PENERAPAN MATRIKS DENGAN KOEFISIEN BINOMIAL NEWTON SEBAGAI PENGAMAN PESAN MENGGUNAKAN ALGORITMA HILL CIPHER

Skripsi

disusun sebagai salah satu syarat

untuk memperoleh gelar Sarjana Sains

Program Studi Matematika

oleh

Khayatul Fahmi

4111413016

JURUSAN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI SEMARANG

2018

PERNYATAAN

Saya menyatakan bahwa skripsi ini bebas plagiat, dan apabila di kemudian hari terbukti terdapat plagiat dalam skripsi ini, maka saya bersedia menerima sanksi sesuai ketentuan peraturan perundang-undangan.

PENGESAHAN

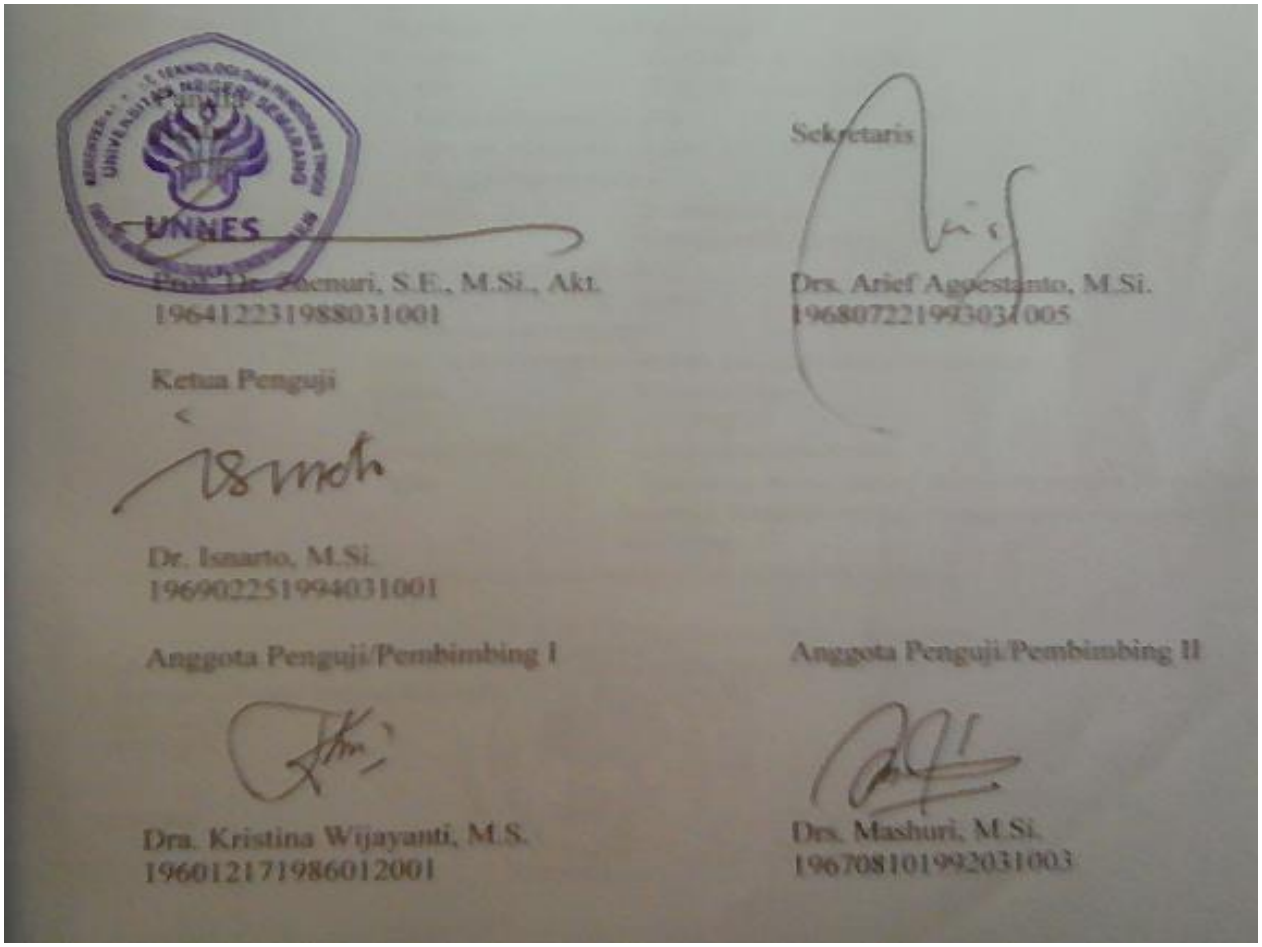
Skripsi yang berjudul

Penerapan Matriks dengan Koefisien Binomial Newton sebagai Pengaman Pesan Menggunakan Algoritma Hill Cipher disusun oleh

Khayatul Fahmi

4111413016

telah dipertahankan dihadapan sidang Panitia Ujian Skripsi FMIPA UNNES pada tanggal 02 Agustus 2018.



MOTTO DAN PERSEMBAHAN

MOTTO

Dari proses yang baik akan diperoleh hasil yang dapat diterima

PERSEMBAHAN

Teruntuk Keluargaku, Bapak, & Ibu

PRAKATA

Puji syukur penulis panjatkan kepada Allah SWT yang Maha Pengasih dan Penyayang, atas limpahan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "**Penerapan Matriks dengan Koefisien Binomial Newton sebagai Pengaman Pesan Menggunakan Algoritma Hill Cipher**".

Penulis menyadari dalam menyelesaikan skripsi ini memperoleh banyak bantuan dan dukungan dari berbagai pihak. Untuk itu, dengan rasa hormat, penulis menyampaikan terima kasih kepada.

1. Prof. Dr. Fathur Rokhman, M.Hum. Rektor Universitas Negeri Semarang.
2. Prof. Dr. Zaenuri S.E, M.Si,Akt. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Semarang.
3. Drs. Arief Agoestanto, M.Si. Ketua Jurusan Matematika FMIPA Universitas Negeri Semarang.
4. Dr. Isnarto M.Si. Penguji yang telah memberikan arahan dan masukan dalam memperbaiki skripsi ini.
5. Dr. Rochmad M.Si. Dosen wali Prodi Matematika Jurusan Matematika FMIPA Universitas Negeri Semarang angkatan 2013.
6. Dra. Kristina Wijayanti, M.S. Pembimbing yang telah memberikan arahan dan masukan dalam penyelesaian skripsi ini.
7. Drs. Mashuri, M.Si. Pembimbing yang telah memberikan arahan dan masukan dalam penyelesaian skripsi ini.
8. Bapak dan Ibu Dosen Jurusan Matematika serta staf Tata Usaha Universitas Negeri Semarang yang telah membekali penulis dengan ilmu selama mengikuti perkuliahan dan penulisan skripsi.

9. Orang Tua dan Keluarga yang selalu memberika doa, dukungan, dan semangat.
10. Teman-teman seangkatan Matematika 2013 yang selalu memberi dukungan, motivasi, dorongan, dan doa.
11. Semua pihak yang tidak dapat disebutkan satu per satu yang telah memberikan bantuan.

Semoga skripsi ini dapat memberikan manfaat bagi penulis dan para pembaca. Terima kasih.

Semarang, 02 Agustus 2018

Penulis

ABSTRAK

Fahmi, Khayatul. 2018. *Penerapan Matriks dengan Koefisien Binomial Newton sebagai Pengaman Pesan Menggunakan Algoritma Hill Cipher*. Skripsi, Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Semarang. Pembimbing Pertama Dra Kristina Wijayanti, MS dan Pembimbing Kedua Drs. Mashuri, M.Si.

