Aplikasi Teori Bilangan dan Operasi Logika pada Algoritma Kriptografi RC4

Priagung Satyagama 13516089
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
priagungsatyagama@students.itb.ac.id

Abstrak*—Pada zaman sekarang dimana teknologi semakin maju dengan sangat pesat, dimana informasi bisa sangat cepat terkirim walaupun terpisah oleh jarak ribuan kilometer. Kemudahan-kemudahan yang ditawarkan oleh teknologi saat ini pun dapat dimanfaatkan oleh para kriminal di dunia maya atau lawan politik untuk dapat menyadap informasi yang bersifat rahasia sehingga dibutuhkan keamanan ekstra untuk menjamin bahwa informasi rahasia yang dikirim tidak dapat dibaca oleh siapapun selain oleh penerima. Kriptografi adalah salah satu solusi nya, kriptografi membuat pesan yang kita kirim tidak dapat dibaca oleh siapapun kecuali oleh orang yang dapat melakukan dekripsi. Ilmu matematika diskrit merupakan ilmu yang mendasari ada nya kriptografi ini. Salah satu algoritma kriptografi yang sampai saat ini masih efektif untuk digunakan adalah algoritma RC4. Teori bilangan dan operasi logika digunakan pada algoritma ini. Pada makalah ini, penulis akan menjabarkan mengenai aplikasi dari teori bilangan dan operasi logika tersebut pada algoritma RC4.

***Kata Kunci*—Algoritma, Dekripsi, Enkripsi, Kriptografi, RC4.**

I. PENDAHULUAN

Dewasa ini, perkembangan teknologi semakin pesat. Kita dapat mengirimkan pesan kepada seseorang yang terpisah oleh jarak yang jauh bahkan mencapai puluhan ribu kilometer hanya dalam orde waktu milidetik. Bayangkan ketika jaman dahulu belum ada aplikasi semacam *instant messaging* sehingga membuat setiap orang yang ingin menyampaikan informasi harus menunggu berhari-hari bahkan berminggu-minggu untuk memastikan pesan itu sampai.

Dibalik kemudahan tersebut, ternyata terdapat momok yang menghantui pengirim atau penerima pesan yaitu rasa cemas akan keamanan informasi dan kerahasiaan informasi yang disampaikan. Memang benar, salah satu manfaat dari teknologi *instant messaging*, *e-mail*, dsb adalah kemudahan untuk mendapatkan informasi. Informasi yang berseliweran melewati jaringan internet sangat banyak dan sangat bermacam-macam. Mulai dari pesan yang tidak begitu penting yang disampaikan diantara dua pasangan kekasih hingga pesan yang mengandung rahasia negara tertentu. Internet merupakan jaringan yang bisa diakses oleh siapa saja, sehingga pada dasarnya informasi yang dikirim melalui jaringan internet bisa disadap dan diakses oleh penyadap.

Disinilah pentingnya atau urgensi dari penjagaan terhadap keamanan informasi. Salah satu metode yang sampai saat ini masih digunakan karena untuk teknologi saat ini masih efektif untuk mengamankan informasi adalah kriptografi. Kriptografi adalah teknik mengenkripsi informasi sehingga informasi tersebut tidak bisa dibaca oleh penyadap dan hanya bisa dibaca oleh penerima saja. Ada berbagai macam algoritma kriptografi saat ini, mulai dari kriptografi yang memiliki kompleksitas sangat tinggi dengan konsekuensi tingkat keamanannya tinggi, hingga algoritma dengan kompleksitas rendah sehingga didapatkan kepraktisan dan portabilitas.

Salah satu algoritma kriptografi yang cukup powerful dan mangkus adalah algoritma RC4. RC4 menggunakan teori bilangan dan operator logika untuk melakukan enkripsi maupun dekripsi nya. Pada makalah ini, saya akan menjelaskan mengenai aplikasi teori bilangan dan operator logika terhadap algoritma kriptografi RC4.

II. TEORI DASAR

A. Logika Proposisi

Logika adalah studi yang mempelajari tentang bagaimana cara bernalar, disandarkan pada hubungan antara fakta-fakta yang ada dalam bentuk kalimat-kalimat. Berdasarkan fakta-fakta yang ada itu, dapat diturunkan fakta baru dengan menggunakan aturan-aturan logika yang ada. Dengan aturan-aturan logika tersebut juga lah kita dapat mengetahui apakah suatu pernyataan bisa diturunkan dari kumpulan fakta-fakta yang sudah ada atau tidak. Jika bisa, maka pernyataan tersebut bernilai benar (true), sebaliknya jika tidak bisa maka pernyataan tersebut bernilai salah (false).

