan semua solusi lain yang kongruen dalam modulus m dengan solusi ini).

2.1.6 Aritmetika Modulo dan Kriptografi

Aritmetika modulo layak digunakan dalam kriptografi karena dua alasan:

1. Nilai-nilai aritmetika modulo berada dalam himpunan berhingga (0 sampai modulus m – 1).
2. Dengan mengoprasikan bilangan bulat, maka tidak ada kehilangan informasi akibat pembulatan (round off).

2.1.7 Bilangan Prima

Bilangan prima adalah bilangan bulat positif p dengan $(p > 1)$ yang pembaginya hanya 1 dan p. Bilangan prima harus lebih besar dari 1, maka barisan bilangan prima dimulai dari 2, yaitu 2, 3, 5, 7, 11, 13, …. Seluruh bilangan prima adalah bilangan ganjil, kecuali 2 yang merupakan bilangan genap.

Teorema 6. (The Fundamental Theorem of Arithmetic)

Setiap bilangan yaitu x $(x \geq 2)$ dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

Untuk menguji apakah x adalah bilangan prima atau komposit (bilangan selain prima), yaitu dengan membagi x dengan sejumlah bilangan prima, mulai dari 2, 3, … , bilangan prima $\leq \sqrt{x}$. Jika x habis dibagi dengan salah satu dari bilangan prima tersebut, maka x adalah bilangan komposit, tetapi jika x tidak habis dibagi oleh semua bilangan prima tersebut, maka x adalah bilangan prima.

Ada metode lain yang digunakan untuk menguji keprimaan suatu bilangan bulat, yaitu dikenal dengan Teorema Fermat. Fermat (dibaca “Fair-ma”) adalah seorang matematikawan Perancis pada tahun 1640.

Teorema 7. (Teorema Fermat)

Jika p adalah bilangan prima dan a adalah bilangan bulat yang tidak habis dibagi dengan p, yaitu $PBB(a, p) = 1$, maka

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

2.2 Kriptografi

2.2.1 Istilah-Istilah dalam Kriptografi

Kriptografi adalah istilah yang berasal dari Bahasa Yunani, yaitu Crypto yang berarti rahasia dan Graphia yang berarti tulisan. Kriptografi juga dapat diartikan sebagai teknik menjaga keamanan pesan dengan cara mengubahnya menjadi bentuk lain yang tidak bermakna sehingga tidak dapat dibaca oleh pihak ketiga dan dapat terjaga kerahasiannya.

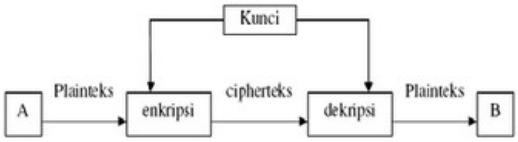
Sejarahnya, teknik kriptografi pertama kali dipakai oleh Julius Caesar, seorang pemimpin militer Romawi pada Zaman Romawi Kuno. Julius Caesar ingin mengirimkan pesan kepada seorang jendral melalui seorang kurir. Raja tersebut tidak ingin pesannya dapat dibaca oleh pihak lain sehingga Julius Caesar mengacak pesan tersebut menjadi suatu pesan yang tidak dapat dibaca dan dipahami terkecuali jendralnya.

Teknik yang digunakan dalam kriptografi adalah metode scrambling, yaitu teknik pengubahan teks biasa menjadi teks sandi. Teknik scrambling tersebut dikenal dengan istilah enkripsi dan dekripsi. Yang mana, terdapat beberapa komponen dasar di dalam algoritma kriptografi sendiri, antara lain yaitu:

1. Enkripsi : pengamanan data dengan mengubah plaintext (pesan asli) menjadi ciphertext atau kode yang tidak dapat dimengerti oleh pihak lain, sehingga pesan tersebut dapat terjaga kerahasiaannya.
2. Dekripsi : kebalikan dari enkripsi, yaitu pesan yang masih acak dan tidak bermakna atau hasil enkripsi akan dikembalikan ke bentuk asalnya, sehingga pesan tersebut dapat dibaca.
3. Kunci : kunci yang digunakan untuk melakukan enkripsi dan dekripsi pesan.Terdapat dua jenis kunci, yaitu kunci rahasia (private key) dan kunci umum (public key).
4. Ciphertext : pesan ter-enkrip (tersandi) hasil dari enkripsi yang tidak memiliki makna lagi.
5. Plaintext : atau teks asli merupakan data atau informasi yang dapat dibaca dan dimengerti maknanya yang akan diproses untuk menjadi ciphertext.