Kata kunci : Pengaman Pesan, Koefisien Binomial, Algoritma Hill Cipher

Matriks dapat digunakan sebagai kunci pada proses pengamanan pesan atau kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Terdapat dua jenis algoritma kriptografi yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsinya. Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik (public key)* dan *kunci rahasia (secret key)*. Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Hill cipher adalah salah satu teknik kriptografi dari jenis algoritma simetris dimana kunci yang digunakan dalam proses enkripsi/dekripsi menggunakan kunci yang sama.

Hill cipher merupakan teknik kriptografi yang menggunakan matriks persegi sebagai kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. Masalah yang umum muncul pada algoritma ini terletak pada pemilihan kunci. Pemilihan kunci yang dilakukan secara sebarang dapat menyebabkan kegagalan dalam proses dekripsi, karena algoritma ini memberikan syarat kunci yang digunakan dapat dibalik atau memiliki invers (*invertible*). Pada penelitian ini, matriks yang digunakan pada proses pengamanan adalah matriks yang dibagun dengan memanfaatkan koefisien binomial Newton sebagai entri dalam matriks kunci. Jika A adalah matriks persegi ordo k x k yang entri baris ke-n kolom ke-r adalah H_r^n dengan $n, r \in \{1,2,3 \dots, k\}$, maka $det\ (A) = 1$.

Analisis yang dilakukan yakni melihat tingkat keacakan berdasarkan nilai entropy. Entropy, dalam teori informasi menyatakan derajat ketidakpastian. Secara matematis entropy dinyatakan dalam persamaan berikut: $H(X) = -\sum_{i=0}^{n} P(x_i) \log_2 P(x_i)$, dengan $H(X)$ menyatakan nilai entropy dan $P(x_i)$ menyatakan probabilitas kemunculan karakter ke. Dalam anlisis data, konversi karakter yang digunakan sebanyak 73. Untuk nilai entropy maksimal yang diperoleh adalah 6,18982455888002 bit. Hasil analisis berdasarkan nilai entropy diperoleh informasi bahwa, semakin panjang karakter yang berbeda semakin tinggi nilai entropy yang diperoleh dan sebaliknya.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Matematika merupakan ilmu pengetahuan yang luas dalam penerapannya, seperti halnya dalam bidang teknologi dan informasi. Hampir semua bidang pengetahuan umum atau teknologi, ilmu murni, maupun penerapannya memerlukan peran matematika sebagai ilmu bantunya.

Zaman akan terus berkembang dan kebutuhan akan informasi semakin meningkat. Salah satu contoh nyata adalah kebutuhan menggunakan internet. Perkembangan teknologi serta informai yang semakin marak, internet tidak lagi menjamin penyediaan informasi yang aman. Selain itu dalam dunia internet banyak sekali kasus kejahatan, seperti pencurian data yang bersifat rahasia dilakukan oleh pihak tidak bertanggung jawab.

Keamanan informasi merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama informasi-informasi yang sifatnya rahasia yang hanya diketahui pihak-pihak tertentu saja, apalagi jika pengirimannya dilakukan melalui jaringan publik. Jika data atau suatu pesan tersebut tidak diamankan terlebih dahulu, maka kemungkinan besar dapat disadap atau diketahui isinya oleh pihak tidak bertanggung jawab. Hal ini merupakan salah satu masalah dalam sebuah pengiriman dan pengamanan data atau pesan, maka diperlukan sebuah cara agar permasalahan tersebut dapat terselesaikan.

Pengamanan data melalui metode penyandian telah lama berkembang sejak zaman Yunani sekitar tahun 400 SM. Mereka menggunakan alat yang

disebut *scytale*. Alat ini terbuat dari sebuah pita panjang yang dililitkan pada sebatang silinder. Pesan yang akan dikirim ditulis horizontal baris per baris. Bila dilepaskan, maka huruf-huruf didalamnya telah tersusun membentuk pesan rahasia. Untuk membaca pesan, penerima melilitkan kembali pada batang silinder dengan diameter yang sama. Teknik ini dikenal dengan nama transposisi cipher yang merupakan metode sandi tertua.

Kriptografi merupakan ilmu yang mempelajari bagaimana mengamankan sebuah pesan atau data yang dikirim oleh *sender* (pengirim pesan) dan diterima oleh *receiver* (penerima pesan) dengan aman, yaitu dengan menjadikan pesan asli (*plaintext*) yang akan dikirim menjadi sebuah kode-kode atau sandi yang tidak dapat dimengerti melalui sebuah proses yang disebut dengan enkripsi (Rathi dan Atya, 2014). Sedangkan untuk mengolah sandi yang telah terbentuk dari proses enkripsi menjadi pesan asli, disebut dengan dekripsi (Rathi dan Atya, 2014).

Secara umum dalam ilmu kriptografi dikenal dua algoritma, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi sama dengan kunci dekripsinya (Kromodimoeljo, Sentot. 2009). Contoh algoritma simetris adalah Hill Cipher (Ravan dan Nigavekar, 2013). Sedangkan apabila proses enkripsi dan dekripsi menggunakan kunci yang berbeda maka disebut algoritma asimetris, dimana kunci yang digunakan untuk enkripsi disebut dengan *public-key* dan kunci untuk dekripsinya disebut *private-key* (Kromodimoeljo, Sentot. 2009).

Hill Cipher adalah teknik kriptografi yang memanfaatkan matriks dan operasinya dalam melakukan proses enkripsi dan dekripsi. Matriks sendiri didefinisikan sebagai sususan segi empat siku-siku dari bilangan-bilangan.

Bilangan-bilangan dalam susunan tersebut dinamakan entri dalam matriks (Anton, 1995).

Proses enkripsi pada Hill Cipher dilakukan dengan cara mengalihkan matriks kunci dengan matriks *plaintext* yang kemudian diperoleh *ciphertext*. Untuk proses dekripsi tekniknya sama dengan proses enkripsi hanya saja kunci yang digunakan merupakan invers dari kunci pada proses enkripsi. Sedangkan invers matriks didefinisikan, jika A adalah matriks persegi, dan jika terdapat matriks B yang ukurannya sama sedemikian rupa $AB = BA = I$, maka A dikatakan mempunyai invers (*invertible*) dan B disebut invers (*inverse*) dari A. Jika matriks B tidak dapat didefinisikan, maka A dinyatakan matriks singular (Anton, 1995).

Masalah yang terdapat pada kriptografi menggunakan algoritma Hill Cipher. Proses pengaman pesan pada algoritma Hill Cipher dibagi menjadi dua tahap, pertama enkripsi yang kedua dekripsi. Pada proses dekripsi masalah yang umum mucul adalah pada matriks kunci. Matriks kunci yang disyaratkan pada Hill Cipher harus *invertible*. Pemilihan suatu matriks kunci yang dilakukan secara sebarang, menyebabkan ada kemungkinan matriks dipilih tersebut tidak mempunyai invers sedangkan pada Hill Cipher mensyaratkan matriks kunci harus *invertible* (Ravan dan Nigavekar, 2013). Masalah lain saat syarat matriks kunci telah terpenuhi yaitu invers dari matriks kunci yang bukan bilangan bulat. Ketika invers dari matriks kunci bukan bilangan bulat, maka harus diubah dengan prosedur tertentu untuk menghasilkan invers matriks kunci yang elemen-elemennya bilangan bulat. Jadi masalah mendasar yang sering muncul pada algoritma Hill Cipher yaitu pada matriks kunci itu sendiri.

Ide awal dari invers matriks tergeneralisasi (*Generalized Inverse of Matrix*) adalah menggeneralisasi pengertian invers matriks. Dari teori invers matriks tergeneralisasi tersebut maka ada kemungkianan untuk matriks dengan ordo *m x n* atau ordo *n x n* dapat dicari inversnya. Beberapa jenis matriks ditinjau dari unsur pembangunnya ada matriks Hermite dan matriks real. Matriks yang memuat entri bilangan kompleks disebut matriks Hermite.