Dalam konteks logika, kalimat yang bisa digunakan untuk menggambarka fakta-fakta yang memiliki nilai kebenaran yang pasti salah satunya adalah kalimat proposisi. Kalimat proposisi adalah kalimat yang mempunyai nilai kebenaran (*true or* false) yang pasti. Beberapa kalimat proposisi ini bisa digabungkan oleh operator-operator logika dan disajikan pada tabel kebenaran. Kalimat yang mengandung beberapa kalimat proposisi disebut dengan proposisi majemuk. Berikut adalah contoh dari kalimat proposisi.

Jakarta adalah ibukota Jawa Barat

12 adalah bilangan genap

3 habis membagi 7

Operator-operator logika dibagi menjadi dua yaitu operator biner dan operator uner. Operator biner adalah operator yang menghubungkan dua buah kalimat proposisi. Sedangkan operator uner adalah operator yang digunakan pada satu kalimat proposisi saja. Contoh operator uner adalah operator komplemen/negasi (~). Sedangkan contoh operator biner antara lain operator *and* ($\wedge$), *or* ($\vee$), *exclusive of/xor* ($\oplus$).

Nilai kebenaran dari beberapa kalimat proposisi yang dihubungkan dengan operator biner dapat digambarkan dengan tabel kebenaran. Tabel kebenearan adalah salah satu cara praktis dalam menentukan nilai kebenaran dari proposisi majemuk. Berikut adalah contoh-contoh dari tabel kebenaran.

P	Q	P ∧ Q
TRUE	TRUE	TRUE
TRUE	FALSE	FALSE
FALSE	TRUE	FALSE
FALSE	FALSE	FALSE

Tabel 1. Tabel Kebenaran Operator *AND*

P	Q	P ∨ Q
TRUE	TRUE	TRUE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

Tabel 2. Tabel Kebenaran Operator *OR*

P	Q	P ⊕ Q
TRUE	TRUE	FALSE
TRUE	FALSE	TRUE
FALSE	TRUE	TRUE
FALSE	FALSE	FALSE

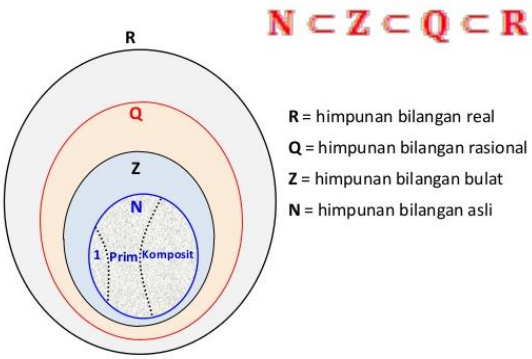
Tabel 3. Tabel Kebenaran Operator *XOR*

P	~P
TRUE	FALSE
FALSE	TRUE

Tabel 4. Tabel Kebenaran Operator Negasi

B. Bilangan Bulat

Bilangan terbagi menjadi berbagai macam yaitu bilangan riil, bilangan rasional, bilangan bulat, bilangan cacah, dan bilangan asli. Klasifikasi bilangan-bilangan tersebut dapat digambarkan dengan diagram venn seperti dibawah ini.



Gambar 1. Diagram Venn Klasifikasi Bilangan
Sumber : https://www.slideshare.net/Adhi99/matbab-i-sistem-bilangan-riil

Bilangan bulat adalah bilangan yang tidak mempunyai pecahan desimal. Contoh bilangan bulat antara lain 0, -2, 10, 9, -4. Sedangkan bilangan yang bukan bilangan bulat (yang mempunyai pecahan desimal) adalah seperti 2.5, 0.3, 1.99, dsb.

Bilangan bulat mempunyai sifat pembagian yang dituliskan dengan notasi "a | b" yang artinya a habis membagi b atau bisa diartikan sebagai b adalah kelipatan dari a. Definisi formal nya adalah sebagai berikut.

