Teori Bilangan dalam Ilmu Kriptografi

Farhan Yusuf Akbar and 13519202[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13519202@std.stei.itb.ac.id

***Abstract*—Teori Bilangan memainkan peran penting dalam Ilmu Kriptografi. Kriptografi adalah praktik menyembunyikan informasi dengan mengubah beberapa informasi rahasia menjadi teks yang tidak bisa dibaca. Makalah ini bertujuan untuk mengenalkan pembaca kepada aplikasi Teori Bilangan dalam kriptografi. Banyak *tools* dalam Teori Bilangan seperti bilangan prima, pembagi, PBB, kongruensi dan fungsi Euler's 'ϕ' yang digunakan dalam kriptografi. Penulis secara singkat akan menjelaskan ide enkripsi/dekripsi dalam *Caesar chipering* dan RSA *public key cryptography*.**

***Keywords*—Enkripsi, Euler, Informasi, Kriptografi .**

I. Latar Belakang

Selama ribuan tahun manusia telah mencari cara untuk mengirim pesan secara rahasia. Pada zaman dahulu, seorang raja seringkali perlu mengirim pesan rahasia kepada jenderalnya dalam masa pertempuran. Untuk mengirim pesan tersebut, Raja akan mengambil seorang pelayan, mencukur rambutnya, dan menulis pesan di kepalanya. Dia menunggu rambut pelayan itu tumbuh kembali dan kemudian mengirimnya. Jenderal kemudian mencukur kepala pelayan dan membaca pesan itu. Jika musuh menangkap pelayan tersebut, mereka mungkin tidak akan terpikir untuk mencukur rambut kepalanya dan pesan raja akan tetap aman.

Kriptografi berasal dari bahasa Yunani dengan memadukan dua kata, yaitu *kryptos* dan *graphein*. *Kryptos* berarti tersembunyi atau rahasia, sedangkan *graphein* memiliki arti menulis. Makna kriptografi secara harfiah ialah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya. Tujuan dari ilmu kriptografi adalah melakukan berbagai upaya komunikasi antar individu atau kelompok secara aman tanpa kehadiran pihak-pihak yang tidak diinginkan. Pun salah satu tujuannya yang lain ialah menganalisis komunikasi yang sulit dipahami.

Ilmu kriptografi telah membantu kehidupan manusia dalam bertukar pesan rahasia atau memecahkan pesan rahasia untuk kepentingan tertentu. Dalam aplikasinya, kriptografi ini menggunakan konsep dalam Teori Bilangan yang akan dibahas dalam makalah ini.

II. Dasar Teori

A. Teori Bilangan

Teori Bilangan adalah cabang matematika murni yang ditujukan untuk mempelajari bilangan bulat (*integer*) atau fungsi bernilai bilangan bulat. Berikut adalah konsep-konsep dasar dari teori bilangan

1. Pembagi

   Pembagi (atau faktor) dari bilangan a adalah bilangan b yang membagi a. Untuk bilangan bulat, biasanya hanya pembagi positif yang diperhitungkan, meskipun jelas pembagi negatif itu sendiri adalah pembagi. b habis membagi a (b *divides* a) jika terdapat bilangan bulat c sedemikian sehingga a = bc. Notasi :

   $$b \mid a \text{ jika } a = bc,\ c \in Z \text{ dan } b \neq 0.$$

   Tabel berikut memuat pembagi dari beberapa bilangan bulat positif pertama.

n	pembagi
1	1
2	1,2
3	1,3
4	1,2,4
5	1,5
6	1,2,3,6
7	1,7
8	1,2,4,8
9	1,3,9
10	1,2,5,10
11	1,11
12	1,2,3,4,6,12
13	1,13
14	1,2,7,14