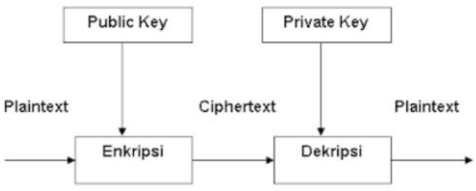
Kriptografi sebagai metode enkripsi data terdiri dari tiga jenis, yaitu:

1. Algoritma Simetris : atau sering disebut dengan single-key algorithm merupakan algoritma hanya menggunakan satu kunci yang sama untuk melakukan kegiatan enkripsi dan dekripsi. Pada algoritma ini, pengirim dan penerima harus memilih satu kunci yang sama untuk digunakan sebagai enkripsi dan dekripsi dan harus dijaga kerahasiaannya dari pihak yang tidak berkepentingan sehingga pihak lain tidak dapat melakukan enkripsi dan dekripsi terhadap informasi. Berikut diagram proses enkripsi dan dekripsi pada algoritma simetris.



Gambar 1. Penggunaan kunci simetris
(Sumber : https://maizarti.wordpress.com/2011/04/12/kriptografi-asimetris/)

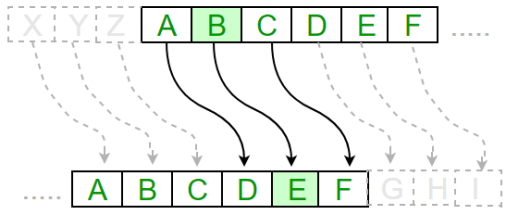
2. Algoritma Asimetris : atau biasa disebut dengan algoritma kunci publik yang menggunakan dua kunci yang berbeda untuk enkripsi dan dekripsinya. Pada algoritma ini, digunakan dua kunci yakni kunci umum (public key) dan kunci rahasia (private key). Kunci publik diketahui ohel semua orang (dipublikasikan). Berbeda dengan kunci rahasia yang hanya boleh diketahui satu orang saja. Berikut diagram proses enkripsi dan dekripsi pada algoritma asimetris.



Gambar 2. Penggunaan kunci Asimetris
(Sumber : http://w-learningeducation.blogspot.com/2017/05/algoritma-algoritma-klasik.html)

2.2.2 Algoritma Caesar Cipher

Dalam kriptografi, sandi Caesar atau sandi geser merupakan sandi substitusi dimana setiap huruf pada teks asli (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Algoritma ini bisa dibilang cukup mudah untuk digunakan. Intinya adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Caesar cipher merupakan bagian dari algoritma simetris, yang artinya pada proses enkripsi dan dekripsi memiliki kunci yang sama.



Gambar 3. Caesar cipher pada Kriptografi
(Sumber : https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/)

Algoritma dari Caesar Cipher untuk alfabet ASCII 256 karakter adalah

1. Proses Enkripsi
   Enkripsi : $c = E(p) = (p + k)\ mod\ 256$
2. Proses Dekripsi
   Dekripsi : $p = D(c) = (c - k)\ mod\ 256$

2.2.3 Algoritma RSA

Algoritma RSA diperkenalkan oleh tiga peneliti dari MIT (Massachussets Institute of Technology) yaitu, Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Algoritma RSA merupakan algoritma kriptografi kunci publik (asimetris) sehingga RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Proses enkripsi dan dekripsi pada algoritma RSA didasari pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (kunci publik), tetapi kunci untuk dekripsi bersifat rahasia (kunci privat). Kunci dekripsi, ditentukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Namun, memfaktorkan bilangan bulat menjadi faktor primanya tidaklah mudah. Cara yang dapat digunakan adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin sulit pemfaktorannya sehingga semakin lama waktu yang dibutuhkan dan semakin kuat pula algoritma RSA.

Berikut ini adalah proses pembentukan kunci dalam algoritma kriptografi RSA :

1. Pilih dua bilangan prima sembarang sebagai p dan q (nilai $p \neq q$).
2. Hitung nilai $n = p.q$
3. Hitung $m = (p - 1)(q - 1)$.
4. Pilih kunci publik e yang relatif prima terhadap m. Didapatkan PBB (e, m) = 1
5. Bangkitkan kunci privat dengan persamaan $e.d \equiv 1\ (mod\ n)$. Perhatikan bahwa persamaan $e.d \equiv 1\ (mod\ n)$ ekivalen dengan $e.d = 1 + kn$, sehingga untuk mencari nilai d dapat dihitung dengan $d = \frac{1+kn}{e}$.

