Penerapan Teori Bilangan dalam Kriptografi

Mgs. Tabrani (13519122)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13519122@std.stei.itb.ac.id

***Abstrak*—Makalah ini terdiri dari 5 bab. Bab 1 berisi pendahuluan. Bab 2 berisi landasan teori yang mencakup teori bilangan, kriptografi, dan sejarah dalam kriptografi. Bab 3 berisi pembahasan yang menjabarkan algoritma-algoritma yang menerapkan teori bilangan, seperti algoritma RSA, algoritma Elgamal, algoritma pertukaran Kunci Diffie-Hellman, dan algoritma Kriptografi Knapsack. Bab 4 berisi simpulan. Bab 5 berisi ucapan terima kasih dari penulis.**

Kata Kunci—Teori Bilangan, Kriptografi, Algoritma.

I. PENDAHULUAN

Matematika merupakan salah satu bidang yang vital dalam kehidupan manusia. Teori bilangan adalah salah satu topik yang dipelajari dalam Matematika. Teori bilangan menjadi salah satu topik yang banyak diterapkan dalam kehidupan manusia.

Dewasa ini, teknologi kian berkembang pesat. Perkembangan teknologi tersebut dapat menimbulkan dampak positif atau bahkan negatif. Dampak positif teknologi ini membuat kita lupa bahwa teknologi juga memiliki dampak negatif. Teknologi yang hakikatnya ditujukan untuk mempermudah dan mempercepat urusan manusia justru akan menjadi boomerang apabila teknologi digunakan untuk hal yang tidak baik.

Kejahatan di dunia teknologi kerap kali timbul berupa kejahatan siber. Kejahatan ini berupa kejahatan dalam bidang teknologi informasi. Peretasan terhadap informasi dan data penting menjadi sangat sering dilakukan pada zaman ini. Kejahatan tersebut membuat para pengguna teknologi informasi ini menjadi tidak nyaman. Oleh karena itu dibuatlah sebuah sistema yang dapat menangani ketidaknyamanan tersebut. Kriptografi menjadi salah satu solusi agar dapat mengurangi kejahatan siber tersebut. Kriptografi berfungsi untuk merubah informasi atau data menjadi kode-kode acak dengan algoritma tertentu agar informasi atau data tersebut tidak mudah untuk dibaca oleh orang lain.

Kriptografi memanfaatkan teori bilangan dalam penerapannya. Teori bilangan digunakan untuk menyusun algoritma yang dapat mengubah suatu informasi atau data. Pada makalah ini, penulis akan membahas beberapa penerapan teori bilangan dalam kriptografi.

II. LANDASAN TEORI

A. Teori Bilangan

Teori bilangan adalah cabang Matematika murni yang ditujukan untuk mempelajari bilangan bulat (*integer*) atau fungsi bernilai bilangan bulat. Bilangan bulat (*integer*) adalah bilangan yang tidak mempunyai pecahan decimal, misalnya 8, 21, -5, dan 0. Berlawanan dengan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 6.7, dan 1.9.

Pembagian pada bilangan bulat memenuhi suatu sifat, misalkan a dan b adalah bilangan bulat, dengan a tidak bernilai 0. a habis membagi b, jika terdapat bilangan bulat c sedemikian sehingga $b = ac$. Sifat pembagian tersebut ditulis dengan notasi $a \mid b$ jika $b = ac$, $c \in \boldsymbol{Z}$ dan $a \neq 0$.

Teori bilangan juga melingkupi teorema Euclidean. Teorema Eclidean memisalkan nilai m dan n adalah bilangan bulat, dan n lebih dari 0. Jika m dibagi dengan n maka hasil pembagiannya adalah q (*quotient*) dan sisanya r (*remainder*), sedemikian sehingga

$$m = nq + r$$

dengan $0 \leq r \leq n$.

Selain itu, Pembagi Bersama Terbesar (PBB) merupakan salah satu hal yang ada dalam teori bilangan. Misalkan a dan b adalah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB atau *greatest common divisor*) dari a dan b adalah bilangan bulat terbesar d sedemikian hingga $d \mid a$ dan $d \mid b$. Hal tersebut dapat dinyataka bahwa PBB(a,b) = d.