2. Bilangan prima

   Bilangan prima (atau bilangan bulat prima) adalah bilangan bulat positif yang lebih besar dari 1 dan tidak memiliki pembagi bilangan bulat positif selain 1 dan bilangan itu sendiri. Lebih tepatnya, bilangan prima p adalah bilangan bulat positif yang memiliki tepat satu pembagi positif selain 1, yang berarti bilangan tersebut tidak dapat difaktorkan. Contoh : satu-satunya pembagi dari 13 adalah 1 dan 13, sehingga 13 menjadi bilangan prima, sedangkan bilangan 24 memiliki pembagi 1, 2, 3, 4, 6, 8, 12, dan 24 (sesuai dengan faktorisasi 24 = 2 ^ 3 · 3), menjadikan 24 bukan bilangan prima. Bilangan bulat positif selain 1 yang bukan bilangan prima disebut bilangan komposit.
3. Pembagi Bersama Terbesar (PBB)

Pembagi Bersama Terbesar (PBB) atau *Greatest Common Divisor* (GCD) atau juga disebut pembagi persekutuan tertinggi (Hardy dan Wright, 1979:20) dari dua bilangan bulat positif a dan b adalah pembagi terbesar bersama untuk a dan b. Misalnya, PBB (3,5) = 1, PBB(12,60) = 12, dan PBB (12,90) = 6. Pembagi persekutuan terbesar PBB (a,b,c,...) juga dapat ditentukan untuk tiga atau lebih bilangan bulat positif sebagai pembagi terbesar yang dimiliki oleh semuanya. Dua atau lebih bilangan bulat positif yang memiliki pembagi persekutuan terbesar 1 dikatakan relatif prima satu sama lain.

4. Relatif Prima

   Dua buah bilangan bulat a dan b dikatakan relatif prima jika PBB(a, b) = 1.

   - 20 dan 3 relatif prima sebab PBB(20, 3) = 1.
   - 7 dan 11 relatif prima karena PBB(7, 11) = 1.
   - 20 dan 5 tidak relatif prima sebab PBB(20, 5) = 5 ≠ 1

5. Aritmatika Modulo

   Misal a dan m adalah bilangan bulat (m > 0). Operasi a mod m (dibaca "a modulo m") menghasilkan sisa (*remainder*) jika a dibagi dengan m. m disebut modulus atau modulo dan hasil aritmetika modulo m terletak di dalam himpunan {0, 1, 2, …, m – 1}. Notasi:

   a mod m = r sedemikian sehingga a = mq + r,
   dengan 0 ≤ r < m

   Untuk kasus a negatif, bagi |a| dengan m. Akan didapat sisa r'. Maka a mod m = m – r' bila r' ≠ 0. Hasi |– 41| mod 9 adalah 5, sehingga –41 mod 9 = 9 – 5 = 4. Beberapa contoh hasil operasi dengan operator modulo ditunjukkan sebagai berikut:

   - 23 mod 5 = 3
   - 27 mod 3 = 0
   - 6 mod 8 = 6
   - 0 mod 12 = 0
   - -41 mod 9 = 4
   - -39 mod 13 = 0

6. Kongruensi

   Misal 38 mod 5 = 3 dan 13 mod 5 = 3, maka dikatakan 38 ≡ 13 (mod 5) (dibaca: 38 kongruen dengan 13 dalam modulus 5). Pada kehidupan sehari-hari dalam menggunakan jam, kita mengenal

   - jam 14.00 = jam 2 siang → 14 ≡ 2 (mod 12)
   - jam 18.00 = jam 6 sore → 18 ≡ 6 (mod 12)
   - jam 21.00 = jam 9 malam → 21 ≡ 9 (mod 12)
   - jam 24.00 = jam 0 → 24 ≡ 0 (mod 12).

   Misalkan a ≡ a' (mod m) dan b ≡ b' (mod m), maka sifat penting kongruensi meliputi berikut ini, di mana tanda "=>" berarti "implikasi":

   - *Equivalence*: a ≡ b (mod 0) => a = b
   - *Determination*: menetukan apakah a ≡ b (mod m) atau a≢b (mod m)
   - *Reflexivity*: a ≡ a (mod m)
   - *Symmetry*: a ≡ b (mod m) => b ≡ a (mod m)
   - *Transitivity*: a ≡ b (mod m) dan b ≡ c (mod m) => a ≡ c (mod m)
   - a + b ≡ a' + b' (mod m)
   - a - b ≡ a' - b' (mod m)
   - ab ≡ a'b' (mod m)
   - a ≡ b (mod m) => ka ≡ kb (mod m)
   - a ≡ b (mod m) => a^n ≡ b^n (mod m)
   - a ≡ b (mod m1) dan a ≡ b (mod m2) => a ≡ b (mod [m1, m2]), di mana [m1, m2] adalah kelipatan persekutuan terkecil
   - ak ≡ bk (mod m) => a ≡ b (mod m / ((k, m))), di mana (k, m) adalah pembagi bersama terbesar
   - Jika a ≡ b (mod m), maka P (a) ≡ P (b) (mod m), untuk P (x) sebuah polinomial

