Aplikasi Teori Bilangan dalam Kriptografi untuk Pengamanan Data

Muhammad Rifko Favian - 13521075
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13521075@itb.ac.id

***Abstract*—Pada zaman yang penuh dengan teknologi ini membuat kehidupan menjadi berubah. Diawali dengan sulitnya mencari suatu informasi, saat ini informasi dapat dicari secara mudah dan cepat dengan teknologi. Selain itu, manusia juga bisa menyimpan suatu informasi di dalam perangkat lunak atau internet dengan mudah. Namun, kita tidak ingin informasi-informasi itu sampai bocor ke pihak orang yang tidak diinginkan. Maka dari itu, dibutuhkan suatu pengaman data yang diterapkan dengan ilmu Kriptografi yang memanfaatkan materi Teori Bilangan. Penelitian ini akan melihat beberapa algoritma kriptografi dan proses enkripsi dan dekripsi data.**

***Keywords*— aes-128, kriptografi, pengaman data, teori bilangan ,**

I. PENDAHULUAN

Informasi merupakan suatu hal yang berperan penting dalam kejalanannya kehidupan kita. Tanpa informasi, kita kemungkinan besar akan tersesat dalam menentukan suatu pilihan dalam kehidupan. Informasi itu bisa kita dapat dari eksperimen diri kita sendiri, dari orang lain, atau dari suatu tempat seperti surat, berita, dan lain-lain. Beberapa informasi atau pengetahuan yang awalnya sulit didapat perlahan-lahan akan lebih mudah, karena mengikuti perkembangan zaman. Saat ini di zaman yang serba teknologi, sangat mudah mencari suatu informasi lewat perangkat lunak. Informasi itu dapat dicari lewat internet, video, dan hal lain secara mudah dan cepat.

Adanya teknologi juga memudahkan kita untuk menyimpan informasi yang besar, sulit diingat, atau sangat penting di dalam suatu perangkat lunak. Dengan itu, beberapa informasi yang sangat penting dan rahasia harus diolah agar tidak mudah diakses oleh orang lain. Kita pasti tidak mau informasi rahasia yang kita simpan di *storage*, atau internet terbuka oleh orang lain yang bahkan tidak kita kenal.

Oleh karena itu, para pengembang teknologi mencari cara atau metode yang dapat digunakan untuk mengamankan informasi atau data tersebut saat disimpan. Pencarian terus dilakukan sampai ditemukan suatu metode untuk mengolah atau memanipulasi data yang dinamakan ilmu Kriptografi. Metode Kriptografi ini memanfaatkan suatu materi yang dinamakan Teori Bilangan.

Berdasarkan latar belakang tersebut, penulis memiliki ide untuk membuat makalah yang berjudul "Aplikasi Teori Bilangan dalam Kriptografi untuk Pengamanan Data" yang akan membahas bagaimana contoh penerapan teori bilangan dalam kriptografi sebagai pengaman data.

II. LANDASAN TEORI

A. Teori Bilangan

1. Bilangan Bulat

Teori bilangan adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (integer) atau fungsi bernilai bilangan bulat. Bilangan bulat adalah bilangan yang tidak mempunyai pecahan decimal. Contoh dari bilangan bulat sendiri ialah 1,4,10,-1,-12,0. Berlawanan dengan bilangan bulat adalah bilangan riil yang mempunyai titik desimal, seperti 8.0, 34.25, 0.02.

2. Sifat Pembagian pada Bilangan Bulat

Misal terdapat a dan b yang di mana $a \neq 0$. a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga $b = ac$. Sifat pembagian ini dapat ditulis dalam bentuk notasi

$a \mid b$ jika $b = ac$, $c \in Z$ (Z adalah bilangan bulat) dan $a \neq 0$.

Contohnya $4 \mid 8$ karena $8/4 = 2$ (bilangan bulat) atau $8 = 4 \times 2$.