Bila dua buah bilangan bulat a dan b memenuhi pernyataan PBB(a,b) = 1, dua bilangan tersebut dikatakan relatif prima. PBB(20,3) = 1, maka 20 dan 3 relatif prima.Apabila hal tersebut dikaitkan dengan kombinasi linier, kemudian a dan b relatif prima, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$ma + nb = 1$$

PBB(a,b) dapat dinyatakan sebagai kombinasi linier a dan b dengan koefisien-koefisiennya. Misalkan a dan b adalah bilangan bulat positif, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$\text{PBB}(a,b) = ma + nb.$$

Selain itu, aritmetika modulo merupakan salah satu hal yang ada di dalam teori bilangan. Misalkan a dan m adalah bilangan bulat, dengan m lebih dari 0. Operasi $a \bmod m$ (dibaca "a *modulo* m") memberikan sisa jika a dibagi dengan m. $a \bmod m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$. m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0,1,2,..,m-1\}$.

Kemudian, kongruen juga merupakan salah satu ilmu dalam

teori bilangan. Misalkan a dan b adalah bilangan bulat dan $m > 0$, maka

$$a \equiv b \pmod{m}$$ jika dan hanya jika $m \mid (a - b)$.

Jika a tidak kongruen dengan b dalam modulus m, maka ditulis

$$a \not\equiv b \pmod{m}.$$

Misalkan m adalah bilangan bulat positif.

1) Jika $a \equiv b \pmod{m}$ dan c adalah sembarang bilangan bulat maka
   - $(a + c) \equiv (b + c) \pmod{m}$
   - $ac \equiv bc \pmod{m}$
   - $a^p \equiv b^p \pmod{m}$, p bilangan bulat tak-negatif
2) Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka
   - $(a + c) \equiv (b + d) \pmod{m}$
   - $ac \equiv bd \pmod{m}$

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 $1/a$, sedemikan sehingga $a \times \frac{1}{a} = 1$. Balikan a dilambangkan dengan a^{-1}. Di dalam aritmetika modulo, balikan modulo sebuah bilangan bulat lebih sukar dihitung. Diberikan sebuah bilangan bulat $a \pmod{m}$. Jika a dan m relatif prima dan $m > 1$, maka balikan (*invers*) dari $a \pmod{m}$ ada. Balikan dari $a \pmod{m}$ adalah bilangan bulat x sedemikian sehingga

$$xa \equiv 1 \pmod{m}$$

Dalam notasi lainnnya dapat ditulis sebagai

$$a^{-1} \pmod{m} = x.$$

Gabungan dari kongruen dan kombinasi linier adalah kekongruenan linier (*linier congruence*). Kekongruenan linier berbentuk

$$ax \equiv b \pmod{m}$$

($m > 0$, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat).

$$ax = b + km$$

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

dengan k adalah bilangan bulat yang menghasilkan x bilangan bulat.

Algoritma Euclidean meruapakan salah satu algoritma penyelesaian PBB dari dua bilangan bulat yang terkenal. Penemu algoritma ini adalah Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya dalam buku *Element*.

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

Berikut ini merupakan algoritma Euclidean yang ditulis dalam bentuk *pseudcode*.

```
procedure Euclidean(input m, n : integer,
                    output PBB : integer)
{ Mencari PBB(m, n) dengan syarat m dan n bilangan tak-
  negatif dan m ≥ n
  Masukan: m dan n, m ≥ n dan m, n ≥ 0
  Keluaran: PBB(m, n)
}
Kamus
   r : integer

Algoritma:
   while n ≠ 0 do
      r ← m mod n
      m ← n
      n ← r
   endwhile
   { n = 0, maka PBB(m,n) = m }
   PBB ← m
```

Algoritma Euclidean
Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf

Penjelasan dari algoritma tersebut sebagai berikut.

1) Jika $n = 0$ maka m adalah PBB(m, n) dan berhenti, tetapi jika $n \neq 0$, lanjutkan ke langkah 2.
2) Bagilah m dengan n dan misalkan r adalah sisanya.
3) Ganti nilai m dengan nilai n dan nilai n dengan nilai r, lalu ulang kembali ke langkah 1.