7. Fungsi Totient Euler

   Sebuah fungsi aritmatika, fungsi Totient Euler 'ϕ' didefinisikan sebagai ϕ(n) = jumlah bilangan bulat positif yang kurang atau sama dengan n dan relatif prima dengan n. Dapat juga diartikan ϕ(n) = jumlah bilangan bulat positif a dimana 1 ≤ a ≤ n dan PBB(a,n) = 1. Fungsi ϕ(mn) dapat dipecah menjadi ϕ(m) ϕ(n) dimana m dan n relatif prima.

   Contoh: ϕ(15) = 8, karena bilangan bulat positif yang kecil dari 15 dan relatif prima terhadap 15 adalah 1,2,4,7,8,11,13, dan 14. Semuanya berjumlah 8 bilangan.

B. Kriptografi

Kriptografi adalah ilmu menjaga keamanan informasi dengan mengubahnya menjadi bentuk yang tidak dapat dipahami oleh penerima yang tidak diinginkan. Dalam kriptografi, pesan asli yang dapat dibaca manusia, disebut sebagai *plaintext*, diubah dengan menggunakan algoritma dan rangkaian operasi matematika tertentu menjadi sesuatu yang bagi pengamat awam akan terlihat seperti *gibberish* atau pesan tidak berarti. Teks tidak memiliki arti ini disebut *ciphertext*.

Sistem kriptografi memerlukan beberapa metode agar penerima yang dituju dapat menggunakan pesan terenkripsi. Penerima pesan dapat menggunakan pesannya setelah *ciphertext* diubah ke *plaintext* kembali. Enkripsi adalah apa yang kita sebut sebagai proses mengubah *plaintext* menjadi *ciphertext*. Enkripsi adalah bagian penting dari kriptografi. Lawan dari enkripsi adalah dekripsi. Dekripsi adalah proses mengubah *ciphertext* menjadi *plaintext*.

Salah satu aspek penting dari proses enkripsi adalah algoritma dan *key*. *Key* adalah sebuah informasi, biasanya berupa angka, yang menentukan bagaimana algoritma diterapkan ke *plaintext* untuk mengenkripsinya. Meskipun kita tahu metode enkripsi beberapa pesan, sulit bahkan tidak mungkin untuk mendekripsi tanpa *key* itu.

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

kriptografi.

1. *Secret key cryptography*.

   Caesar cipher adalah contoh dari *secret key cryptography*. Jika pesan terenkripsi dipertukarkan antara Caesar dan salah satu perwiranya, kedua belah pihak harus mengetahui *key*-nya, dalam hal ini *key*-nya adalah berapa banyak huruf maju atau mundur dalam alfabet yang perlu dipindahkan untuk mengubah *plaintext* menjadi *ciphertext* atau sebaliknya. Tetapi *key* tersebut harus tetap menjadi rahasia di antara mereka berdua. Caesar dan perwiranya tidak dapat mengirim *key* bersama dengan pesannya, karena jika keduanya jatuh ke tangan musuh, pesan tersebut akan dengan mudah dipecahkan, sehingga tujuan enkripsi pesan menjadi sia-sia. Caesar dan perwiranya hanya bisa bertukar *key* ketika mereka bertemu satu sama lain secara langsung, meskipun jelas ini kurang ideal ketika perang terjadi dalam jarak yang jauh.

   Secret key cryptography banyak 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* rahasia. *Secret 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 teknik dan algoritma yang menggunakan kriptografi jenis ini adalah sebagai berikut.