Koefisien binomial Newton merupakan bilangan real dengan pola yang cukup unik. Pola yang dibangun menggunakan aturan kombinasi $C(n,k)$. Matriks yang dibangun dari koefisien binomial Newton merupakan bentuk matriks khusus dari matriks dengan unsur bilangan real.

Berdasarkan uraian latar belakang di atas, maka perlu dilakukan penelitian lebih lanjut terhadap proses pengaman pesan atau kriptografi dengan menggunakan matriks dan koefisien binomial Newton dengan topik "Penerapan Matriks dengan Koefisien Binomial Newton sebagai Pengaman Pesan Menggunakan Algoritma Hill Cipher".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan maka rumusan masalah dalam penelitian ini adalah sebagai berikut.

1. Bagaimana membangun matriks dengan koefisien binomial Newton sebagai matriks kunci dalam pengaman pesan menggunakan algoritma Hill Cipher?
2. Bagaimana penerapan matriks dengan koefisien binomial Newton sebagai pengaman pesan menggunakan algoritma Hill Cipher?

3. Bagaimana tingkat keacakan dari hasil proses enkripsi Hill Cipher menggunakan matriks kunci dengan entri koefisien binomial Newton?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan dari penelitian ini adalah sebagai berikut.

1. Mengetahui proses pembentukan matriks dengan koefisien binomial Newton sebagai matriks kunci dalam pengaman pesan menggunakan algoritma Hill Cipher.
2. Mengetahui penerapan matriks dengan koefisien binomial Newton dalam pengaman pesan menggunakan algoritma Hill Cipher.
3. Mengetahui tingkat keacakan dari hasil proses enkripsi Hill Cipher menggunakan matriks kunci dengan entri koefisien binomial Newton.

1.4 Batasan Masalah

Untuk mendapatkan hasil penelitian yang lebih terarah, maka ditentukan batasan penelitian sebagai berikut.

1. Matriks kunci yang digunakan pada penelitian ini dimulai dari ordo 2×2 sampai ordo 11×11.
2. Matriks yang digunakan adalah matriks yang dibangun dari koefisien binomial Newton.

1.5 Manfaat Penelitian

1. Penulis

   Penulisan skripsi sebagai sarana untuk latihan membuat kariya ilmiah yang harapannya dapat berkelanjutan ke depannya. Manfaat lain

yang diperoleh yakni memotivasi diri dalam mengembangkan ilmu pengetahuan yang dimiliki terutama dibidang Aljabar dan penerapannya.

2. Mahasiswa Jurusan Matematika

   Penulisan skripsi ini bermanfaat untuk mahasiswa sebagai referensi ilmu pengetahuan dalam kajian bidang kriptografi yang merupakan penerapan dari ilmu Aljabar.

3. Almamater Unnes

   Menambah referensi karya ilmiah mahasiswa yang dapat dijadikan rujukan bagi peneliti dalam mengembangkan ilmu dibidang Aljabar.

1.6 Sistematika Penulisan

Secara garis besar, penulisan skripsi ini terdiri atas tiga bagian, yaitu bagian awal, bagian isi, dan bagian akhir, yang masing -masing diuraikan sebagai berikut.

1. Bagian Awal

   Bagian ini terdiri atas halaman judul, pernyataan keaslian tulisan, halaman pengesahan, persembahan, motto, prakata, abstrak, daftar isi, daftar tabel, dan daftar lampiran.

2. Bagian Isi

   Bagian ini merupakan bagian laporan penelitian yang terdiri atas lima bab dengan rincian sebagai berikut.

   a. BAB I PENDAHULUAN

      Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan skripsi.

b. BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori yang mendasari pemecahan masalah-masalah yang berhubungan dengan rumusan masalah.

c. BAB III METODE PENELITIAN

Bab ini berisi prosedur pemecahan masalah, metode analisis data, dan penarikan kesimpulan.

d. BAB IV HASIL DAN PEMBAHASAN

Bab ini merupakan pembahasan dari penelitian yang dilakukan.

e. BAB V PENUTUP

Bab ini merupakan jawaban dari rumusan masalah dan berisi simpulan hasil penelitian dan saran yang berkaitan dengan hasil penelitian yang diperoleh.

3. Bagian Akhir

Bagian ini terdiri dari daftar pustaka dan lampiran-lampiran.

BAB II

TINJAUAN PUSTAKA

2.1 Kriptografi

Pada bagian ini akan dibahas tentang, sejarah kriptografi, definisi kriptografi, sistem kriptografi, tujuan kriptografi, algoritma kriptografi, dan prinsip kerja kriptografi.

2.1.1 Sejarah Kriptografi

Kriptografi sudah digunakan sekitar 40 abad yang lalu oleh orang-orang Mesir untuk mengirim pesan ke pasukan yang berada di medan perang dan agar pesan tersbut tidak terbaca oleh musuh. Sekitar 400 SM, kriptografi digunakan oleh bangsa Spartan dalm bentuk sepotong papirus atau perkamen yang dibungkus dengan batang kayu. Pada zaman Romawi Kuno, ketika Julius Caesar ingin mengirimkan pesan rahasia pada seorang jendral dimedan perang. Pesan tersebut harus dikirimkan melalui seorang prajurit, tetapi karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka ditengah jalan. Di sini Julius Caesar memikirkan bagaimana mengatasinya yaitu dengan mengacak isi pesan tersebut menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh Jendralnya saja. Tentu sang Jendral telah diberi tahu sebelumnya bagaimana cara membaca pesan yang teracak tersebut, karena telah mengetahui kuncinya. Pada tahun 1992 Lester S. Hill menciptakan Hill Cipher. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan

teknik analisis frekuensi. Hill Cipher tidak mengganti semua abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Hill Cipher yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher* karena teks yang diproses akan dibagi menjadi blok-blok dengankuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama bemlum tentu dipetakan menjadi karakter yang sama pula (Stinson, D.R.1995).

Pada perang dunia kedua, Jerman menggunakan mesin enigma atau juga disebut dengan mesin rotor yang digunakan Hilter untuk mengirim pesan kepada tentaranya di medan perang. Jerman sangat percaya bahwa pesan yang dienkripsi menggunakan ennigma tidak dapat dipecahkan. Tapi anggapan itu keliru, setelah bertahun-tahun sekutu mempelajarinya dan berhasil memecahkankode-kode tersebut. Setelah Jerman mengetahui bahwa enigma dapat dipecahkan, maka enigma mengalami beberapa kali perubahan. Enigma yang digunakan Jerman dapat mengenkripsi suatu pesan sehingga mempunyai 15×10^{18} kemungkinan untuk dapat mendekripsi pesan. Perkembangan komputer dan sistem komunikasi pada tahun 60-an berdampak pada permintaan pada pihak-pihak tertentu sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. Dimulai dari usaha Feistel dari IMB di awal 70-an dan mencapai puncaknya pada 1977 dengan pengangkatan DES *(Data Encryption Standard)* sebagai standar pemrosesan informasi federal Amerika Serikat untuk mengenkripsi informasi yang belum diklasifikasi. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah. Pengembangan paling

mengejutkan dalam sejarah kriptografi terjadi pada tahun 1976 saat Diffie dan Hellman mempublikasikan *"New Directions in Cryptography"*. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret. Meskipun Diffie dan Hellman tidak memiliki dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi. Pad 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik yang sekarang disebut RSA. Rancangan RSA berdasar pada masalah faktorisasi bilangan yang sulit, dan mengingatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran.