B. Kriptografi

Kriptografi merupakan fondasi yang sangat berguna dalam keamanan informasi. Kata *cryptography* berasala dari bahasa Yunani, yaitu *cryptos* dan *graphein*. *Cryptos* berarti rahasia, sedangkan *graphein* bermakna menulis, sehingga *cryptography* bermakna tulisan rahasia. Menurut Menez, Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Sedangkan menurut Schneier, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Aman di sini maksudnya adalah terjaga kerahasiaannya (*confidentiality*), terjaga keasliannya (*data integrity*), yakin pengirim pesan adalah asli (*authentication*), bukan pihak ketiga yang menyamar, dan pengirim pesan tidak dapat menyangkal (*non repudiation*) telah mengirim pesan.

Terdapat beberapa terminologi atau istilah di dalam dunia kriptografi. Berikut ini adalah terminologi umum yang ada di dalam kriptografi.

1. Pesan atau informasi yang dapat dibaca dan dimengerti maknanya, baik secara visual maupun audial.
2. Pengirim atau pihak yang mengirim pesan.
3. Penerima atau pihak yang menerima pesan.
4. *Cipherteks* atau pesan yang telah disandikan sehingga tidak bermakna lagi. Tujuan dari penyandian pesan ini agar pesan tidak dapat dibaca oleh pihak yang tidak memiliki hak.
5. Enkripsi (*encryption*) atau proses menyandikan *plainteks* menjadi *cipherteks*.
6. Dekripsi (*decryption*) atau proses mengembalikan *cipherteks* menjadi *plainteks* semula.
7. *Cipher* atau algoritma enkripsi dan dekripsi.
8. Kunci atau parameter yang digunakan di dalam enkripsi dan dekripsi.
9. Penyadap atau orang/mesin yang mencoba menangkap pesan selama proses transmisi pesan.
10. Kriptanalisis (*cryptanalysis*) atau ilmu dan seni untuk memecahkan *chiperteks* menjadi *plainteks* tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis adalah kriptanalis. Kriptanalisis dikemukakan pertama kali oleh seorang ilmuwan Arab pada Abad IX bernama Abu Yusuf Yaqub Ibnu Ishaq Ibnu As-Sabbah Ibnu ‘Omran Ibnu Ismail Al-Kindi atau yang lebih dikenal sebagai Al-Kindi.
11. Kriptologi (*cryptology*) atau studi mengenai kriptologi dan kriptanalisis.

Lukisan Al-Kindi

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

Number footnotes separately in superscripts (Insert | Footnote)[1]. Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes.

Please note that the references at the end of this document are in the preferred referencing style. Give all authors’ names; do not use “*et al*.” unless there are six authors or more. Use a space after authors' initials. Papers that have not been published should be cited as “unpublished” [4]. Papers that have been submitted for publication should be cited as “submitted for publication” [5]. Papers that have been accepted for publication, but not yet specified for an issue should be cited as “to be published” [6]. Please give affiliations and addresses for private communications [7].

C. Sejarah Kriptografi

Kriptografi telah menjadi bagian hidup dari manusia sejak lama. Dibalik kecanggihan kriptografi pada masa sekarang ini, ternyata kriptografi memilki sejarah panjang sebelum menjadi teknologi yang canggih seperti saat ini. Kriptografi pada zaman Mesir Kuno diketahui terjadi sekitar 4000 tahun yang lalu dengan menggunakan *hieroglyph* yang tidak biasa untuk menulis pesan di dinding piramida.

Kriptografi Zaman Mesir Kuno

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

Selain pada zaman Mesir Kuno, kriptografi juga terkenal pada zaman Yunani dan Romawi Kuno. Di Yunani, kriptografi seudah digunakan 400 tahun sebelum Masehi. Alat yang digunakan pada saat itu adalah *scytale*. Bangsa Arab juga memiliki sejarah tentang kriptografi, yaitu yang tertuang dalam seri buku *Arabic Origins of Cryptology* yang diterbitkan oleh King Faisal Center for Reasearch and Islamic Studies, Arab Saudi.

Kriptografi juga digunakan pada zaman India Kuno. Di India, kriptografi dgunakan untuk berkomunikasi tanpa diketahui orang lain. Bukti ini ditemukan di dala buku Kama Sutra yang menyarankan wanita untuk mempelajari seni memahami tulisan menggunakan *cipher*. Ada 2 macam *cipher*, yang pertama bernama *Kautiliyam* dan kedua *Mulavediy*.