   - Triple DES
   - Advanced Encryption Standard (AES)
   - Blowfish

2. *Public key cryptography*

   Caesar mungkin dapat berunding dengan perwiranya secara langsung, tetapi kita pasti tidak ingin repot-repot pergi ke bank dan meminta teller untuk memberi *private key* agar bisa mengenkripsi komunikasi elektronik kita dengan bank, itu akan menghilangkan tujuan perbankan online. Permasalah ini dapat diselesaikan dengan *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, dibagikan kepada siapa pun yang perlu untuk mendekripsi pesan-pesan itu. Sebagai metafora, anggap *key* publik seperti membuka celah di kotak surat agar orang-orang dapat memasukkan surat. Kita memberikan kebebasan kepada siapa saja yang menurut kita mungkin akan mengirimi surat. *Key* pribadi adalah apa yang kita gunakan untuk membuka kotak surat sehingga kita bisa mengeluarkan surat-surat itu.

   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.

   Perhitungan yang diperlukan untuk *public key cryptography* jauh lebih kompleks dan menghabiskan sumber daya daripada *secret key cryptography*. Untungnya kita tidak perlu menggunakannya untuk melindungi setiap pesan yang kita kirim secara online.

   Public key cryptography membantu menjaga kerahasiaan. *Public key cryptography* ini juga merupakan bagian dari serangkaian fungsi yang lebih besar, dikenal sebagai *public key infrastructure* (PKI). PKI memastikan bahwa *key* publik tertentu diasosiasikan dengan orang atau lembaga tertentu. Sebuah pesan yang dienkripsi dengan *key* publik akan terkonfirmasi identitas pengirimnya.

   Beberapa teknik dan algoritma yang menggunakan kriptografi jenis ini adalah sebagai berikut:

   - Diffie-Hellman key exchange
   - RSA
   - ElGamal

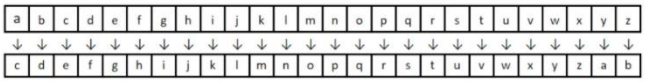
3. Fungsi hash

   Algoritma *public key cryptography* dan *secret key cryptography* melibatkan transformasi *plaintext* menjadi *ciphertext* dan kemudian kembali menjadi *plaintext*. Sebaliknya, fungsi hash adalah algoritma enkripsi satu arah. 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). Ini membuat algoritma hashing menjadi alat yang hebat untuk memastikan integritas data. Misalnya sebuah pesan dikirim beserta hashnya. Setelah menerima pesan, kita dapat menjalankan algoritma hashing yang sama pada teks pesan. Jika hash yang dihasilkan berbeda dari hash yang menyertai pesan, kita tahu pesan tersebut telah dimodifikasi saat sedang dikirim.

   Hashing juga digunakan untuk memastikan kerahasiaan kata sandi. Menyimpan kata sandi sebagai *plaintext* adalah kesalahan besar yang tidak boleh dilakukan karena itu membuat pengguna rentan terhadap pencurian akun dan identitas melalui pembobolan data. Jika kita menyimpan versi hash dari kata sandi pengguna, peretas tidak akan dapat mendekripsi dan menggunakannya di tempat lain bahkan jika mereka berhasil menembus pertahanan kita. Ketika pengguna yang sah masuk dengan kata sandi mereka, kita dapat memeriksa hash yang kita miliki di file.

III. Implementasi Teori Bilangan dalam Kriptografi

A. Caesar Cipher Key Cryptography



Sumber : https://windsongtraining.ca/encryption-part-1-the-caesar-cipher/

Salah satu sistem kriptografi tertua digunakan oleh kaisar romawi Julius Caesar. *Plaintext* diubah ke *ciphertext* dengan mensubstitusikan setiap huruf dengan huruf alphabet yang ada di bawahnya, seperti pada gambar di atas. Contoh:

NUMBER THEORY IS EASY -> *plaintext*
QXPEHU WKHRUB LV HDVB -> *ciphertext*

Dengan konsep kekongruenan/kongruensi, inti dari *Caesar cipher* ini dengan mudah dijelaskan. Setiap huruf pada alfabet dikorespondensikan dengan urutan bilangan bulat tertentu seperti berikut.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Sumber : https://www.ques10.com/p/47687/substitution-cipher-in-cryptography-1/

Jika P adalah *plaintext* dan C adalah *ciphertext*, maka metode enkripsi *Caesar cipher* dapat dijelaskan dengan persamaan C ≡ P + 3 (mod 26). Contoh :

N	U	M	B	E	R		T	H	E	O	R	Y		I	S		E	A	S	Y
13	20	12	1	4	17		19	7	4	14	17	24		8	18		4	0	18	24

↓ C ≡ P + 3 (mod 26).