3. Teorema Euclidean

Teorema 1 (Teorema Euclidean)

Misalkan m dan n bilangan bulat, $n > 0$. Jika m dibagi dengan n maka hasil pembagiannya adalah q (quotient) dan sisanya r (remainder), sedemikian sehingga

$$m = nq + r$$

dengan syarat

$$0 \leq r < n$$

Contoh : (i) $25/4 = 6$, sisa 1

$$25 = 6 \cdot 4 + 1$$

(ii) $-25/4 = -7$, sisa 3

$$-25 = -7 \cdot 4 + 3$$

Perlu diingat bahwa $0 \leq r < n$, di mana r adalah sisa bagi, maka nilai r tidak boleh di bawah 0.

(iii) $-25/4 = -6$, sisa -1 (salah!!)

4. Pembagi Bersama Terbesar (PBB)

Misalkan a dan b bilangan bulat tidak nol. Pembagi bersama terbesar (PBB) dari a dan b adalah bilangan bulat terbesar d sedemikian hingga

$$d \mid a \text{ dan } d \mid b.$$

Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

Contohnya PBB(6,18) = 6, karena 6 adalah bilangan bulat terbesar yang memenuhi 6 | 6 dan 6 | 18.

Teorema 2.

Misalkan m dan n bilangan bulat, dengan syarat n > 0 sedemikian sehingga

$$m = nq + r,$$
$$0 \le r < n$$

maka PBB(m, n) = PBB(n, r).

Algoritma Euclidean Mencari PBB

Diberikan dua buah bilangan bulat tak-negatif m dan n (m ≥ n), maka dengan teorema-teorema yang telah dijelaskan sebelumnya, dapat dicari PBB dengan langkah-langkah berikut :

1. Jika n = 0 maka m adalah PBB(m, n);
   tetapi jika n ≠ 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.

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

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

Maka didapat :

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

Contoh : m = 76, n = 16 dan dipenuhi syarat m ≥ n

$$76 = 4 \cdot 16 + 12$$
$$16 = 1 \cdot 12 + 4$$
$$12 = 3 \cdot 4 + 0$$

Maka didapat :

$$PBB(76,16) = PBB(16,12) = PBB(12,4) = PBB(4,0) = 4$$

Algoritma Euclidean merupakan salah satu algoritma yang cukup terkenal. Penemu dari algoritma ini adalah Euclides, seorang matematikawan Yunani yang menuliskan algoritmanya tersebut dalam buku, Element.

Gambar 1. Lukisan Euclides
(Sumber : https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf)

5. Kombinasi Linier

PBB(a,b) dapat dinyatakan sebagai kombinasi linier (linear combination) a dan b dengan koefisien-koefisennya.

Contoh

$$PBB(80, 12) = 4 ,$$
$$4 = (-1) \cdot 80 + 7 \cdot 12$$

Teorema 3.

Misalkan a dan b bilangan bulat positif, maka terdapat bilangan bulat m dan n sedemikian sehingga

$$PBB(a, b) = ma + nb$$

Untuk mencari nilai m dan n menggunakan algoritma euclidean dan penyusunan mundur.

Contoh : Nyatakan PBB(76, 16) sebagai kombinasi linier dari 76 dan 16.

- Melakukan pencarian PBB(76,16)

$$76 = 4 \cdot 16 + 12 \quad (i)$$
$$16 = 1 \cdot 12 + 4 \quad (ii)$$
$$12 = 3 \cdot 4 + 0 \quad (iii)$$
$$PBB(76,16) = 4$$

- Kemudian dilakukan penyusunan :
  - Susun pembagian no (ii) dan (i) menjadi
    $4 = 16 - 1 \cdot 12$ (iv)
    $12 = 76 - 4 \cdot 16$ (v)
  - Sulihkan no (v) ke dalam no (iv) menjadi
    $4 = 16 - 1 \cdot (76 - 4 \cdot 16) = 5 \cdot 16 - 1 \cdot 76$
  - Jadi, $PBB(76, 16) = 4 = 5 \cdot 16 - 1 \cdot 76$

6. Relatif Prima

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

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

Contoh :

(i) 20 dan 3 relatif prima sebab PBB(20, 3) = 1.

(ii) 16 dan 4 tidak relatif prima sebab PBB(16, 4) = 4 ≠ 1.