Ternayat kriptografi juga digunakan pada zaman Renaisans di Eropa, yaitu pada abad 15 sampai abad 16. Ada beberapa *cipher* yang terkenal pada abad pertengahan, yaitu

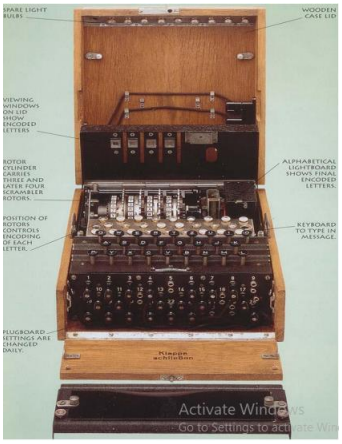
1. *Vigenere Cipher*, yaitu *cipher* yang dipublikasikan oleh diplomat Perancis bernama Blaise de Vigenere pada tahun 1586.
2. *Playfair Cipher*, yaitu *cipher* yang dipromosikan oleh diplomat Inggris yang bernama Lord Playfair. Penemu asli dari *playfair cipher* adalah Charles Wheastone pada tahun 1854.

Ternyata kriptografi ini juga mengakibatkan suatu tragedi. Pada abad ke-17 Queen Mary of Scotland dipancumg setelah pesan rahasianya dari balik penjara (pesan terenkripsi yang isinya rencana untuk membunuh Ratu Elizabeth I) pada abad pertengahan berhasil dipecahkan oleh Thomas Phelippes, seorang pemecah kode.

Lukisan Queen Mary of Scotland

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

Pada Perang Dunia II juga telah digunakan kriptografi. Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*. *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu. Keberhasilan memecahkan *Enigma* ini sering dianggap sebagai penyebab singkatnya Perang Dunia II.



Enigma

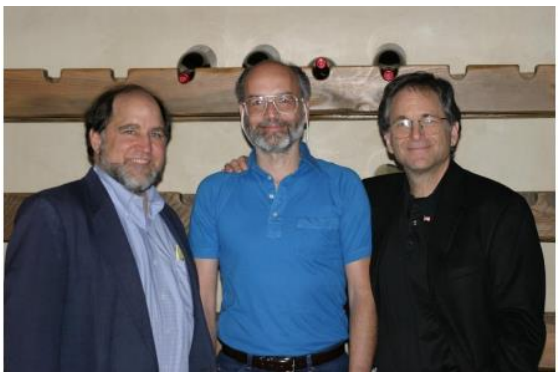
Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Pengantar-Kriptografi-(2020).pdf

III. PEMBAHASAN

Pada penerapannya, kriptografi memanfaatkan algoritma-algoritma yang didasari oleh ilmu-ilmu pada teori bilangan. Banyak algoritma yang dapat ditemukan dalam dunia kriptografi ini. Beberapa algoritma kriptografi adalah algoritma RSA, algoritma Elgamal, algorita pertukaran kunci Diffie-Hellman, dan algoritma kriptgrafi knapsack.

A. Algoritma RSA

RSA merupakan salah satu algoritma kunci public yang terkenal dan paling banyak aplikasinya. Algoritma ini ditemukan oleh 3 oang peneliti dari Massachussets Institute of Technology, yaitu Ronal Rivest, Adi Shamir, dan Len Adleman pada tahun 1976. RSA adalah singkatan dari Rivest-Shamir-Adleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan bulat yang besar menjadi factor-faktor prima.



Rivest, Shamir, dan Adleman

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Algoritma-RSA-2020.pdf

Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan bulat n factor-faktor prima (p dan q), dengan $n = p \times q$. Sekalin n berhasil difaktorkan menjadi p dan q, maka $\phi(n) = (p-1) \times (q-1)$ dapa dihitung. Selanjutnya, kunci dekripsi d dapat dihitung dari

kekongruenan $ed \equiv 1 \ (mod \phi(n))$, jika kunci enkripsi e tidak rahasia.