Hasil dari pembentukan pasangan kunci di atas adalah

1. Kunci publik (e, n)
2. Kunci rahasia (d, n)

Untuk proses enkripsi diperoleh dari pasangan kunci publik dengan plaintext dan menghasilkan ciphertext, yaitu

$$C \equiv P^e\ (mod\ n)$$

Untuk proses dekripsi diperoleh dari pasangan kunci privat dengan ciphertext dan menghasilkan plaintext, yaitu

$$P \equiv C^e\ (mod\ n)$$

2.2.4 ASCII

Plainteks yang akan dienkripsi oleh algoritma RSA berupa angka-angka, sedangkan terdapat informasi yang dikirimkan dalam bentuk teks sehingga dibutuhkan suatu kode yang sifatnya universal untuk mengubah informasi menjadi plainteks yang berbentuk angka. ASCII (American Standard Code for Information Interchange) atau Kode Standar Amerika untuk Pertukaran Informasi adalah suatu standar internasional dalam kode huruf dan simbol yang bersifat universal. Kode ASCII memiliki komposisi bilangan biner 8 bit dimulai dari 0000 0000 sampai 1111 1111. Total kombinasi yang dihasilkan sebanyak 256 dimulai dari 0 sampai 255.

III. Implementasi Algoritma Caesar Cipher dan RSA Dalam Mengamankan Sebuah Informasi

3.1. Proses Enkripsi

Untuk mengamankan sebuah informasi, pertama, penulis melakukan enkripsi pada sebuah informasi menggunakan algoritma caesar cipher. Akan dilakukan enkripsi terhadap sebuah informasi "InfOrmAtIkA 2021" dengan kunci atau pergeseran 7 posisi berdasarkan ASCII.

Enkripsi menggunakan persamaan:

$$c = E(p) = (p + k)\ mod\ 256$$

dengan,
$c = hasil\ enkripsi\ caesar\ cipher\ (ASCII)$
$p = ASCII$ dari karakter pada plaintext
$k = kunci$

Karakter (plaintext)	p	c	Karakter (ciphertext)
I	73	80	P
n	110	117	u
f	102	109	m
O	79	86	V
r	114	121	y
m	109	116	t
A	65	72	H
t	116	123	{
I	105	80	P
k	107	114	r
A	65	72	H
space	32	39	‘
2	50	57	9
0	48	55	7
2	50	57	9
1	49	56	8

Tabel 1. Proses Enkripsi dengan Caesar cipher

Kedua, lakukan enkripsi kembali terhadap hasil enkripsi caesar cipher menggunaka algoritma RSA. Enkripsi informasi dengan lagoritma RSA memiliki beberapa tahapan, yaitu:

1) Pilih 2 bilangan prima acak sebagai p dan q, pada kasus ini penulis menggunakan p = 19 dan q = 13.
2) Hitung nilai n yang dapat dicari dengan n = p * q = 19 * 13 = 247.
3) Hitung nilai totient(n) = m = (p - 1) * (q - 1) = 18 * 12 = 216.
4) Pilih sebuah bilangan bulat untuk kunci publik (e) yang relatif prima terhadap m, yaitu PBB(e, m) = 1, maka harus didapatkan nilai $e \,.\, d \; mod \; 216 = 1$, yaitu e = 7.
5) Hitung kunci dekripsi (d) di dapat melalui persamaan d = (1 + km)/e. Dengan melakukan percobaan untuk k = 1, 2, 3, … diperoleh nilai d = 31.

Setelah ditemukan nilai dari setiap besaran-besaran yang akan digunakan pada algoritma RSA, dapat dilakukan enkripsi terhadap informasi "PumVytH{PrH'9798" yang merupakan hasil dari enkripsi informasi "InfOrmAtIkA 2021" menggunakan caesar cipher.

Enkripsi algoritma RSA menggunakan persamaan berikut:

$$C_i = M_i^e \; mod \; n$$

dengan,
C_i : hasil enkripsi RSA ke-i
M_i : c (hasil enkripsi caesar cipher ke-i)
e : kunci publik = 7
n : 247

i	M_i	C_i	Karakter (ciphertext)
1	80	63	?
2	117	78	N
3	109	60	<
4	118	148	”
5	121	121	y
6	116	90	Z
7	104	32	*space*
8	123	137	‰
9	112	63	?
10	114	114	r
11	104	32	*space*
12	39	39	‘
13	57	190	¾
14	55	81	Q
15	57	190	¾
16	56	56	8

Tabel 2. Proses Enkripsi dengan RSA

Didapatkan hasil enkripsi "?N<”yZ ‰?r ‘¾Q¾8".

3.2. Proses Dekripsi

Setelah informasi yang kita miliki diubah menjadi ciphertext atau kode acak yang tidak memiliki makna, untuk mengembalikannya menjadi plaintext perlu dilakukan dekripsi, sehingga informasi tersebut dapat dibaca.