7. Aritmatika Modulo

Misalkan a dan m bilangan bulat (m > 0). Operasi **a mod m** (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Modulo ini dapat ditulis dalam bentuk notasi

$$a \bmod m = r$$

sedemikian sehingga

$$a = mq + r,$$

dengan

$$0 \le r < m.$$

m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan {0, 1, 2, …, m – 1}.

Contoh :

- 23 mod 5 = 3
- 28 mod 7 = 0

- –41 mod 9 = –5 (salah!!)
- –41 mod 9 = 4 (benar)

8. Kongruen

Misalnya 38 mod 5 = 3 dan 13 mod 5 = 3, maka dikatakan 38 ≡ 13 (mod 5), dibaca 38 kongruen dengan 13 dalam modulus 5.

Secara definisi, Misalkan a dan b bilangan bulat dan m adalah bilangan > 0, maka a ≡ b (mod m) jika dan hanya jika m | (a – b).

Jika a tidak kongruen dengan b dalam modulus m, maka ditulis a ≡ b (mod m) .

Teorema 4.

Misalkan m adalah bilangan bulat positif.

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

9. Balikan Modulo (Invers Modulo)

Di dalam aritmetika bilangan riil, balikan sebuah bilangan yang tidaknol adalah bentuk pecahannya sedemikian sehingga hasil perkalian keduanya sama dengan 1. Jika a adalah sebuah bilangan tidak-nol, maka balikannya adalah 1/a sedemikian sehingga a × 1/a = 1, seperti balikan 4 adalah 1/4, sebab 4 × 1/4 = 1.

Balikan a dilambangkan dengan a^{-1}.

Di dalam aritmetika modulo, balikan modulo sebuah bilangan bulat lebih sukar dihitung.

Diberikan sebuah bilangan bulat a(mod m). Bagaimana menghitung balikan a (mod m)? Syaratnya adalah jika a dan m relatif prima dan m > 1, maka balikan dari a (mod m) ada.

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

$$x \cdot a \equiv 1 \pmod m$$

Notasinya dapat ditulis sebagai :

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

Bukti : a dan m relatif prima, jadi PBB(a, m) = 1, dan terdapat bilangan bulat x dan y sedemikian sehingga :

$$x \cdot a + y \cdot m = 1$$

yang mengimplikasikan bahwa

$$x \cdot a + y \cdot m \equiv 1 \pmod m$$

karena $y \cdot m \equiv 0 \pmod m$, maka

$$x \cdot a \equiv 1 \pmod m$$

Kekongruenan yang terakhir ini berarti bahwa x adalah balikan dari a (mod m).

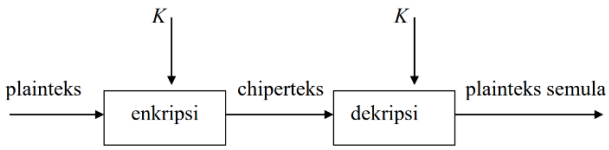
B. Kriptografi

1. Definisi, Istilah, dan Konsep Kriptografi

Istilah *kriptografi* berasal dari bahasa Yunani, *kryptos* yang berarti "rahasia, tersembunyi", dan *graphos* yang berarti "tulisan". Secara etimologi, kriptografi dapat diartikan sebagai "secret writing" atau "tulisan rahasia". Istilah kriptografi mengarah kepada aktivitas dalam merencanakan cara yang aman untuk berkomunikasi secara rahasia antara dua atau lebih pihak, dan untuk melakukan cara-cara yang dimaksud merupakan tugas dari pihak-pihak tersebut. Pihak-pihak tersebut dapat disebut sebagai *kriptografer*.

Kriptografi adalah teknik untuk menyamarkan dan memproteksi pesan. Pesan yang asli disebut teks-asal (*plaintext*), pesan yang disamarkan disebut teks-sandi (*ciphertext*).