Penemu algoritma RSA merekomendasikan nilai p dan q panjangnya lebih dari 100 digit, sehingga hasil kali $n = p \times q$ akan berukuran lebih dari 200 digit. Algoritma pemfaktoran yang tercepat saat ini memiliki kompleksitas

$$O(\exp(\sqrt[3]{\frac{64}{9}b(\log(b)^2)}))$$

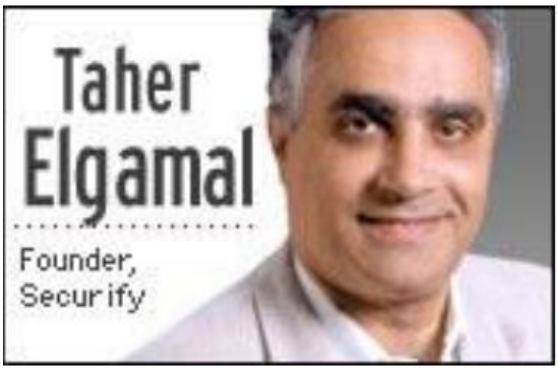
Untuk bilangan bulat n sepanjang b-bit. Hingga saat ini, makalah ini ditulis, belu ditemukan algoritma pemfaktoran bilangan bulat besar dalam waktu polynomial. Fakta inilah yang membuat algoritma RSA dianggap masih aman untuk saat ini. Semakin panjang bilangan bulatnya, maka semakin banyak waktu yang dibutuhkan untuk memfaktorkannya.

Algoritma RSA memiliki beberapa kelemahan. RSA lebih dambat daripada algoritma kriptografi kunci-simetri seperti DES dan AES. RSA tidak digunakan untuk mengenkripsi pesan, tetapi mengenkripsi kunci simetri (kunci sesi) dengan kunci publik penerima pesan. Pesan dienkripsi dengan algoritma simetri seperti DES atau AES. Pesan dan kunci simetri dalam algoritma RSA dikirim bersamaan. Peneria mendekripsi kunci simetri dengan kunci privatnya, lalu mendekripsi pesan dengan kunci simetri tersebut.

B. Algoritma Elgamal

Algoritma Elgamal dibuat oleh Taher Elgamal pada tahun 1985. Algoritma ini pertama kali dikemukakan dalam makalah berjudul "*A public key cryptosystem and a signature scheme base don discrete logarithms*". Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Masalah logaritma diskrit terjadi jika p adalah bilangan prima dan g dan y adalah sembarang bilangan bulat, sehingga x dicari dan memenuhi

$$g^x \equiv y \ (mod \ p)$$



Elgamal

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Algoritma-Elgamal-2020.pdf

Adapun prosedur enkripsi dari algoritma Elgamal adalah sebagai berikut.

1. Susun *plainteks* menjadi blok-blok.
2. Pilih bilangan acak k, yang memenuhi $1 \leq k \leq p - 2$.
3. Setiap blok dienkripsi dengan rumus

$$a = g^k \ mod \ p$$
$$b = y^k m \ mod \ p$$

Pasangan a dan b adalah cipherteks untuk blok pesan. Jadi, ukuran cipherteks 2 kali ukuran plainteksnya.

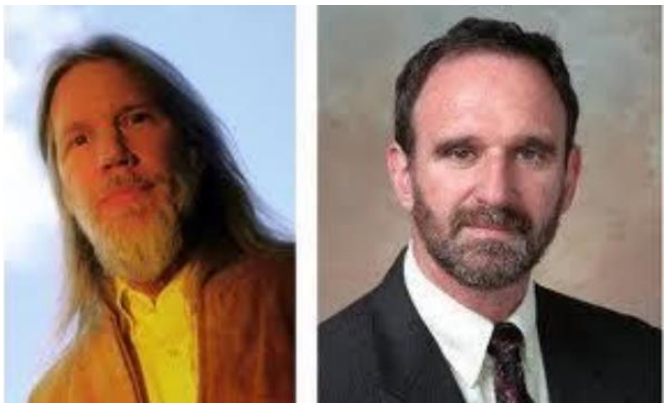
Selain itu, terdapat pula prosedur dekripsi. Prosedur dekripsi tersebut meliputi sebagai berikut.

