Ztalis Block Cipher

Didik Supriadi [1]

Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika (STEI), Institut Teknologi Bandung (ITB), Jalan Ganesha 10, Bandung 40132, Indonesia

[1] Email: 13517069@std.stei.itb.ac.id

Abstraksi. Cipher blok adalah teknik yang banyak digunakan saat ini dalam algoritma kriptografi modern yang terstandarisasi. Keunggulan cipher blok yang melakukan operasi pada blok bit atau blok byte memungkinkan perancang algoritma untuk merancang algoritma yang rumit dan sulit dipecahkan. Ztalis cipher merupakan salah satu algoritma cipher blok yang mengimplementasikan jaringan feistel dan memiliki 128 bit kunci yang beroperasi pada 128 bit blok data. Nama Ztalis terinspirasi dari terminologi *Talisman* atau jimat yang berarti benda okultisme yang berasal dari praktik keagamaan atau astrologi.

Kata-kata kunci. Kriptografi, Blok cipher, Jaringan Feistel, Ztalis, Talisman.

1) Pendahuluan

Kriptografi merupakan sebuah seni atau ilmu yang digunakan untuk mengamankan suatu data atau pesan yang tidak ingin diketahui maknanya selain oleh sang penerima pesan. Kriptografi sudah dikenal sejak jaman sebelum masehi seperti misalnya pada zaman mesin kuno yang menggunakan simbol untuk sebuah pesan, zaman Yunani dan romawi kuno yang melahirkan salah satu algoritma terkenal yaitu Caesar Cipher, dan pada zaman arab kuno yang menimbulkan banyak kemajuan pada bidang kriptografi.

Kriptografi juga memiliki peranan penting dalam sejarah kehidupan manusia seperti pada zaman renaissance, peristiwa hukuman mati kepada ratu Mary dari

Skotlandia akibat terpecahkannya pesan yang berisi rencana pembunuhan ratu inggris, dan yang paling terkenal adalah pada jaman perang dunia kedua dimana Alan Turing berhasil memecahkan Enigma cipher sehingga memperpendek perang dunia ke-2.

Pada saat ini kriptografi masih sangat berperan dalam menyediakan pelayanan keamanan dalam pertukaran pesan. Terutama pada penggunaan internet yang semakin meluas dan tingkat ketergantungan yang tinggi terhadap penggunaan internet untuk mengirim dan menerima informasi. Perkembangan pada era internet ini ternyata tidak hanya memberikan akses informasi yang cepat dan mudah tetapi juga kemudahan untuk mencuri atau menyedot suatu informasi yang ditransmisikan melalui internet. Munculnya era kriptografi modern ini dikarenakan kebutuhan pengamanan pesan yang jauh lebih kompleks dan dapat diterapkan pada pesan yang ditukarkan melalui internet.

Blok cipher merupakan salah satu teknik yang banyak diterapkan pada algoritma kriptografi modern seperti AES (Advanced Encryption Standard) dan DES (Data Encryption Standard) yang menjadi standarisasi untuk beberapa proses enkripsi suatu data. Teknik chiper blok merupakan teknik operasi yang mengoperasikan chiper untuk setiap blok bit atau blok byte dari sebuah pesan, pengoperasian yang dilakukan untuk setiap blok dari suatu data ini memungkinkan para perancang algoritma untuk merancang chiper yang lebih kompleks dan susah dipecahkan.

Ztalis Cipher merupakan algoritma cipher blok yang terinspirasi dari algoritma DES dan AES, dimana algoritma ini menggunakan dan mengimprovisasi beberapa teknik yang digunakan dalam kedua algoritma tersebut, misalnya:

1. Penggunaan round constants seperti pada AES untuk key-scheduling
2. Penggunaan fungsi ekspansi dan kompresi seperti pada algoritma DES namun dibuat lebih kompleks.
3. Beberapa fungsi dari algoritma AES yang diimprovisasi menjadi lebih kompleks
4. Penggunaan jaringan Feistel seperti pada DES.