Definisi 1
Misalkan a dan b adalah dua buah bilangan bulat dengan syarat $a \neq 0$. Kita menyatakan bahwa a **habis membagi** b jika terdapat bilangan bulat c sedemikian sehingga b = ac

Sebagai contoh,
7 | 14, dengan mengambil c = 2, didapat 14 = 7x2, maka 7 habis membagi 14 atau 14 adalah kelipatan dari 7.

Secara umum, suatu bilangan bulat jika dibagi dengan bilangan bulat lainnya akan menghasilkan suatu hasil bagi yang merupakan bilangan bulat, dan sisa yang juga merupakan bilangan bulat. Sifat ini dituliskan secara formal dalam teorema berikut.

Teorema 1
Misalkan m dan n adalah dua buah bilangan bulat dengan syarat n>0. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (hasil) dan r (sisa), sedemikian sehingga

$$m = nq + r$$

Dengan $0 \leq r < n$.

Teorema tersebut ditemukan oleh matematikawan yang lahir pada tahun 350 SM yang bernama Euclid sehingga teorema itu sering disebut sebagai **teorema Euclidean.** Notasi lain yang biasa digunakan untuk mengekspresikan hasil dan sisa adalah dengan menggunakan operator *modulus* (mod) dan operator *division* (div). Berikut adalah penggunaan operator mod dan div

dalam mengekspresikan hasil dan sisa dari pembagian pada teorema Euclidian diatas.

$$q = m \; \boldsymbol{div} \; n,$$
$$r = m \; \boldsymbol{mod} \; n$$

Sebagai contoh, 20 dibagi dengan 3 akan memberikan hasil bagi 6 dan sisa bagi 2.

$$20 = 3.6 + 2$$
$$20 \; \boldsymbol{mod} \; 3 = 2$$
$$20 \; \boldsymbol{div} \; 3 = 6$$

Contoh lain, -22 dibagi dengan 7.

Ingatlah bahwa syarat $0 \leq r < n$ harus berlaku. Sehingga sisa dari pembagian haruslah selalu positif.

$$-22 = 7.(-4) + 6$$
$$-22 \; \boldsymbol{mod} \; 7 = 6$$
$$-22 \; \boldsymbol{div} \; 7 = -4$$

Operator *modulus* atau mod memiliki banyak kegunaan karena operator mod dapat memberikan batas maksimum dan minimum pada bilangan bulat. Sebagai contoh, a **mod** b = c, maka nilai c akan dibatasi hanya pada *range* $0 \leq c < a$.

Dalam aritmetika modulo, terdapat istilah kongruen. suatu nilai a dan b dikatakan kongruen dalam modulus m jika dan hanya jika a dan b memberikan sisa yang sama ketika dibagi dengan m. Ekspresi tersebut dapat dituliskan sebagai berikut.

$$a \equiv b \; (\boldsymbol{mod} \; m)$$

(Notasi $' \equiv '$ dibaca 'kongruen')

Sebagai contoh, 38 **mod** 5 = 3, dan 13 **mod** 5 = 3, maka ekspresi tersebut dapat ditulis sebagai

$$38 \equiv 13 \; (\boldsymbol{mod} \; 5)$$

Definisi formal dari kekongruenan dapat dituliskan sebagai berikut.

Definisi 2
Misalkan a, b, dan m adalah bilangan bulat dan m > 0, maka

$$a \equiv b \; (\boldsymbol{mod} \; m)$$

Jika m | (a-b).

Dalam aritmetika modulo, terdapat beberapa sifat-sifat aljabar yang berlaku sehingga dapat memudahkan perhitungan aritmetika modulo. Sifat-sifat tersebut terangkum dalam teorema berikut.

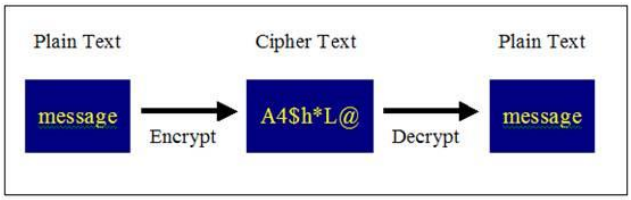
Teorema 2
1. Jika a = b (**mod** m) dan c adalah sembarang bilangan bulat, maka
   a) $(a + c) \equiv (b + c)$ (**mod** m)
   b) $ac \equiv bc$ (**mod** m)
   c) $a^c \equiv b^c$ (**mod** m), dengan syarat $c \geq 0$

2. Jika $a \equiv b$ (**mod** m) dan $c \equiv d$ (**mod** m), maka
   a) $(a + c) \equiv (b + d)$ (**mod** m)
   b) $ac \equiv bd$ (**mod** m).