2.1.2 Definisi Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes, Oorschot and Vanstone, 1996). Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan teknik kriptografi. Kriptografi dapat pula diartikan sebagai ilmu sekaligus seni untuk menjaga keamanan pesan (Munir, 2012). Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

2.1.3 Sistem Kriptografi

Suatu sistem kriptografi merupakan sebuah himpunan algoritma, seluruh kemungkinan *plaintext, ciphertext,* kunci, dan proses manajemen kunci yang digunakan. Sistem kriptografi merupakan suatu fasilitas untuk mengkonversikan *plaintext* menjadi *ciphertext*, dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan proses *plaintext* menjadi *ciphertext* tertentu disebut dengan set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci. Secara umum, kunci–kunci yang digunakan untuk proses enkripsi dan dekripsi tidak perlu identik, tergantung dari sistem yang digunakan.

Definisi 2.1 (Buchman, 2000)

Sistem kriptografi *(cryptosystem)* tersusun dari 5 parameter *(*$P, C, K, \mathcal{E}, D$*)* yang memenuhi kondisi sebagai berikut.

(1)P adalah himpunan *plaintext*;

(2)C adalah himpunan *ciphertex;*

(3)K adalah himpuan kunci;

(4)untuk setiap $k \in K$, terdapat proses enkripsi $e_K \in \mathcal{E}$ dan proses dekripsi $d_k \in D$. Untuk $e_K : P \to C$ dan $d_K : C \to P$ adalah suatu fungsi sedemikin sehingga $d_K\left(e_K(x)\right) = x$ untuk setiap elemen *plaintext* $x \in P$.

2.1.4 Tujuan Kriptografi

Beberapa tujuan dari kriptografi juga merupakan aspek keamanan informasi. Tujuan kriptografi (Menezes, 1997) antara lain.

1. *Kerahasiaan*, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
2. *Integritas data,* adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain kedalam data sebenarnya.
3. *Autentikasi*, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendriri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri, informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. *Non-repudiation* (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut (Menezes, Oorschot and Vastone).

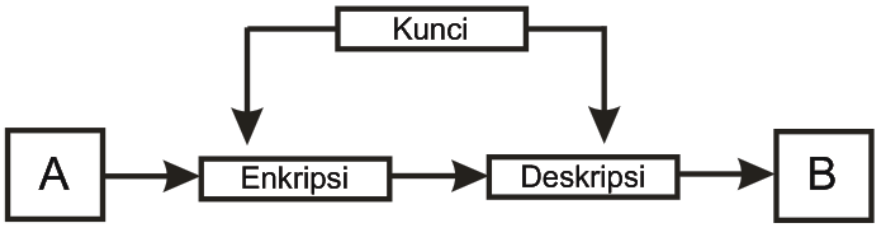
2.1.5 Algoritma Kriptografi

2.1.5.1 Algoritma Simetris

Algoritma Simetris adalah algoritma kriptografi yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsinya (Kromodimoeljo, 2010). Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan

algoritma simetris tergantung pada kunci, membocorkan kunci pada yang tidak berhak berarti sama dengan membocorkan pesan rahasia. Agar komunikasi tetap terjaga dan aman, kunci harus dirahasiakan. Algoritma Simetris sering juga disebut dengan algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci.

Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya. Contoh dari algoritma kriptografi simetris adalah Cipher Permutasi, Cipher Substitusi, Vernam Cipher, Caesar Cipher, Cipher Hill, OTP, RC6, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rajndael (AES), Blowfish, GOST, A5, Kasumi, DES, dan IDEA.



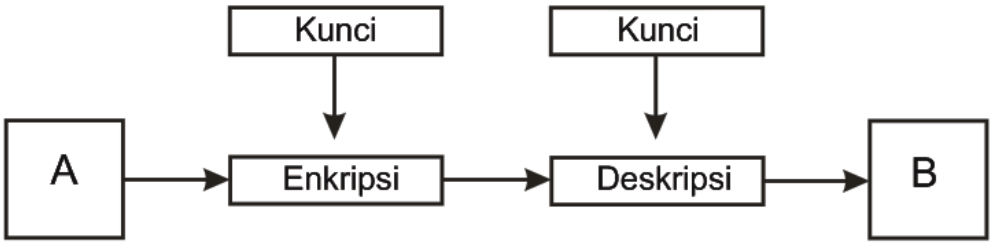
Gambar 2.1 Skema Algoritma Simetris

Ada beberapa kelebihan menggunakan algoritma simetris yang sudah diketahui yaitu (1) kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetris walaupun hal ini berbanding lurus dengan penambahan ukuran file (Quasim, 2013), (2) kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file, semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi (Basri, 2016).

2.1.5.2 Algoritma Asimetris

Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik (public key)* dan *kunci rahasia (secret key)*. Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan (Kromodimoeljo, 2010).

Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun diantara mereka tidak ada kesepakatanmengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.



Gambar 2.2 Skema Algoritma Asimetris

Algoritma asimetris pertama kali dipublikasikan oleh Diffie dan Hellman pada tahun 1976 dalam papernya yang berjudul *"New Directions in Cryptography"*. Menurut Diffie dan Hellman dalm melakukan proses enkripsi, sering digunakan *plaintext* berupa data ataupun pesan yang besar, sehingga membutuhkan waktu yang lama apabila dilakukan proses sekaligus pada *plaintext*

tersebut. Oleh karena itu, *plaintext* dapat dipotong-potong menadi beberapa blok-blok yang sama panjang. Kemudian dari blok-blok yang diperoleh tersebut dilakukan proses enkripsi, dan hasil *ciphertext*nya dapat didekripsi dan digabungkan kembali menjadi *plaintext*.

2.1.6 Prinsip Kerja kriptografi

Prinsip kerja kriptografi terdapat dua fungsi mendasar, yaitu fungsi enkripsi dan fungsi dekripsi.

Fungsi enkripsi yaitu fungsi untuk mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan sandi (*ciphertext*). Fungsi enkripsi secara matematis dapat ditulis sebagai berikut:

$$C = E\ (P)$$

dimana

C : pesan sandi (*ciphertext*);

E : fungsi enkripsi;

P : pesan asli (*plaintext*).

Fungsi dekripsi yaitu fungsi untuk mengubah suatu pesan sandi (*ciphertext*) menjadi pesan asli (*plaintext*). Fungsi dekripsi dapat ditulis sebagai berikut:

$$P = D\ (C)$$

dimana

P : pesan asli (*plaintext*);

D : fungsi dekripsi;

C : pesan sandi (*ciphertext*).

Fungsi enkripsi dan fungsi dekripsi biasanya diberi suatu parameter tambahan yang disebut sebagai istilah kunci (Rohmanu, 2017).

2.2 Hill Cipher

Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929 (Stinson, 1995), yang merupakan penerapan aritmetika modulo pada kriptografi (Thangarasu & Selvakumar, 2015). Teknik kriptografi ini menggunakan matriks persegi sebagai kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Hill Cipher tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Pasaribu, 2016).

Hill Cipher yang merupakan *polyalphabetic* cipher dapat dikategorikan sebagai *block-cipher* (Forouzan, 2006) karena teks yang akan diproses dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula.

Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja (Pasaribu, 2016). Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext*. Teknik kriptanalisis ini disebut known-plaintext attack (Farmambar, 2012).

2.2.1 Dasar Teknik Hill Cipher

Dasar teknik Hill Cipher adalah aritmetika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks $n \times n$ dengan *n* merupkan ukuran blok. Matriks *K* yang menjadi kunci dalam kriptografi ini haruslah matriks yang *invertible*, hal ini dikarenakan saat kunci tidak *invertible* maka pada saat proses deskripsi tidak bisa dilakukan. Secara matematis matriks kunci yang digunakan memenuhi syarat sebagai berikut:

$$K.K^{-1} = I.$$

Matriks *K* sebagia kunci untuk proses enkripsi, sedangkan K^{-1} sebagai kunci pada proses dekripsi.

Berikut merupakan langkah-langkah dalam pengamanan pesan menggunakan algoritma Hill Cipher.