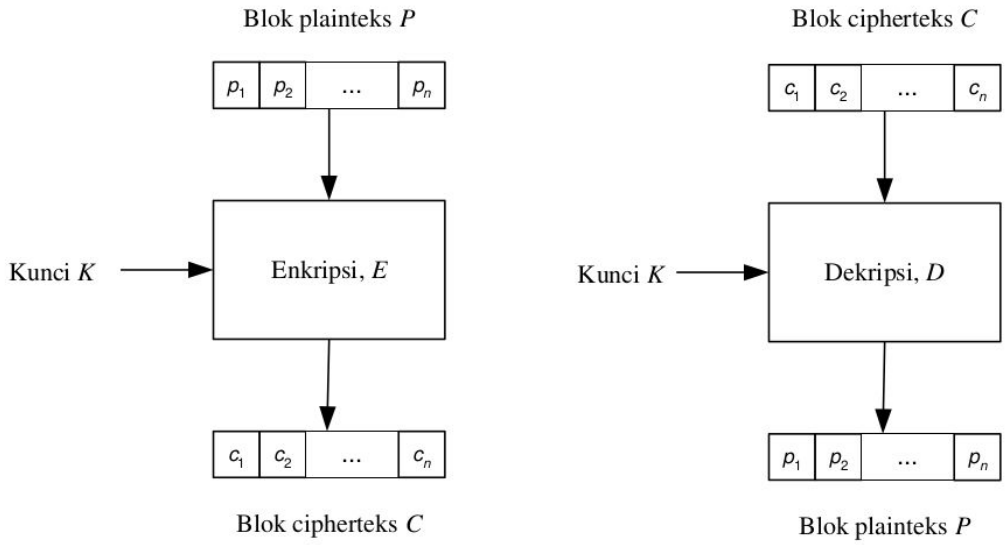
Penjelasan algoritma secara mendetail akan dibahas dalam makalah ini, untuk selanjutnya, makalah akan disusun dengan susunan sebagai berikut. Bagian dua akan membahas studi pustaka yang relevan dengan pekerjaan yang dilakukan. Bagian tiga akan membahas rancangan detail dari algoritma Ztalis Cipher. Bagian empat akan

membahas eksperimen dan analisis hasil penggunaan algoritma Ztalis Cipher. Bagian kelima akan membahas kesimpulan dan saran pengembangan.

2) Studi pustaka

A. Block Cipher

Block cipher adalah sebuah teknik operasi yang digunakan dalam kriptografi modern dimana pada block cipher, pesan dibagi menjadi sekumpulan blok n-bit yang kemudian akan dipetakan dengan fungsi chiper menjadi sebuah blok chiper, hal ini diulang untuk semua blok dari data yang ada, hal ini berbeda dengan jenis teknik operasi kriptografi modern yang lain yaitu stream cipher yang melakukan operasi untuk 1 bit.