C. Kriptografi

Kriptografi adalah seni dalam menyandikan pesan sehingga pesan tersebut tidak dapat dibaca selain oleh pengirim dan penerima pesan tersebut. Kriptografi sangatlah penting di zaman sekarang karena banyak sekali informasi-informasi yang sangat rahasia dikirimkan lewat internet.

Pesan yang akan di enkripsi atau pesan asli yang akan dikirimkan kepada penerima disebut *plaintext*. Sedangkan pesan yang sudah di enkripsi sedemikian sehingga informasi yang terdapat pada pesan itu tidak dapat dibaca oleh siapapun selain orang yang dapat mendekripsikan pesan tersebut dinamakan *ciphertext*. Proses enkripsi dan dekripsi sebuah pesan digambarkan pada diagram berikut.



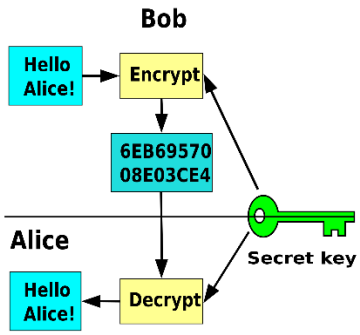
Gambar 2. Diagram Proses Enkripsi Dekripsi Pesan
Sumber : https://www.sqa.org.uk/e-learning/WebTech02CD/images/pic006.jpg

Kriptografi pertama kali diaplikasikan oleh tentara yunani sekitar tahun 400 SM. Mereka menggunakan alat semacam batang yang memiliki diameter tertentu yang dinamakan *scytale*.

Kriptografi di era modern seperti sekarang sangatlah bermacam-macam jenisnya. Berdasarkan jenis kunci nya kriptografi dibagi menjadi 2 kategori yaitu.

1. Kriptografi Kunci Simetris

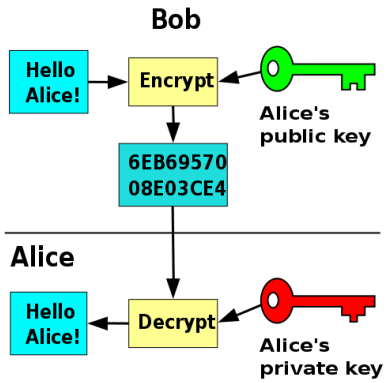
   Kriptografi jenis ini menggunakan kunci yang sama ketika ingin melakukan enkripsi ataupun dekripsi. Sehingga keberhasilan atau efektifitas dari kriptografi jenis ini adalah tergantung pada kerahasiaan kuncinya. Salah satu contoh algoritma kriptografi yang menggunakan sistem kunci simetris adalah algoritma RC4 yang mana algoritma ini menjadi pembahasan utama pada makalah ini.



Gambar 3. Ilustrasi Kriptografi Kunci Simetris
Sumber : https://upload.wikimedia.org/wikipedia/commons/thumb/2/27/Symmetric_key_encryption.svg

2. Kriptografi Kunci Publik

Kriptografi jenis ini menggunakan dua buah kunci yang berbeda ketika ingin melakukan enkripsi pesan atau dekripsi pesan. Kunci yang digunakan untuk mengenkripsi pesan adalah kunci publik, yang semua orang bisa mengakses nya. Sedangkan kunci yang digunakan untuk melakukan dekripsi adalah kunci privat, yaitu kunci yang hanya dimiliki oleh penerima pesan tersebut. Salah satu algoritma kriptografi yang sampai saat ini dipakai dan menggunakan sistem kunci publik adalah algoritma RSA.



Gambar 4. Ilustrasi Kriptografi Kunci Publik
Sumber: https://upload.wikimedia.org/wikipedia/commons/f/f9/Public_key_encryption.svg

Sedangkan kriptanalisis adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang diberikan. Tujuan dari kriptanalisis ialah untuk menemukan kelemahan dan ketidakamanan dalam skema kriptografi sehingga memungkinkan peningkatan atau perbaikan.