1. Menentukan *plaintext* yang akan disandi
2. Menentukan matriks kunci yang akan digunakan.
3. Mengubah *plaintext* menjadi bentuk numerik sesuai dengan konversi yang telah ditetapkan. Banyaknya karakter konversi yang digunakan 73.
4. Menghitung banyaknya karakter pada *plaintext*. Selanjutnya banyaknya karakter dari *plaintext* dibagi dengan ordo dari matriks kunci yang telah ditentukan. Jika pembagian memiliki sisa > 0, maka *palintext* ditambah dengan karakter tambahan (karakter boneka) sampai sisa hasil bagi sama dengan 0. Karakter boneka yang digunakan adalah titik (.).
5. Menyusun *plaintext* yang berupa numerik menjadi suatu matriks.

6. Mengalihkan matriks kunci dengan matriks *plaintext* sehingga diperoleh matriks baru dari hasil perkalian kedua matriks tersebut.
7. Matriks baru hasil dari perkalian matriks kunci dengan matriks *plaintext* dalam modulo 73 dan selanjutnya dikonversi menjadi huruf/teks sesuai tabel konversi.
8. Sehingga diperoleh *ciphertext* atau karakter sandi yang merupakan hasil dari proses enkripsi.
9. Untuk mengubah *ciphertext* menjadi *plaintext* menggunakan proses dekripsi.
10. Menentukan invers matriks kunci dari matriks kunci yang digunakan pada proses enkripsi.
11. Mengubah *ciphertext* menjadi bentuk numerik sesuai dengan konversi yang telah ditetapkan
12. Menyusun *ciphertext* yang berupa numerik menjadi suatu matriks.
13. Kalihkan invers matriks kunci dengan matriks *ciphertext* dalam modulo 73.
14. Selanjutnya konversikan sesuai tabel konversi, diperoleh teks asli kembali (*plaintext*).
15. Pesan dapat dibaca kembali.

2.2.2 Enkripsi Hill Cipher

Enkripsi adalah proses penyandian pesan atau proses mengubah *plaintext* menjadi bahasa sandi (*ciphertext*) dengan aturan tertentu. Proses enkripsi pada Hill Cipher dilakukan per blok *plaintext* (vektor kolom). Ukuran blok tersebut sama dengan ukuran matriks kunci yang digunakan. Sebelum membagi menjadi

deretan blok-blok, *plaintext* terlebih dahulu dikonversi menjadi bentuk numerik. Secara matematis proses enkripsi dinyatakan sebagai berikut:

$$E_C = K\ (P)$$

dimana

E_C : fungsi enkripsi (*Ciphertext)*;

K : kunci enkripsi (matriks);

P : pesan asli (*Plaintext).*

Contoh 2.1

Diketahui *plaintext* "mulai"

Plaintext dikonversi dalam bentuk numerik "38 46 37 26 34"

P = 38 46 37 26 34

Plaintext tersebut akan di enkripsi dengan menggunakan kunci K yang merupakan matrisk 2 x 2

$$K = \begin{bmatrix} 1 & 1 \\ 2 & 3 \end{bmatrix}$$

Karena matriks kunci berukuran 2, maka banyaknya karakter *plaintext* dibagi 2 kemudian disusun dalam vektor kolom. Jika banyaknya karakter pada *plaintext* ganjil maka karakter terahir ditambah 1 karakter lain. Hal ini bertujuan agar setiap blok mempunyai ukuran yang sama, sehingga diperoleh blok dari *plaintext*.

Cara penyusunannya adalah perblok disusun menjadi vektor kolom, diperoleh vektor kolom *plaintext sebagai berikut*:

$$P_1 = \begin{bmatrix} 38 \\ 46 \end{bmatrix};\ P_2 = \begin{bmatrix} 37 \\ 26 \end{bmatrix};\ P_3 = \begin{bmatrix} 34 \\ 64 \end{bmatrix}.$$

Pada P_3 ditambah satu karakter, karena hasil bagi dari ordo kunci terhadap banyaknya karakter *plaintext* tidak sama dengan nol. Karakter tambahan ini adalah karakter "*titik*".

Untuk meng-enkripsi P_1, proses yang dilakukan adalah bentuk hasil kali matriks $K(P_1)$

$$\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}\begin{bmatrix}38\\ 46\end{bmatrix} = \begin{bmatrix}84\\ 214\end{bmatrix} \qquad (1)$$

Namun, terdapat masalah dalam hal ini, karena bilangan 84 dan 214 tidak mempunyai abjad yang setara (tabel 2.1). Untuk memecahkan masalah ini kita membuat kesepakatan sebagai berikut.

Bilamana hasil bilangan yang diperoleh lebih besar dari 73, akan digantikan dengan sisa yang dihasilkan bilamana bilangan ini dibagi 73.

Karena sisa setelah pembagian oleh 73 adalah salah satu dari bilangan-bilangan bulat 0, 1, 2, 3 ,4, ... , 72, dengan prosedur ini akan selalu menghasilkan bilangan bulat dengan abjad yang setara.

Jadi dalam (1) kita gantikan 84 dan 214 dengan 11 dan 68, yang merupakan sisa setelah pembagian 84 dan 214 oleh 73. Karakter yang mewakili 11 68 berturut-turut adalah "L)".

Untuk meng-enkripsi P_2, proses yang dilakukan adalah bentuk hasil kali matriks $K(P_2)$

$$\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}\begin{bmatrix}37\\ 26\end{bmatrix} = \begin{bmatrix}63\\ 152\end{bmatrix} \qquad (2)$$

Dengan menggunakan kesepakatan di atas, jadi dalam (2) kita gantikan 152 dengan 6, yang merupakan sisa setelah pembagian 152 oleh 73. Karakter yang mewakili 63 6 berturut-turut adalah "!G".

Untuk meng-enkripsi P_3, proses yang dilakukan adalah bentuk hasil kali matriks $K(P_3)$

$$\begin{bmatrix}1 & 1\\ 2 & 3\end{bmatrix}\begin{bmatrix}34\\ 64\end{bmatrix} = \begin{bmatrix}98\\ 260\end{bmatrix} \qquad (3)$$

Dengan menggunakan kesepakatan di atas, jadi dalam (3) kita gantikan 98 dan 260 dengan 25 dan 41, yang merupakan sisa setelah pembagian 98 dan 260 oleh 73. Karakter yang mewakili 25 41 berturut-turut adalah "Zp".

Setelah melakukan proses enkripsi pada P_1, P_2, dan P_3 diperoleh *ciphertext* "L)!GZp".

2.2.3 Dekripsi Hill Cipher

Proses dekripsi atau bisa disebut proses kebalikan dari enkripsi, yaitu proses penerjemahan kembali dari kalimat sandi (*ciphertext*) menjadi kalimat asli (*plaintext*). Proses ini pada dasarnya memiliki metode yang sama dengan proses enkripsi Hill Cipher. Hanya saja kunci yang digunakan merupakan invers dari kunci yang digunakan dalam proses enkripsi. Secara matematis proses dekripsi dinyatakan sebagai berikut:

$$D_P = K^{-1}(C)$$

dimana

D_p : fungsi dekripsi (*plaintext*)*;*

K^{-1} : kunci dekripsi (matriks);

C : pesan sandi (*ciphertext).*

Contoh 2.2

Diketahui ciphertext "L)!GZp".