Pertama, deskripsi dilakukan dengan menggunakan algoritma RSA.

$$M_i = C_i^e \; mod \; n$$

dengan,
C_i : hasil enkripsi RSA ke-i
M_i : c (hasil dekripsi RSA ke-i).
e : kunci publik = 7
n : 19

i	C_i	M_i	Karakter
1	63	80	P
2	78	117	u
3	60	109	m
4	148	86	V
5	121	121	y
6	90	116	t
7	32	72	H
8	137	123	{
9	63	80	P
10	114	114	r
11	32	104	H
12	39	39	‘
13	190	57	9
14	81	55	7
15	190	57	9
16	56	56	8

Tabel 3. Proses dekripsi dengan RSA

Selanjutnya, dilakukan dekripsi dengan Algoritma caesar cipher.

$$p = D(c) = (c - \; k) \; mod \; 256$$

dengan,
p : hasil deskripsi menggunakan caesar cipher (ASCII)
c : ASCII
k : kunci = 7

Karakter (ciphertext)	c	p	Karakter (plaintext)
P	80	73	I
u	117	110	n
m	109	102	f
V	86	79	O
y	121	114	r
t	116	109	m
H	72	65	A
{	123	116	t
P	80	105	I
r	114	107	k
H	72	65	A
‘	39	32	*space*
9	57	50	2
7	55	48	0
9	57	50	2
8	56	49	1

Tabel 4. Proses Dekripsi dengan Caesar cipher

Setelah dilakukan dekripsi menggunakan caesar cipher, hasilnya berupa plaintext yang berisikan informasi awal, yaitu "InfOrmAtIkA 2021".

VI. KESIMPULAN

Teori bilangan sangat bermanfaat dalam kehidupan nyata, salah satunya di dalam kriptografi. Mengamankan sebuah informasi dengan menggabungkan dua algoritma, Caesar cipher dan RSA berhasil dilakukan. Algoritma caesar cipher yang dapat dipecahkan dengan cara brute force attack dan diperkuat dengan menggunakan RSA, efektif dalam menjaga kerahasiaan sebuah informasi jika dibandingkan hanya menggunakan satu algoritma saja. Menggunakan perhitungan dengan struktur ASCII, alfabet, dan dipadukan dengan menggunakan pemfaktoran bilangan prima dapat meningkatkan sistem keamanan data, sehingga informasi yang tersimpan akan semakin terjaga.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih Penulis sampaikan kepada pihak yang sudah membantu dalam menyelesaikan makalah ini. Kepada Allah SWT yang sudah memberikan kesehatan dan kesempatan kepada penulis untuk menulis makalah ini. Selain itu, penulis secara khusus mengucapkan terima kasih kepada keluarga, Bapak Dr. Ir. Rinaldi Munir, MT. selaku dosen pengampu mata kuliah IF2120 Matematika Diskrit kelas 03, seluruh tim dosen matematika diskrit yang telah berperan juga dalam kegiatan perkuliahan, dan teman-teman. Terima kasih juga kepada pembuat referensi yang sudah berkenan untuk berbagi ilmu.

REFERENSI

[1] "Kriptografi: Definisi, Sejarah, Jenis. Dan Algoritmanya," April 19, 2021. https://www.sekawanmedia.co.id/blog/pengertian-kriptografi/.
[2] "10 Jenis Bilangan - Zenius Untuk Guru." Accessed December 12, 2022. https://www.zenius.net/blog/10-jenis-bilangan#Jenis-Jenis_Bilangan.
[3] https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf
Diakses pada tanggal 10 Desember 2022, pukul 9.41 WIB.
[4] https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian2.pdf
Diakses pada tanggal 10 Desember 2022, pukul 9.41 WIB.
[5] https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf
Diakses pada tanggal 10 Desember 2022, pukul 9.52 WIB.
[6] https://media.neliti.com/media/publications/144706-ID-implementasi-algoritma-kriptografi-rsa-u.pdf
Diakses pada tanggal 10 Desember 2022, pukul 12.05 WIB.
[7] https://medium.com/bisa-ai/kriptografi-klasik-caesar-cipher-a33334fe2965
Diakses pada tanggal 10 Desember 2022, pukul 12.08 WIB.
[8] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Teori%20Bilangan.pdf
Diakses pada tanggal 11 Desember 2022, pukul 9.55 WIB.
[9] http://repository.upi.edu/2939/6/S_MTK_0905803_CHAPTER3.pdf
Diakses pada tanggal 11 Desember 2022, pukul 13.31 WIB.
[10] http://etheses.uin-malang.ac.id/13318/1/13610118.pdf
Diakses pada tanggal 11 Desember 2022, pukul 14.05 WIB.

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, 12 Desember 2022

Jauza Lathifah Annassalafi (13521030)