III. Analisis Algoritma RC4

RC4 adalah algoritma kriptografi yang menggunakan sistem kunci simetris dimana kunci yang digunakan untuk melakukan enkripsi sama dengan kunci yang digunakan untuk melakukan dekripsi. Algoritma RC4 pertama kali ditemukan oleh seorang kriptografer yang juga merupakan salah satu professor di MIT yang bernama Ronald Linn Rivest. Algoritma ini ditemukan pada tahun 1987.

Enkripsi yang dilakukan oleh algoritma RC4 adalah byte per byte dengan cara melakukan operasi XOR untuk setiap byte pada plaintext dengan setiap byte pada *pseudorandom stream* yang dihasilkan oleh algoritma RC4 ini. Output dari generator *pseudorandom stream* tersebut dinamakan *keystream*. *Keystream* dihasilkan dari pemrosesan input kunci privat dari pengirim pesan yang kemudian diproses oleh algoritma RC4 sedemikian sehingga dihasilkan *keystream* sepanjang 256 byte.

```
  11001100  plaintext
⊕ 01101100  key stream
  10100000  ciphertext
```

```
  10100000  ciphertext
⊕ 01101100  key stream
  11001100  plaintext
```

Gambar 5. Enkripsi dan Dekripsi dengan Operasi XOR

Untuk menghasilkan *keystream* sepanjang 256 byte, pertama-tama inisialisasi dahulu sebuah struktur data *array of char* S yang akan menyimpan *keystream* dengan elemen sebanyak 256 buah, dan kemudian inisialisasi nilai dari setiap elemen array dengan indeks array tersebut. Kemudian inisialisasi sebuah struktur data temporer T dengan tipe data *array of char* dengan elemen sebanyak 256 buah. Inisialisasi setiap elemen T dengan setiap elemen *key* yang menjadi kunci privat untuk melakukan enkripsi dan dekripsi. Berikut adalah *pseudocode* nya.

```
/* Initialization */
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen];
```

Setelah itu, permutasikan setiap isi dari array S dengan setiap isi dari array T, yang kemudian disimpan pada array S. berikut adalah *pseudocode* nya.

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j]);
```

Terlihat bahwa operasi yang terjadi hanyalah *swap* antar elemen array S, sehingga nilai dari elemen array S masih sama, yaitu 0 sampai 255, hanya saja posisi nya yang sudah berubah sesuai dengan proses pengacakan dengan melibatkan kunci privat yang diinput oleh pengirim pesan.

Setelah ini, proses untuk mendapatkan *keystream* yang dapat digunakan untuk dekripsi ataupun enkripsi. Proses ini juga secara umum hanya melakukan swap untuk setiap elemen dari array S. berikut adalah *pseudocode* nya.

```
/* Stream Generation */
i, j = 0;