Ciphertext dikonversi dalam bentuk numerik "11 68 63 6 25 41"

C = 11 68 63 6 25 41

Ciphertext tersebut akan didekripsi dengan menggunakan invers dari kunci yang digunakan saat proses enkripsi.

$$K^{-1} = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix}$$

Karena matriks kunci berukuran 2, maka banyaknya karakter dari *ciphertext* dibagi 2 kemudian disusun dalam vektor kolom. Diperoleh vektor kolom dari *ciphertext* sebagai berikut:

$$C_1 = \begin{bmatrix} 11 \\ 68 \end{bmatrix};\ C_2 = \begin{bmatrix} 63 \\ 6 \end{bmatrix};\ C_3 = \begin{bmatrix} 25 \\ 41 \end{bmatrix}.$$

Untuk men-dekripsi C_1, proses yang dilakukan adalah bentuk hasil kali matriks $K^{-1}(C_1)$

$$\begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix}\begin{bmatrix} 11 \\ 68 \end{bmatrix} = \begin{bmatrix} -35 \\ 46 \end{bmatrix} \qquad (1)$$

Dengan menggunakan kesepakatan pada proses enkripsi diatas diperoleh bilangan pengganti atas -35 adalah 38 dan untuk 46 tetap karena tidak melebihi 73. Karakter yang mewakili 38 46 berturut-turut adalah “mu”.

Untuk men-dekripsi C_2, proses yang dilakukan adalah bentuk hasil kali matriks $K^{-1}(C_2)$

$$\begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix}\begin{bmatrix} 63 \\ 6 \end{bmatrix} = \begin{bmatrix} 183 \\ -120 \end{bmatrix} \qquad (2)$$

Dengan menggunakan kesepakatan pada proses enkripsi diatas diperoleh bilangan pengganti atas 183 dan -120 secara berturut-turut adalah 37 dan 26. Karakter yang mewakili 37 26 berturut-turut adalah “la”.

Untuk men-dekripsi C_3, proses yang dilakukan adalah bentuk hasil kali matriks $K^{-1}(C_3)$

$$\begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 25 \\ 41 \end{bmatrix} = \begin{bmatrix} 34 \\ -9 \end{bmatrix} \quad (3)$$

Dengan menggunakan kesepakatan pada proses enkripsi diatas diperoleh bilangan pengganti atas -9 adalah 64 dan untuk 34 tetap karena tidak melebihi 73. Karakter yang mewakili 34 64 berturut-turut adalah "i.".

Setelah melakukan proses dekripsi pada C_1, C_2, dan C_3 diperoleh kalimat asli atau *plaintext*-nya adalah "mulai.".

2.3 Tabel Konversi

Penggunaan modulo yang bukan merupakan bilangan prima, menyebabkan terbatasnya matriks kunci yang dapat digunakan (Hidayat & Alawiyah, 2013). Proses perhitungan pada enkripsi maupun dekripsi menggunakan modulo 73, artinya inputan data ada 73 karakter. Karakter ini terdiri dari huruf A, B, C, ..., Z, a, b, c, ..., z, angka yang dimulai dari 0, 1, 2, 3, ..., 9, dan 11 karakter tanda baca yakni @, !, [titik], [*space*], &, (,), [koma], /, ?, dan %. Berikut merupakan tabel konversi karakter ke bilangan.

Tabel 2.1 Konversi Karakter

A	***B***	***C***	***D***	***E***	***F***	***G***	***H***	***I***	***J***	***K***	***L***	***M***	***N***	***O***	***P***
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Q	***R***	***S***	***T***	***U***	***V***	***W***	***X***	***Y***	***Z***	***a***	***B***	***c***	***d***	***e***	***f***
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
g	***h***	***i***	***j***	***k***	***l***	***m***	***n***	***o***	***p***	***q***	***R***	***s***	***t***	***u***	***v***
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
w	***x***	***y***	***z***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***0***	***@***	***!***
47	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
.	***␣***	***&***	***(***	***)***	***,***	***/***	***?***	***%***							
64	65	66	67	68	69	70	71	72							

2.4 Aritmetika modular

Definisi 2.2 (Stinson, D.R 1995)

Diberikan $a, n \in Z$. Bilangan bulat a dikatakan membagi n jika terdapat $b \in Z$ sedemikian hingga $n = ab$. Jika a membagi n, maka a disebut pembagi n dan n merupakan kelipatan a. Bilangan bulat a yang membagi n ditulis $a|n$.

Contoh 2.3

(1) $2|6$; (2) $(-6)|24$; (3) $(-4)|(-20)$.

Dalam arimetika modular diberikan sebuah bilangan bulat positif m yang disebut dengan modulus, dan dua bilangan bulat sebarang yang selisihnya sebesar kelipatan bulat dari modulus tersebut diangggap sama atau ekuivalen dengan modulus tersebut (Anton dan Rorres, 2000).

Definisi 2.3 (Anton dan Rorres, 2000)

Jika m adalah sebuah bilangan bulat positif, a dan b adalah bilangan bulat sebarang, maka dapat dikatakan bahwa a ekuivalen dengan b modulo m, ditulis $a = b \ (mod\ m)$, jika $a - b$ adalah kelipatan bilangan bulat dari m.

Contoh 2.5

(1) $7 = 2 \ (mod\ 5)$; (2) $17 = 2 \ (mod\ 3)$; (3) $15 = 0 \ (mod\ 5)$.

Jika a adalah sebuah bilangan bulat tak negatif, maka residu dari modulo m secara sederhana adalah sisa yang dihasilkan ketika a dibagi dengan m. Untuk sebarang bilangan bulat a, sisa dapat ditentukan dengan menggunakan Teorema 2.1.

Teorema 2.1 (Anton dan Rorres, 2000)

Untuk sebarang bilangan bulat a dan modulus m, misalkan

$R =$ sisa dari $\frac{|a|}{m}$, maka residu r dari modulo m dapat ditentukan dengan

(1) $r = R$ jika $a \geq 0$

(2) $r = m - R$ jika $a < 0$ dan $R \neq 0$

(3) $r = 0$ jika $a < 0$ dan $R = 0$

Bukti

Kasus $a \geq 0$

Dipunyai $R =$ sisa dari $\frac{|a|}{m}$

Jelas $\frac{|a|}{m} = \frac{a}{m}$. Karena R adalah sisa dari $\frac{|a|}{m} = \frac{a}{m}$, maka residu r dari $(modulo\ m) = R$. Jadi $r = m$.

Kasus $a < 0$

Dipunyai $R =$ sisa dari $\frac{|a|}{m}$

Jelas $\frac{|a|}{m} = \frac{-a}{m}$. Karena R adalah sisa dari $\frac{|a|}{m} = \frac{-a}{m}$, maka residu r dari $(modulo\ m) = m - R$.

Jika $R = 0$, jelas $m - R = m - 0 = m$. Jadi residu r dari $(modulo\ m) = 0$.

Contoh 2.6

Tentukan residu modulo 25 dari (a) 77; (b) -37; dan (c) -25

Penyelesaian

(a) Pembagian $|77| = 77$ dengan 25 menghasilkan sisa $R = 2$, sehingga $r = 2$. Dengan demikian, $77 = 2\ (mod 25)$.

(b) Pembagian $|-37| = 37$ dengan 25 menghasilkan sisa $R = 12$, sehingga $r = 25 - 12 = 13$. Dengan demikian, $-37 = 13\ (mod\ 25)$.

(c) Pembagian $|-25| = 25$ dengan 25 menghasilkan sisa $R = 0$. Dengan demikian, $-25 = 0\ (mod\ 25)$.

Definisi 2.4 (Anton dan Rorres, 2000)

Jika a adalah suatu bilangan pada Z_m, maka suatu bilangan $a^{-1} \in Z_m$ disebut suatu resiprok atau invers perkalian dari a modulo m, jika $aa^{-1} = a^{-1}a = 1(mod\ m)$.

Contoh 2.7

Tentukan resiprok dari 3 mod 26.