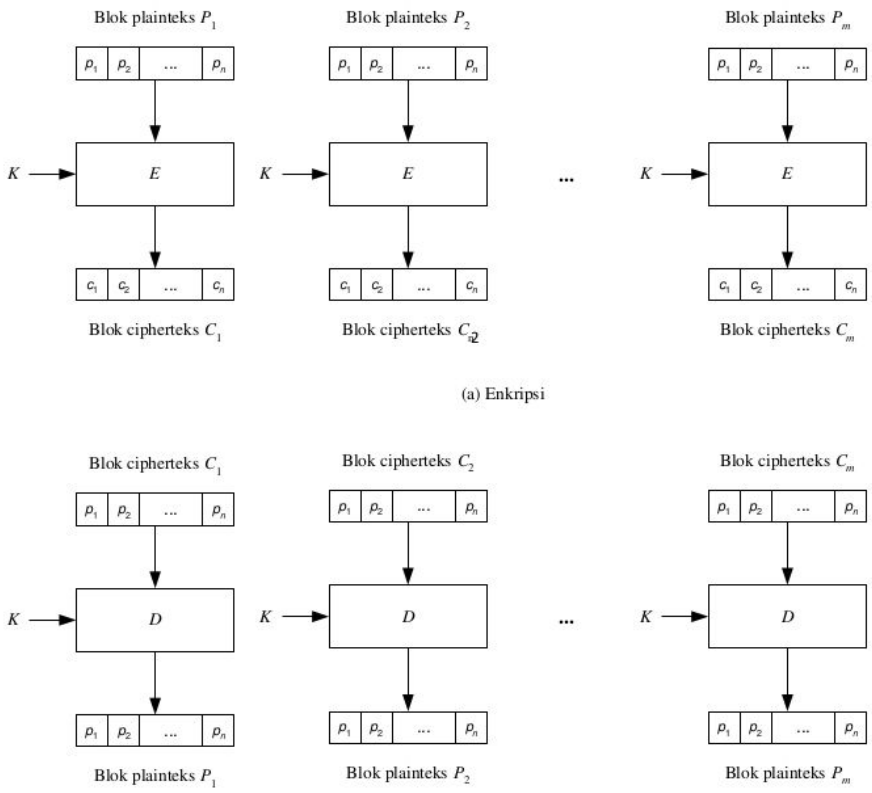


Gambar 1: Skema enkripsi dan dekripsi pada block cipher

Dalam block cipher terdapat beberapa mode untuk pengoperasian pada tiap blok, yaitu:

1. Electronic Codebook (ECB)

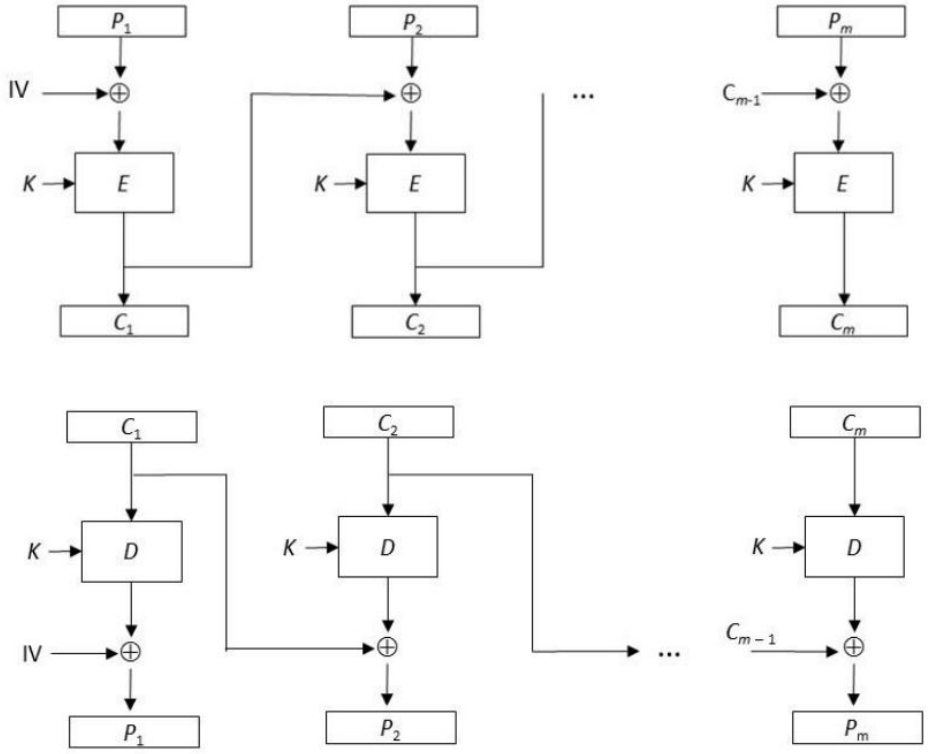
Pada mode ECB, setiap blok dioperasikan secara independen sehingga setiap blok dapat bisa dioperasikan secara tidak terurut.



Gambar 2: Skema enkripsi dan dekripsi pada ECB

2. Cipher Block Chaining (CBC)

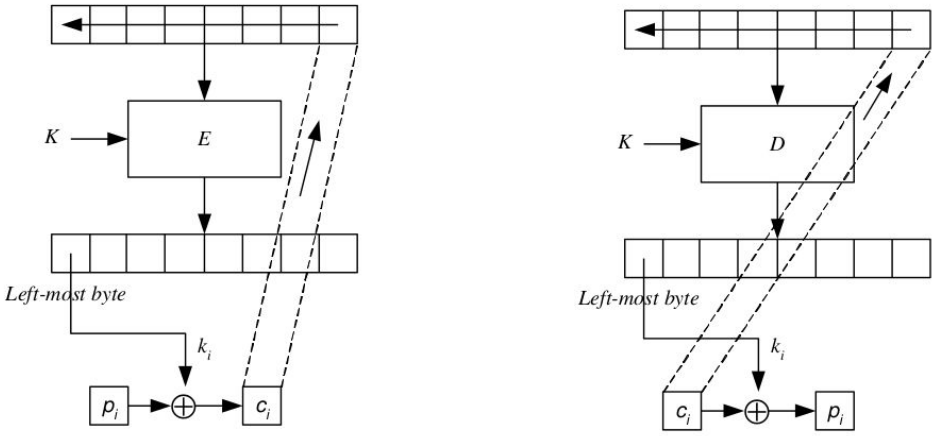
   Mode operasi CBC setiap hasil enkripsi blok plainteks bergantung pada hasil enkripsi blok sebelumnya.