Persoalan utama di dalam kriptografi adalah bagaimana cara pihak satu, yang disebut "*pengirim*", mengirimkan pesan ke pihak lainnya, yang disebut "*penerima*", dengan berbagai cara yang dilakukan sehingga tidak ada pihak lain yang dapat mengetahui isi pesan tersebut. Pihak lain yang dimaksud yaitu *musuh* atau *lawan* yang ingin tahu isi pesan yang asli. Dalam hal ini, pengirim mengubah teks-asal menjadi bentuk lain yang tidak mudah dipahami yang disebut teks-sandi. Proses ini disebut *enkripsi*. Sedangkan proses yang sebaliknya disebut *dekripsi*, yaitu proses mengubah teks-sandi menjadi teks-asal. Untuk melakukan enkripsi dan dekripsi diperlukan kunci (*key*). Kunci ini sangat penting dan rahasia.



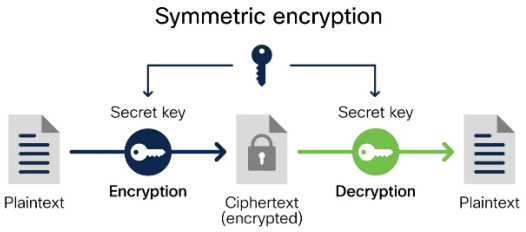
Gambar 2. Konsep Kriptografi Secara Umum
(Sumber :
https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf)

2. Algoritma Kriptografi

Secara umum algoritma kriptografi dapat dibagi menjadi 3 jenis, yaitu *Symmetric Key Cryptography*, *Asymmetric Key Cryptography*, dan *Hash Function*.

1. Symmetric Key Cryptography

Disebut juga *Private* atau *Secret Key Cryptography*. Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi maupun dekripsi. Algoritma ini sudah ada sejak lebih dari 4000 tahun yang lalu. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang terkirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan.



Gambar 3. Konsep *Symmetric Key Cryptography*
(Sumber : https://www.cisco.com/c/en/us/products/security/encryption-explained.html)

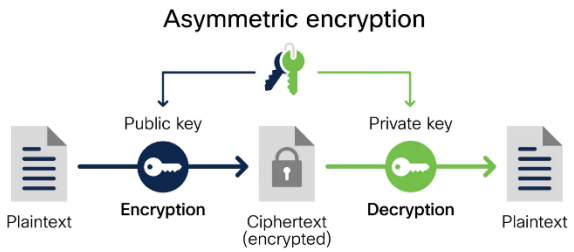
Algoritma yang memakai kunci simetri di antaranya adalah :
- *Data Encryption Standard* (DES)
- RC2, RC4, RC5, RC 6
- *International Data Encryption Algorithm* (IDEA)
- *Advanced Encryption Standard* (AES)
- *On Time Pad* (OTP)
- A5, dan lain sebagainya.

2. Asymmetric Key Cryptography

Disebut juga *Public-key Cryptography*. Maksud dari nama jenis ini, kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri ini, kunci terbagi menjadi dua bagian, yaitu :

1) Kunci umum (*public key*), kunci yang boleh semua orang tahu (dipublikasikan).
2) Kunci rahasia (*private key*), kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan *public-key* orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsikannya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsikan pesan tersebut. Algoritma asimetri bisa mengirimkan pesan dengan lebih aman daripada algoritma simetri.

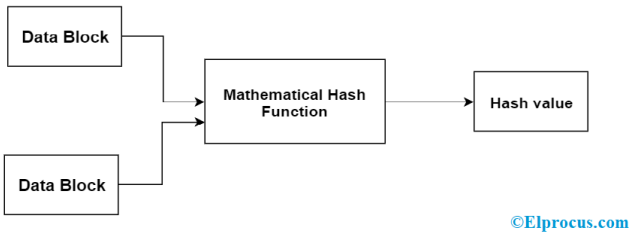


Gambar 4. Konsep *Asymmetric Key Cryptography*
(Sumber : https://www.cisco.com/c/en/us/products/security/encryption-explained.html)

Algoritma yang memakai kunci public di antaranya adalah :
- *Digital Signature Algorithm* (DSA)
- *RSA*
- *Diffle-Hellman* (DH)
- *Elliptic Curve Cryptography* (ECC)
- Kriptografi Quantum, dan lain sebagainya.

3. Hash Function

Fungsi Hash sering disebut dengan fungsi satu arah (*one-way function*), *message digest*, *fingerprint*, fungsi kompresi dan *message authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi Hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan tersebut benar-benar berasal dari orang-orang yang diinginkan.