Penyelesaian

Bilangan 3 mempunyai sebuah resiprok modulo 26 karena 3 dan 26 tidak mempunyai faktor prima yang sama. Resiprok ini dapat diperoleh dengan menentukan bilangan x pada Z_{26} yang memenuhi persamaan modular

$$3x = 1(mod\ 26).$$

Persamaan tersebut dapat diselesaikan dengan mencoba-coba solusi yang mungkin dari 0 sampai 25, satu persatu. Diperoleh

$$3 \cdot 9 = 27 = 1(mod 26)$$

sehingga

$$3^{-1} = 9(mod 26).$$

2.4.1 Pembagi Persekutuan Terbesar

Definisi 2.5 (Rosen, K.H. 1995)

Pembagi persekutuan terbesar (*gcd*) dari dua bilangan bulat a dan b, dimana a dan b tidak bernilai 0, adalah bilangan bulat terbesar yang membagi a dan b. Notasi untuk pembagi persekutuan terbesar dari a dan b adalah (a, b).

Definisi 2.6 (Rosen, K.H. 1995)

Bilangan bulat a dan b disebut relatif prima jika $(a, b) = 1$.

Contoh 2.9

(1) *gcd* (11,3) = 1; (2) *gcd* (19,4) = 1; (3) *gcd* (29,10) = 1.

Teorema 2.2 (Stinson, D.R. 1995)

Suatu persamaan kongruensi $ax = b\ (mod\ m)$ mempunyai solusi tunggal $x \in Z_m$ untuk setiap $b\ \in Z_m$ jika dan hanya jika $(a, m)\ =\ 1$.

Bukti

($\Rightarrow$) Dengan menggunakan kontraposisinya, jika $(a, m) \neq 1$ (karena dalam hal ini nilai gcd selalu non negatif, maka $(a, m) > 1$) maka persamaan kongruensi $ax = 0\ (mod\ m)$ paling sedikit memiliki dua penyelesaian yang berada di Z_m. Yaitu $x\ =\ 0$ dan $x\ = \frac{m}{a}$. Artinya solusi tidak tunggal.

($\Leftarrow$) Diketahui $(a, m) = 1$. Misalkan terdapat x_1, x_2 sedemikian hingga $ax_1 = ax_2 (mod\ m)$, maka $a(x_1 - x_2) = 0\ (mod\ m)$ artinya $m|\ a(x_1 - x_2)$. Dari sifat teori bilangan, diperoleh $(a, b)\ =\ 1$ dan $a|bc$ maka $a|\ c$. Karena $(a, m) = 1$ dan $m|a(x_1 - x_2)$. Maka $x_1 = x_2\ mod\ m$ (solusi tunggal).

Contoh 2.10

(1) $14 = 47\ (mod\ 73)$ karena $(14,73) = 1$.

(2) $64 = 8\ (mod\ 73)$ karena $(64,73) = 1$.

2.5 Binomial Newton

Tahun 1676 Newton menggeneralisasikan teorema binomial untuk mengekspansi/ menjabarkan bentuk $(x + y)^n$, dimana n suatu bilangan bulat asli. Koefisien binomial merupakan bilangan-bilangan yang muncul dari hasil penjabaran penjumlahan dua peubah yang dipangkatkan, misalnya $(x + y)^n$.

Sepintas terlihat bahwa untuk $(x+y)^n$ tidak ada hubungannya dengan kombinasi, akan tetapi kenyataannya bisa mendapatkan rumus untuk penjabaran$(x+y)^n$ dengan menggunakan rumus banyaknya kombinasi r dari n unsur. Teori untuk menurunkan rumus yang diperoleh dari penjabaran$(x+y)^n$ dengan menggunakan kombinasi dikenal dengan Teorema Binomial.

Definisi 2.7 (Rosen, K.H. 1995)

Misalkan n dan r adalah bilangan bulat taknegatif dengan $r \leq n$. Koefisien binomial $\binom{n}{r}$ didefinisikanm dengan

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!}.$$

Teorema 2.3 (Rumus Pascal) (Budayasa, 2008)

Jika *n* dan *r* bilangan bulat dengan $1 \leq r \leq n-1, maka$

$$\binom{n-1}{r} + \binom{n-1}{r-1} = \binom{n}{r}.$$

Bukti

Bukti dari teorema tersebut adalah dengan menghitung langsung ruas kiri dari formula, setelah disederhanakan akan sama dengan ruas kanan.

$$\binom{n-1}{r} + \binom{n-1}{r-1} = \frac{(n-1)!}{r!\,(n-r-1)!} + \frac{(n-1)!}{(r-1)!\,(n-r)!}$$

$$= \frac{(n-1)!\,(n-r)}{r!\,(n-r)(n-r-1)!} + \frac{(n-1)!\,r}{r(r-1)!\,(n-r)!}$$

$$= \frac{(n-1)!\,(n-r)}{r!\,(n-r)!} + \frac{(n-1)!\,r}{r!\,(n-r)!}$$

$$= \frac{(n-1)!\,(n-r) + (n-1)!\,r}{r!\,(n-r)!}$$

$$= \frac{(n-1)!\,((n-r)+r)}{r!\,(n-r)!}$$

$$= \frac{n(n-1)!}{r!\,(n-r)!}$$

$$= \frac{n!}{r!\,(n-r)!} = \binom{n}{r}.$$

Jadi untuk $\binom{n-1}{r} + \binom{n-1}{r-1} = \binom{n}{r}$ terbukti.

Teorema 2.4 (Teorema Binomial) (Budayasa, 2008)

Jika n suatu bilangan bulat non negatif, maka

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

$$= \sum_{r=0}^{n}\binom{n}{r}x^{n-r}y^r$$

Bukti

Induksi pada n. Untuk $n = 0$, jelas pernyataan tersebut benar. Asumsikan pernyataan benar untuk $n - 1 > 0$. Artinya,

$$(x+y)^{n-1} = \sum_{r=0}^{n-1}\binom{n-1}{r}x^r y^{n-1-r}$$

Selanjutnya, akan ditunjukkan pernyataan benar untuk n. Perhatikan bahwa:

$(x+y)^n = (x+y)(x+y)^{n-1}$

$$= (x+y)\sum_{r=0}^{n-1}\binom{n-1}{r}x^r y^{n-1-r}$$

$$= x\sum_{r=0}^{n-1}\binom{n-1}{r}x^r y^{n-1-r} + y\sum_{r=0}^{n-1}\binom{n-1}{r}x^r y^{n-1-r}$$

$$= \sum_{r=0}^{n-1}\binom{n-1}{r}x^{r+1}y^{n-1-r} + \sum_{r=0}^{n-1}\binom{n-1}{r}x^r y^{n-r}$$

$$= \binom{n-1}{n-1} x^n + \sum_{r=0}^{n-2} \binom{n-1}{r} x^{r+1} y^{n-1-r} + \sum_{r=1}^{n-1} \binom{n-1}{r} x^r y^{n-r} + \binom{n-1}{0} y^n$$

$$= \boldsymbol{x^n} + \sum_{r=0}^{n-2} \binom{n-1}{r} x^{r+1} y^{n-1-r} + \sum_{r=1}^{n-1} \binom{n-1}{r} x^r y^{n-r} + y^n$$

Ganti $r + 1$ dengan r pada suku kedua, diperoleh

$$(x+y)^n = \boldsymbol{x^n} + \sum_{r=1}^{n-1} \binom{n-1}{r-1} x^r y^{n-r} + \sum_{r=1}^{n-1} \binom{n-1}{r} x^r y^{n-r} + y^n$$

$$(x+y)^n = \boldsymbol{x^n} + \sum_{r=1}^{n-1} \left\{ \binom{n-1}{r-1} + \binom{n-1}{r} \right\} x^r y^{n-r} + y^n$$

Berdasarkan Teorema 2.3 Rumus Pascal, diperoleh:

$$(x+y)^n = \boldsymbol{x^n} + \sum_{r=1}^{n-1} \binom{n}{r} x^r y^{n-r} + y^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$$

Sehingga pernyataan benar untuk n. Dengan demikian teorema tersebut terbukti.