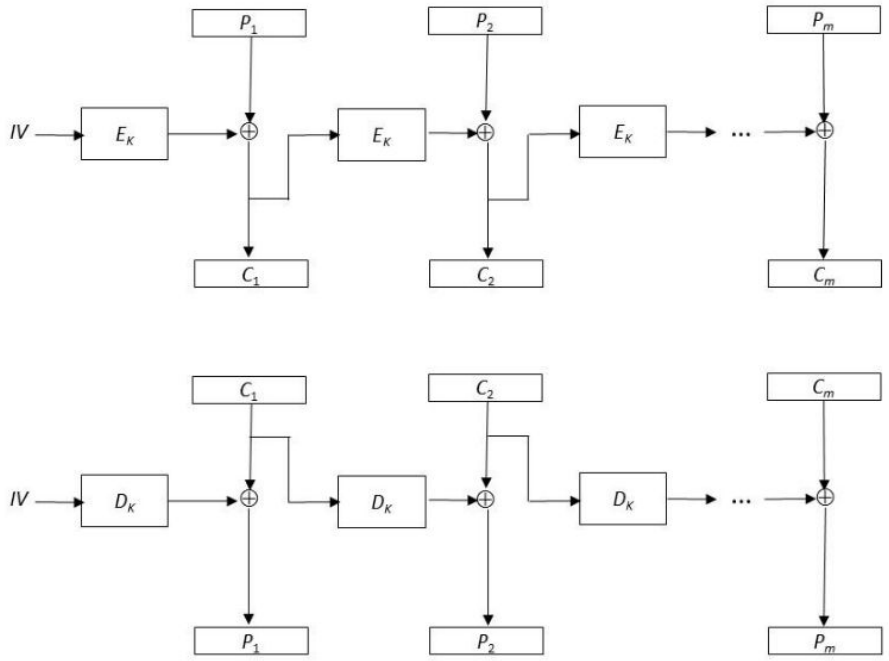
Gambar 3: Skema enkripsi dan dekripsi pada CBC

3. Cipher Feedback (CFB)

Mode operasi CFB melakukan enkripsi dan dekripsi yang bergantung dari blok sebelumnya sama seperti CBC namun perbedaannya adalah CFB dapat mengenkripsi data untuk yang lebih kecil dari ukuran blok.



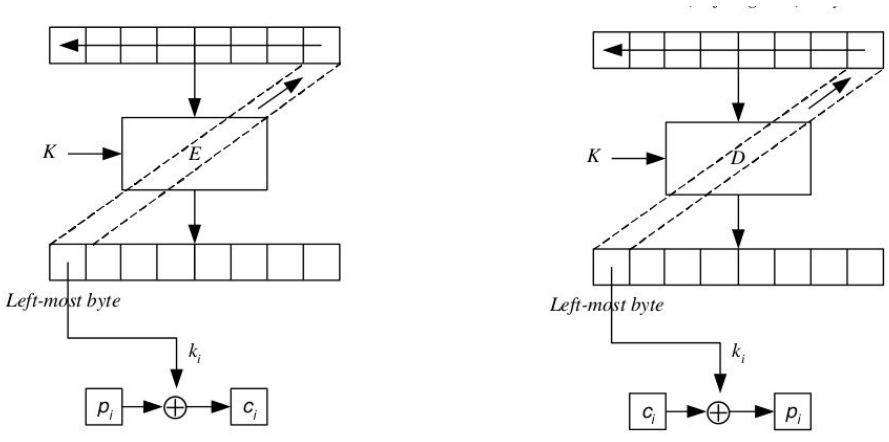
Gambar 4: Skema blok data enkripsi dan dekripsi pada CFB