Gambar 5. Konsep *Hash Function*
(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. Aplikasi Kriptografi dalam Pengamanan Data

A. Algoritma RSA

Algoritma kriptografi RSA merupakan algoritma kriptografi kunci public (asimetris). Ditemukan pertama kali pada tahun 1977 oleh R. Rivest, A. Shamir, dan L. Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci public, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci rahasia hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Algoritma kriptografi RSA terdiri dari tiga proses, yaitu proses ekspansi kunci, proses enkripsi dan proses dekripsi.

Ekspansi Kunci

1) Pilih dua bilangan prima, misalkan p (rahasia) dan q (rahasia).
2) Hitung n = pq (tak-rahasia)
3) Hitung m = (p-1)(q-1) (rahasia)
4) Pilih sebuah bilangan bulat untuk kunci publik, misal e, yang relatif prima terhadap m, yaitu PBB(m, e) = 1.

Enkripsi Pesan

$$p_t^e \equiv c \pmod{n} \Leftrightarrow c = p_t^e \bmod n$$

Dengan c adalah sub-bagian kode enkripsi yang terbentuk dan p_t adalah potongan beberapa karakter pada kode enkripsi atau representasi bilangan bulat dari karakter-karakter sebenarnya yang panjangnya tetap.

Dekripsi Pesan

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

$$c^d \equiv p_t \pmod{n} \Leftrightarrow p_t = c^d \bmod n$$

dengan d merupakan kunci dekripsi.

Berikut merupakan kode enkripsi pada kata "MATDIS". Misalkan tiap karakter pada kata "MATDIS" direpresentasikan dengan kode ASCII sehingga menjadi 776584687383.

1) Misal, p = 59 dan q = 41
2) n = pq = 2419.
3) m = (p-1)(q-1) = 2320
4) Ambil e = 3 karena PBB(2320, 3) = 1.
5) Enkripsi :
   Misal pt merepresentasikan blok-blok plainteks hasil representasi kode ASCII sehingga
   $pt_1 = 776$ $pt_3 = 687$
   $pt_2 = 584$ $pt_4 = 383$
   $c_1 = 776^3 \ mod\ 2419 = 670$
   $c_2 = 584^3 \ mod\ 2419 = 1082$
   $c_3 = 687^3 \ mod\ 2419 = 2362$
   $c_4 = 383^3 \ mod\ 2419 = 612$
   Maka kode enkripsi yang dihasilkan adalah 670 1082 2362 612

B. Algoritma AES-128

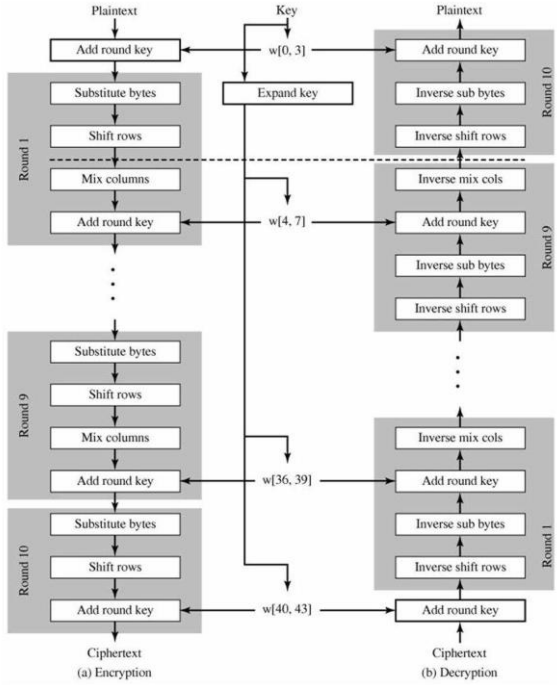
Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256. Masing-masing tipe menggunakan kunci internal yang berbeda yaitu round key untuk setiap proses putaran.

Proses putaran enkripsi AES-128 dikerjakan sebanyak 10 kali, yaitu sebagai berikut :

1. AddRoundKey
2. Putaran sebanyak 9 kali, proses yang dilakukan pada setiap putaran adalah: *SubstituteBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*
3. Final round, adalah proses untuk putaran terakhir yang meliputi *SubBytes*, *ShiftRows*, dan *AddRoundKey*.