1. Gunakan kunci privat x untuk menghitung $(a^x)^{-1} \equiv a^{p-1-x}$.
2. Hitung plainteks dengan persamaan berikut.

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

C. Algoritma Pertukaran Kunci Diffie-Hellman

Algoritma Pertukaran Kunci Diffie-Hellman dicetukan leh Whitfield Diffie dan Martin Hellman. Algoritma Pertukaran Kunci Diffie-Hellman ini digunakan untuk berbagi kunci rahasia yang sama antara dua entitas yang berkomunikasi. Kunci rahasia digunakan untuk mengenkripsi pesan dengan algoritma kriptografi kunci-simetri (DES, AES, dll). Keamanan algoritma didsarkan pada sulitnya menghitung logaritma diskrit.



Whitefield Diffie dan Martin Hellman

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Algoritma-Diffie-Hellman-2020.pdf

D. Algoritma Kriptografi Knapsack

Algoritma kriptografi *knapsack* merupakan salah satu algoritma kriptografi kunci-publik awal yang ditemukan oleh Ralph Merkle dan Martin Hellman pada tahun 1978. Algoritma ini juga disebut algoritma Merkle-Hellman. Algoritma ini didasarkan pada persoalan *knapsack problem*.

Merkle, Hellman, dan Diffie

Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Algoritma-kripto-knapsack-2020.pdf

Dalam teori algoritma, persoalan *knapsack* termasuk ke dalam NP-*complete*. Persoalan yang termasuk Np-*complete* tidak dapat dipecahkan dalam orde waktu polinomial. Ide dasar dari algoritma kriptografi *knapsack* adalah mengkodekan pesan sebagai rangkaian solusi dari persoalan *knapsack*. Setiap bobot w_i di dalam persoalan *knapsack* merupakan kunci rahasia, sedangkan bit-bit plainteks menyatakan b_i.

IV. SIMPULAN

Teori bilangan menjadi salah satu cabang Matematika yang memiliki banyak pengaplikasian. Salah satu penerapan teori bilangan yaitu algoritma dalam kriptografi. Kriptografi digunakan untuk merahasiakan suatu pesan dengan memanfaatkan algoritma atau fungsi tertentu yang dapat mengubah pesan yang awalnya bermakna menjadi tidak bermakna dengan enkripsi. Algoritma kriptografi yang memanfaatkan teori bilangan meliputi algoritma RSA, algoritma Elgamal, algoritma pertukaran kunci Diffie-Hellman, dan algoritma kriptografi *knapsack*.

V. UCAPAN TERIMA KASIH

Puji syukur penulis ucapkan kepada Tuhan Yang Maha Esa, atas berkan dan rahmat-Nya sehingga penulis dapat menyelesaikan makalah ini dengan sebaik mungkin. Terima kasih juga untuk Dra. Harlili, S., M. Sc, selaku pengajar mata kuliah IF2120 Matematika Diskrit Semester I 2020/2021 dan pembimbing dalam pembuatan makalah ini beserta para dosen pengajar IF2120 Matematika Diskrit lainnya, yaitu Fariska Zakhralativa Ruskanda, S.T., M.T., Dr. Ir. Rinaldi, M.T., dan Dr. Nur Ulfa Maulidevi, S.T., M.Sc. Saya harap ilmu yang dipelajari akan penulis gunakan dan bermanfaat di masa yang akan datang.

DAFTAR PUSTAKA

[1] Munir, Rinaldi.2020.Teori Bilangan (Bagian 1) Bahan Kuliah IF2120 Matematika Diskrit.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 9 Desember 2020).

[2] Munir, Rinaldi.2020.Kriptografi Kuliah Pengantar Bahan Kuliah IF4020 Kriptografi.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 11 Desember 2020).

[3] Munir, Rinaldi.2020.Algoritma RSA Bahan Kuliah IF4020 Kriptografi.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 11 Desember 2020).

[4] Munir, Rinaldi.2020.Algoritma Elgamal Bahan Kuliah IF4020 Kriptografi.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 11 Desember 2020).

[5] Munir, Rinaldi.2020.Algoritma Pertukaran Kunci Diffie-Hellman Bahan Kuliah IF4020 Kriptografi.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 11 Desember 2020).

[6] Munir, Rinaldi.2020.Algoritma Kriptografi Knapsack Bahan Kuliah IF4020 Kriptografi.Bandung.Prodi Informatika, Sekolah Teknik Elektro dan Informatika, (diakses pada 11 Desember 2020).

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 2020

Mgs. Tabrani (13519122)