Gambar 5: Skema enkripsi dan dekripsi pada CFB

4. Output Feedback (OFB)

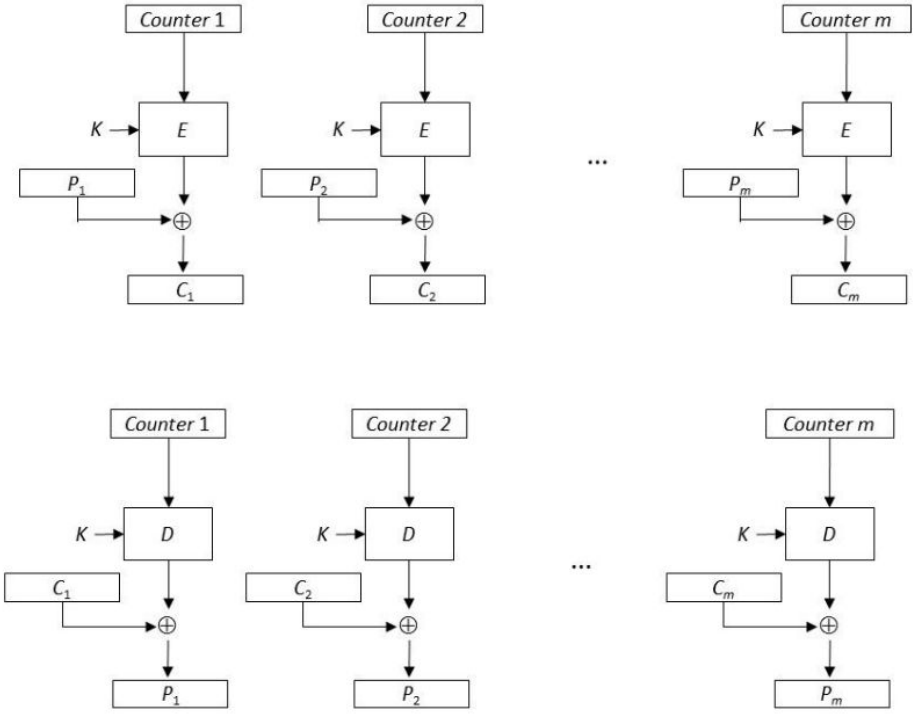
Mode operasi OFB kurang lebih sama dengan mode operasi CFB, yang berbeda adalah hasil enkripsi yang dipakai sebagai posisi paling kanan di antrian.



Gambar 6: Skema blok data enkripsi dan dekripsi pada OFB

5. Counter Mode (CM)

Mode CM tidak melakukan perantaian atau feedback untuk memproses blok selanjutnya, namun menggunakan suatu nilai counter yang nilainya dinaikkan ketika akan memproses blok selanjutnya.



Gambar 7: Skema enkripsi dan dekripsi pada CM

B. *Confusion* dan *Diffusion*

Prinsip yang diperkenalkan oleh *Claud Shannon* dalam makalah klasiknya, *Communication theory of secrecy* system pada tahun 1949. Prinsip ini bertujuan untuk mengatasi serangan statistik.

Confusion merupakan prinsip yang bertujuan untuk menyembunyikan keterhubungan antara plainteks, chiperteks, dan kunci, salah satu caranya adalah menggunakan algoritma substitusi yang kompleks.

Diffusion adalah prinsip yang bertujuan untuk membuat pengaruh perubahan 1 bit menjadi sangat besar terhadap chiperteks yang terbentuk, salah satu caranya adalah dengan menggunakan permutasi yang kompleks.

C. Jaringan Feistel

Jaringan Feistel adalah sebuah skema yang menerapkan mekanisme cipher berulang (*iterated cipher*) dan memungkinkan kita untuk melakukan enkripsi dan dekripsi dengan algoritma chiper yang sama (reversible)

3) Proposed block cipher

A. Ikhtisar algoritma

Algoritma Ztalis adalah sebuah algoritma blok cipher yang menggunakan jaringan feistel dan beroperasi dalam blok byte. Algoritma ini terinspirasi dari DES dan AES yang dimodifikasi dengan fungsi yang lebih kompleks. Spesifikasi dasar dari Ztalis cipher, yakni:

1. Menggunakan jaringan feistel dengan 16 putaran
2. Panjang blok data 128 bit
3. Panjang kunci 128 bit
4. Beroperasi dalam byte

B. Variabel

Bagian ini mendeskripsikan variabel yang digunakan dalam algoritma Ztalis, diantaranya adalah sebagai berikut.