Sedangkan pada proses dekripsi AES-128, proses putaran juga dikerjakan sebanyak 10 kali, yaitu sebagai berikut :

1. AddRoundKey
2. Putaran sebanyak 9 kali, dimana pada setiap putaran dilakukan proses: *InverseShiftRows*, *InverseSubstituteBytes*, *AddRoundKey*, dan *InverseMixColumns*.
3. Final round, adalah proses untuk putaran terakhir yang meliputi *InverseShiftRows*, *InverseSubBytes*, dan *AddRoundKey*.



Gambar 6. Konsep Enkripsi dan Dekripsi AES-128
(Sumber : http://studyinformatics.blogspot.com/2012/07/aes-advanced-encryption-standard.html)

Contoh misal kita enkripsi kata "MATDIS" dengan key "MatematikaDiskri", maka hasil enkripsi nya ialah "NTxYzu70O44iJXldcTTfBQ=="

IV. KESIMPULAN

Teori bilangan merupakan materi cabang matematika yang mempelajari tentang bilangan integer dan bilangan bulat. Banyak aplikasi-aplikasi yang dapat diterapkan dari materi teori bilangan ini. Salah satu aplikasinya adalah ilmu Kriptografi. Kriptografi ini merupakan ilmu yang mempelajari cara mengubah suatu pesan atau informasi yang memiliki arti ke yang tidak memiliki arti dan juga sebaliknya. Kriptografi ini sangat bermanfaat dalam teknologi, karena tujuan dari Kriptografi ini adalah untuk meningkatkan keamanan dan mencegah terjadinya kebocoran data atau informasi yang tidak ingin tersebar ke orang lain. Kriptografi memiliki banyak algoritma-algoritma yang bisa digunakan, dan algoritma yang lebih baik yang mana yang dipakai itu tergantung penggunaannya untuk apa.

V. PENUTUP

Di akhir penghujung makalah ini, penulis ingin mengucapkan terima kasih sebanyak-banyaknya kepada beberapa pihak yang telah membantu penulis dalam menyelesaikan makalah ini :

1) Tuhan yang Maha Esa atas anugerah dan rahmat-Nya, penulis dapat menyelesaikan makalah ini dengan baik.
2) Dr. Nur Ulfa Maulidevi, S.T, M.Sc., selaku dosen kelas K1 karena sudah membimbing penulis dengan sangat baik selama perkuliahan Matematika Diskrit berjalan.
3) Seluruh tim dosen mata kuliah Matematika Diskrit yang

telah berperan dalam memberi wadah pembelajaran kepada penulis dan mahasiswa lainnya.

REFERENSI

[1] Munir, Rinaldi, 2020. "Teori Bilangan (Bagian 1)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian1.pdf. Diakses 08 Desember 2022

[2] Munir, Rinaldi, 2020. "Teori Bilangan (Bagian 3)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2020-2021/Teori-Bilangan-2020-Bagian3.pdf. Diakses 08 Desember 2022

[3] Kriptografi #2 (Macam-macam Algoritma Kriptografi). http://gilang-kurniawan.blogspot.com/2012/05/kriptografi-2-macam-macam-algoritma.html. Diakses pada 10 Desember 2022

[4] Rebu, Marselinus Junardi. 2015. *Kriptografi Klasik*. Yogyakarta: Universitas Sanata Dharma

[5] What Is Encryption?. https://www.cisco.com/c/en/us/products/security/encryption-explained.html. Diakses pada 11 Desember 2022

[6] What is Cryptography : Types, Tools and Its Algorithms. https://www.elprocus.com/cryptography-and-its-concepts/. Diakses pada 11 Desember 2022

[7] Algoritma RSA. https://komputerkata.com/algoritma-rsa/. Diakses pada 12 Desember 2022

[8] AES -Advanced Encryption Standard-. http://studyinformatics.blogspot.com/2012/07/aes-advanced-encryption-standard.html. Diakses pada 12 Desember 2022

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

Muhammad Rifko Favian, 13521075