Q	X	P	E	H	U		W	K	H	R	U	B		L	V		H	D	V	B
16	23	15	4	7	20		22	10	7	17	20	1		11	21		7	3	21	1

Untuk mengembalikan dari *ciphertext* ke *plaintext*, kita hanya perlu memodifikasi fungsi enkripsinya sehingga menjadi P ≡ C-3 (mod26). Inilah yang disebut sebagai fungsi dekripsi.

B. RSA Public Key Cryptography

Dalam sistem kriptografi RSA, penerima pesan memilih dua bilangan prima p dan q (dalam kasus nyata sedikitnya ratusan digit angka) dan menghitung n = p.q. Penerima pesan juga memilih sebuah bilangan e ≠ 1 yang mana bukan angka yang berdigit besar namun relatif prima terhadap ϕ(n) = (p-1)(q-1), sehingga ia memiliki invers dengan modulo [ϕ(n) = (p-1)(q-1)] dan hitung d=e^-1 dengan modulo yang diberikan. Penerima pesan mem-*publish* e dan n. Bilangan d disebut *public key*.

Enkripsi dimulai dengan mengkonversi pesan yang di kirim menjadi bilangan bulat M, di mana setiap huruf, angka atau tanda baca dari *plaintext* diganti dengan dua digit bilangan bulat.

A = 00	U = 20
B = 01	V = 21
C = 02	W = 22
D = 03	X = 23
E = 04	Y = 24
F = 05	Z = 25
G = 06	, = 26
H = 07	. = 27
I = 08	? = 28
J = 09	0 = 29
K = 10	1 = 30
L = 11	2 = 31
M = 12	3 = 32
N = 13	4 = 33
O = 14	5 = 34
P = 15	6 = 35
Q = 16	7 = 36
R = 17	8 = 37
S = 18	9 = 38
T = 19	! = 39

Di sini kita berasumsi M < n, oleh karena itu M dipisah ke dalam beberapa blok digit M1, M2, ..., Ms dari perkiraan besarnya. Setiap blok dienkripsi secara terpisah. Pengirim pesan mengubah *plaintext number* M ke *ciphertext number* 'r' dengan memangkatkan e ke M dan dengan modulus n : M^e ≡ r(mod n). Penerima pesan melakukan dekripsi dengan menentukan bilangan bulat j, bilangan *recovery* rahasia untuk e.j ≡ 1[mod ϕ(n)]. Memangkatkan j ke *ciphertext number* dan dimod dengan n akan mengembalikan *plaintext* numbernya : r^j ≡ M (mod n). Contoh:

1. Kita memilih 2 bilangan prima, p = 59 dan q = 41.
2. n = p.q = 59.41 = 2419
3. ϕ(n) = ϕ(2419) = ϕ(59) ϕ(41) = 58.40 = 2320
4. Kita memilih e = 3 untuk eksponen enkripsi dimana 3 dan 2320 adalah relatif prima.
5. Eksponen recovery j adalah 3.j ≡ 1(mod 2320), maka j = 1547
6. Misal:
   plaintext → GOLD MEDAL
   plaintext number → 061411031204030011
   Karena M > n, jadi pisahkan M ke dalam blok-blok 3 digit bilangan : 061 411 031 204 030 011

   $061^3 \equiv 2014 (\text{mod } 2419)$ $411^3 \equiv 1231 (\text{mod } 2419)$ $031^3 \equiv 0763 (\text{mod } 2419)$
   $204^3 \equiv 1393 (\text{mod } 2419)$ $030^3 \equiv 0391 (\text{mod } 2419)$ $011^3 \equiv 1331 (\text{mod } 2419)$