1. Initialization Vector (IV)

Sebuah inisialisasi vektor yang pertama kali diinisialisasi yang berukuran 16.

233	193	222	145	7	170	63	25
72	197	239	127	8	58	137	50

Tabel 1: Initialization Vector

2. Round Constant (R-Box)

Konstanta matriks berukuran 2 x 4 yang digunakan dalam pembangkitan round keys dari kunci eksternal.

103	105	221	29
65	244	21	87

Tabel 2: Round constant

3. Substitution Box (S-Box)

Ztalis cipher memiliki 4 kotak substitusi.

C. Fungsi Transformasi

Bagian ini menjelaskan fungsi-fungsi transformasi yang digunakan dalam algoritma Ztalis pada bagian Round Function dan Key Scheduling.

1. `subt_expansion`

   Fungsi transformasi ini adalah fungsi transformasi kompleks yang melakukan substitusi dan ekspansi dari sebuah larik dengan ukuran (1 x 4) menjadi sebuah matriks berukuran (4 x 4).

2. `shift_row`

   Fungsi transformasi ini melakukan pergeseran secara siklik untuk setiap baris dari matriks state.

3. `mix_col`

   Fungsi transformasi yang juga digunakan oleh algoritma AES. Fungsi mengalikan matriks state dengan suatu matriks pengacak..

4. `subt_compression`

   Fungsi transformasi yang akan melakukan substitusi dan kompresi pada sebuah matriks state berukuran (4 x 4) menjadi sebuah larik berukuran (1 x 4).

D. Key Scheduling

Dari kunci eksternal sepanjang 128 bit (16 byte) akan dibangkitkan 26 round keys sepanjang 128 bit (16 byte) untuk 16 putaran, setiap putaran dibutuhkan 2 round keys. Proses pembangkitan kunci dibagi menjadi 2 bagian, pembangkitan 16 kunci pertama (Rk l) dan pembangkitan 16 kunci kedua (Rk r).

Untuk final round atau i = 12, Rk 12 = MixCol(V) dimana V adalah hasil operasi xor dari semua nilai Rk 0 ... Rk 11. Proses ini dilakukan 2 kali untuk W l dan W r .

Proses key scheduling akan menghasilkan 16 Rk l dan 16 Rk r yang dimana akan dipakai sebagai round keys untuk 16 ronde putaran. Tiap putaran ke-i akan menggunakan 2 kunci yaitu Rk li dan Rk ri .

E. Round Function

Ztalis cipher menggunakan jaringan feistel dengan 13 putaran yang dimana memiliki round function yang akan dioperasikan untuk enkripsi dan dekripsi pada setiap ronde putaran.

4) Eksperimen dan analisis hasil

Prinsip confusion dan diffusion merupakan prinsip dasar yang dapat mengukur seberapa rumit dan sulitnya suatu algoritma chiper untuk dipecahkan.

Gambar 8: File uji coba

Menggunakan citra lena grayscale dengan ukuran 48077 byte yang akan dienkripsi menggunakan kunci = ‘ztalisztalisztal’ sepanjang 16 byte.

Dari hasil ujicoba dapat dilihat bahwa pergantian 1-bit baik pada kunci maupun pada plainteks akan memberikan chiperteks yang jauh berbeda, dengan persentase perubahan rata-rata sebesar > 99.60%. Hal ini mengindikasikan bahwa prinsip confusion dan diffusion telah terimplementasi dengan baik.

5) Kesimpulan dan saran pengembangan

A. Kesimpulan

Algoritma Ztalis Cipher sudah memberikan hasil yang baik. Hal ini diperoleh karena penggunaan fungsi transformasi yang kompleks seperti SubExp dan SubComp yang dimana menggunakan 4 S-Box untuk melakukan substitusi sekaligus melakukan ekspansi dan kompresi.

B. Saran

Dalam tugas ini belum dicantumkan beberapa hal penting seperti waktu eksekusi dan pemakaian memori dari algoritma. Beberapa optimisasi juga masih bisa dilakukan untuk mengurangi biaya komputasi.

6) Referensi

[1] Munir Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Pengantar Kriptografi

[2] Munir Rinaldi. 2020. Slide Kuliah IF4020 Kriptografi: Kriptografi Modern