while (true)
    i = (i + 1) mod 256;
    j = (j + S[i]) mod 256;
    Swap (S[i], S[j]);
    t = (S[i] + S[j]) mod 256;
    k = S[t];
```

Terlihat bahwa diakhir program, terdapat nilai pada variabel k, nilai dari k ini dapat digunakan untuk melakukan enkripsi ataupun dekripsi dari setiap byte pesan yang akan di enkripsi ataupun di dekripsi, sehingga untuk setiap loop, dengan nilai k yang berubah mengikuti proses dari algoritma tersebut, setiap

byte dari pesan juga dapat diproses dengan operasi XOR terhadap nilai dari k tersebut.

Operator logika XOR dan operator modulus sangat digunakan dalam algoritma ini. Operator XOR digunakan pada proses akhir dari enkripsi ataupun dekripsi, sedangkan operator modulus digunakan untuk membatasi agar pengisian dari setiap array tidak melebihi indeks (*buffer overflow*).

Untuk urusan performa, algoritma RC4 ini sangat cepat karena proses enkripsi yang dilakukan adalah pada orde byte dan operasi yang digunakan yaitu operasi-operasi yang sangat sederhana. Berikut ada data yang saya dapat dari bimacipta.com mengenai pengujian kecepatan dari algoritma RC4 ini.

Pada pengujian ini, enkripsi dilakukan dengan ukuran 256 byte per blok sebanyak 20480 kali atau sekitar 5MB data. Berikut adalah data nya.

Delphi 1.0 pada Windows for Workgroups 3.11

Prosesor	Memori (MB)	Kecepatan (Kbytes/detik)
486/DX4-100	16	557,067
Pentium 100	32	1.079,713
Pentium 166	16	1.792,717

Delphi 4.0 pada Windows 95, kecuali Pentium Pro pada Windows NT 4.0 Server

Prosesor	Memori (MB)	Kecepatan (Kbytes/detik)
486/DX4-100	16	2.563,846
Pentium 100	16	4.285,714
Pentium 133	32	5.380,035
Pentium 166MMX	32	7.191,522
Pentium 200MMX	32	8.668,172
Pentium Pro 200	64	10.651,872

Tes tersebut dilakukan masing-masing sebanyak tiga kali kemudian hasilnya dirata-ratakan. Sebagai perbandingan, algoritma kriptografi Blowfish (sama-sama menggunakan kunci simetris) adalah sekitar 2.300 KB/detik pada Pentium 133 (pada 8 byte per blok). Sehingga terbukti berdasarkan data tersebut bahwa algoritma RC4 sangatlah mangkus.

Walaupun algoritma RC4 ini mangkus, tetapi keamanan yang ditawarkan pun masih sangat dapat diandalkan untuk teknologi saat ini. Satu-satu nya cara paling mungkin untuk membobol *ciphertext* adalah dengan serangan *brute force*. Sehingga keamanan data sepenuhnya bergantung pada panjang kunci.

Ambil contoh panjang kunci 160 bit. Sehingga terdapat 2^{160} kunci yang mungkin. Bila kita anggap rata-rata diperlukan setengahnya untuk mendapat kunci yang benar (kurang lebih 10^{48}). Lalu diberikan beberapa asumsi tentang peralatan yang digunakan untuk memecahkan kunci tersebut :

- Terdapat 1 milyar komputer yang digunakan.
- Setiap komputer digunakan sepenuhnya untuk memecahkan kunci tersebut.
- Setiap computer dapat mencoba 1 milyar kunci per detik.

Maka, dengan peralatan demikian, dibutuhkan 10^{13} tahun untuk mendapatkan kunci tersebut atau sama dengan 1000 kali usia alam semesta. Terbukti bahwa dengan teknologi yang ada saat ini, *ciphertext* yang dihasilkan dari algoritma RC4 tidak akan mungkin bisa diretas dengan serangan *brute force*.

IV. KESIMPULAN

Teori bilangan maupun logika memiliki peranan yang sangat penting dalam bidang ilmu komputer. Salah satunya adalah kriptografi. Kriptografi saat ini merupakan hal yang sangat penting karena di era digital seperti saat ini, informasi dapat dikirim dengan sangat cepat dan efisien melalui internet. Sedangkan hampir siapapun dapat terhubung dengan internet, sehingga diperlukan pengamanan ekstra untuk informasi yang berlalu-lalang melalui internet.

Algoritma RC4 adalah salah satu algoritma kriptografi yang memanfaatkan teori bilangan dan operasi logika. Algoritma ini sampai saat ini masih dapat diandalkan karena memiliki algoritma yang mangkus dan pengamanan yang sangat mumpuni untuk teknologi saat ini.

V. UCAPAN TERIMA KASIH

Pertama-tama, saya ucapkan syukur kepada Allah SWT karena berkat rahmat dan karunia nya, saya diberi kesehatan dan kemampuan untuk menyelesaikan makalah ini dengan baik. Kemudian saya juga mengucapkan terima kasih sebesar-besarnya kepada tim dosen pengampu mata kuliah IF 2120 Matematika diskrit yaitu kepada Dra. Harlili S., M.Sc., Dr. Ir. Rinaldi Munir, M.T., dan Dr. Judhi Santoso, M.Sc. yang telah membimbing dan menyampaikan materi terkait Matematika Diskrit. Semoga makalah ini dapat memberikan manfaat sebesar-besarnya kepada para pembaca.

REFERENCES

[1] Munir, Rinaldi. 2006. Diktat Kuliah IF2120 Matematika Diskrit. Bandung : Institut Teknolgi Bandung.

[2] http://www.crypto-it.net/eng/symmetric/rc4.html?tab=1. Diakses pada tanggal 1 Desember 2017

[3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography

[4] http://www.bimacipta.com/rc4-stream-cipher.html. Diakses pada tanggal 1 Desember 2017

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, 3 Desember 2017

Priagung Satyagama
13516089