7. Didapatkan pesan yang sudah dienkripsi sebagai berikut: 2014 1231 0763 1393 0391 1331

IV. PENTINGNYA KRIPTOGRAFI

Pembentukan jaringan komputer pertama membuat ilmuwan berpikir tentang pentingnya ilmu kriptografi. Komputer berkomunikasi satu sama lain melalui jaringan terbuka, tidak hanya melalui koneksi langsung satu sama lain; jaringan semacam itu sangat transformatif dalam banyak hal, namun membuat kita dengan sangat mudah mengakses data yang berjalan di seluruh jaringan. Karena layanan finansial menjadi tujuan penggunaan awal komunikasi komputer, sangat penting bagi kita untuk menemukan cara merahasiakan informasi.

IBM pada akhir 1960-an memimpin kemajuan keamanan informasi dengan menemukan metode enkripsi yang dikenal sebagai "Lucifer", yang akhirnya dikodifikasikan oleh US National Bureau of Standards sebagai Data Encryption Standard (DES) pertama. Ketika internet menjadi semakin penting dan dibutuhkan, diperlukan enkripsi yang lebih banyak dan lebih baik. Saat ini sebagian besar data yang tersebar di seluruh dunia dienkripsi menggunakan berbagai teknik.

Kegunaan dari ilmu kriptografi sangat luas, dari menyimpan rahasia militer hingga mentransmisikan data keuangan dengan aman di internet. Namun dalam gambaran yang lebih besar, ada beberapa tujuan keamanan *cyber* besar yang ingin dicapai, seperti yang dijelaskan oleh seorang konsultan keamanan *cyber*, Gary Kessler. Dengan menggunakan teknik kriptografi, ahli *cyber security* dapat:

1. Menjaga kerahasiaan data
2. Mengautentikasi identitas pengirim dan penerima pesan
3. Memastikan integritas data, menunjukkan bahwa data belum diubah
4. Mendemonstrasikan bahwa pengirim asli dari pesan benar-benar mengirim pesan, sebuah prinsip yang dikenal sebagai *non-repudiation.*

V. KESIMPULAN

Dalam makalah ini kita dapat melihat bahwa banyak *tools* pada Teori Bilangan yang memainkan peran penting dalam kriptografi. *Tools* dalam Teori Bilangan seperti bilangan prima, pembagi, kongruensi, dan fungsi Euler andil dalam proses enkripsi dan dekripsi pesan. Sistem kriptografi *Caesar cipher* dan kunci publik RSA memberikan gambaran tentang *cryptosystem* dalam konteks aljabar dan Teori Bilangan. Oleh karena itu, dapat disimpulkan Teori Bilangan memegang peranan penting dalam ilmu kriptografi

REFERENSI

[1] "Congruence". mathworld.wolfram.com. 19 November 2020. 11 Desember 2020. https://mathworld.wolfram.com/Congruence.html

[2] "Divisor". mathworld.wolfram.com. 19 November 2020. 10 Desember 2020. https://mathworld.wolfram.com/Divisor.html

[3] "Encryption – Part 1 – The Caesar Cipher". windsongtrainig.ca. 9 Oktober 2019. 10 Desember 2020. https://windsongtraining.ca/encryption-part-1-the-caesar-cipher/

[4] "Greatest Common Divisor". mathworld.wolfram.com. 19 November 2020. 10 Desember 2020/. https://mathworld.wolfram.com/GreatestCommonDivisor.html

[5] "Prime Number". mathworld.wolfram.com. 19 November 2020. 10 Desember 2020. https://mathworld.wolfram.com/PrimeNumber.html

[6] "Substitution Cipher in Cryptography". ques10.com. Agusuts 2019. 10 Desember 2020. https://www.ques10.com/p/47687/substitution-cipher-in-cryptography-1/

[7] "Teori Bilangan". id.wikipedia.org. 8 Desember 2020. 10 Desember 2020. https://id.wikipedia.org/wiki/Teori_bilangan

[8] "What is cyptography? How algorithms keep information secret and safe". cssonline.com. 15 Oktober 2020. 10 Desember 2020. https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html

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

Farhan Yusuf Akbar
13519202