2.6 Entropy

Teori informasi merupakan teori matematis dalam komunikasi data yang dikemukakan oleh Shannon pada tahun 1948 (Stinson, 1995). Dalam teori informasi, *entropy* menyatakan derajat ketidakpastian di dalam sistem (Munir, 2012) atau *entropy* dapat dianggap sebagai ukuran matematis suatu ketidakpastian dalam informasi dan dihitung sebagai fungsi dari distribusi probabilitas (Stinson, 1995). Satuan dari nilai penghitungan *entropy* adalah bit (Jolfaei, 2011). Nilai yang *entropy* semakin tinggi, maka tingkat keacakan semakin baik (Ratnasari, 2017) sehingga pesan tidak mudah diprediksi. Sebagai contoh saat orang yang

akan melempar koin sebanyak 50 kali. Dalam pelemparan sebanyak itu tidak dapat dipastikan pada pelemparan keberapa muncul gambar atau angka. Hal ini dikarenakan dalam proses melempar koin tidak bisa ditentukan kapan saatnya muncul sisi gambar atau sisi angka.

Entropy $H(x)$ dari x merupakan suatu nilai yang bergantung pada probabilitas $P(x_1)$ ... $P(x_n)$ dari hasil x yang mungkin terjadi. *Entropy* dapat dihitung menggunakan persamaan (Jiang, 2013)

$$H(x) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i),$$

dengan $H(x)$ menyatakan nilai *entropy* dan $P(x_i)$ menyatakan probabilitas kemunculan karakter ke-x_i (Rinartha, 2010).

Contoh 2.10

Diketahui *ciphertext*: **u) S(2eKDS**

Langkah untuk mencari nilai *entropy* yaitu, hitung probabilitas dari tiap karakter. Berikut merupakan probabilitas dari tiap karakter.

P(**u**) = 0,1 P(**)**) = 0,1 P(*space*) = 0,1 P(**S**) = 0,2 P(**(**) = 0,1

P(**2**) = 0,1 P(**e**) = 0,1 P(**K**) = 0,1 P(**D**) = 0,1

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$$

$$= -[(0{,}1 \log_2 0{,}1) + (0{,}1 \log_2 0{,}1) + (0{,}1 \log_2 0{,}1) + (0{,}2 \log_2 0{,}2) +$$

$$(0{,}1 \log_2 0{,}1) + (0{,}1 \log_2 0{,}1) + (0{,}1 \log_2 0{,}1) + (0{,}1 \log_2 0{,}1) +$$

$$(0{,}1 \log_2 0{,}1)] = 3{,}1219.$$

Kemudian diperoleh nilai *entropy* dari *ciphertext* adalah 3,1219 bit.

BAB V

PENUTUP

5.1 Kesimpulan

1. Berdasarkan hasil analisis dan pembahasan dapat diambil kesimpulan bahwa untuk membangun matriks dengan entri koefisien binomial Newton langkah yang dilakukan sebagai berikut.
   (1) Menentukan ordo matriks yang akan dibangun.
   (2) Menentukan entri baris ke n dan kolom ke r.
   (3) Isi entri baris ke n dan kolom ke r dengan pola $H_r^n = \binom{r+n-1}{r}$.
   (4) Ulangi langkah ke (3) sampai diperoleh matriks sesuai dengan ordo yang telah ditentukan.

   Secara umum untuk membangun matriks dengan entri koefisien binomial Newton dapat diperoleh dari, jika A adalah matriks persegi ordo k x k yang entri baris ke-n kolom ke-r adalah H_r^n dengan $n, r \in \{1,2,3 \dots, k\}$, maka $det\ (A) = 1$.
2. Matriks yang dibangun dari koefisien binomial digunakan pada proses enkripsi dan dekripsi sebagai kunci pengaman.
3. Tingkat keacakan dilihat dari nilai *entropy* untuk matriks kunci dengan ukuran yang sama. Nilai *entropy* suatu *ciphertext* semakin tinggi artinya tingkat keacakan semakin baik. (a) Untuk tingkat keacakan dari karakter yang berbeda berdasarkan hasil analisis diperoleh semakin panjang *plaintext* dengan karakter berbeda rata-rata nilai *entropy*

semakin naik; (b) Untuk tingkat keacakan pada *plaintext* yang sama berdasarkan hasil analisis diperoleh rata-rata nilai *entropy* yang tidak cenderung turun ataupun cenderung naik; (c) Untuk tingkat keacakan *plaintext* pada bentuk kalimat dengan imbuhan kata berdasarkan analisis yang telah dilakukan diperoleh informasi bahwa semakin panjang *plaintext*, nilai *entropy* yang diperoleh semakin naik.

5.2 Saran

Berdasarkan hasil penelitian maka saran yang dapat disampaikan adalah sebagai berikut.

1. Matriks kunci yang dibangun dari koefisien binomial Newton dapat dikembangkan dengan mengubah susunannya. Teknik mengubah susunan entri-entrinya dapat memanfaatkan sifat pada operasi baris elementer, sehingga kunci yang diperoleh lebih bervariatif.
2. Mengetahui tingakat keacakan selain dengan perhitungan *entropy*, disarankan untuk penelitian berikutnya menggunakan perhitungan *redundancy* kemudian membandingkannya.

DAFTAR PUSTAKA

Anton, Howard. 1995. *Aljabar Linear Elementer* 5^{th}. Jakarta: Erlangga.

Anton, H. & C. Rorres. 2000. *Elementery Algebra Linear Application Version* 8^{th}. USA: John Wiley & Sons, inc.

Bain, L.J. 1992. *Introduction to Probability and Mathematics Statistics* 2^{nd}. United States of America: Arcata Graphics.

Basri. 2016. Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*. 2(2): 17-23.

Buchmann, J. A. 2000. *Introduction to Cryptography*. New York: Springer-Verlag.

Budayasa, I. K. 2008. *Matematika Diskrit*. Surabaya: Unesa Press.

Chuan, C. & Meng, K. 1992. *Principles and Techniques in Combinatorics*. Singapore: World Scientific.

Farmanbar, M. &Alexander G. C. 2012. Investigation of Hill Cipher Modification Based on Permutation and Iteration. *International Journal of Computer Science and Information Security (IJCSIS)*. 9(10): 1–7.

Forouzan, Behrouz. 2006. *Cryptography and Network Security*. New York: McGraw-Hill.

Hasan, M.I. 2013. *Pokok-Pokok Materi Statistik 1 (Statistik Deskriptif)*. Jakarta: Bumi Aksara.

Hidayat, A. & Alawiyah, T. 2013. Enkripsi dan Dekripsi Teks Menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika Integratif*. 1(9): 39-51.

Ibrahim & Mussafi, N. S. M. 2013. *Pengantar Kombinatorika dan Teori Graf*. Yogyakarta: Graha Ilmu.

Jiang, S. 2013. On Unconditional Security of Private Key Encryption. *The British Computer Society*. 10(57): 1571-1579.

Jolfaei, A. 2011. Image Encryption Using Chaos and Block Cipher. *Canadian Center of Science and Education*. 1(4): 172-185.

Kromodimoeljo, S. 2010. *Teori dan Aplikasi Kriptografi*. -: SPK IT Conculting.

Menezes, A. J., P. C. van Orschot, & S. A. Vanstone. 1997. *Handbook of Applied Cryptography*. USA: CRC Press, Inc.

Munir, Rinaldi. 2012. *Matematika Diskrit*. Bandung: Informatika.

Nazir, M. 2003. *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Pasaribu, J. S. 2016. Penerapan Algoritma Hill Chiper dalam Pengamanan Data dengan Teknik Enkripsi dan Dekripsi. *Seminar Nasional Telekomunikasi dan Informatika*. Bandung: Politeknik Piksi Ganesha.

Quasim, T. MD. 2013. Security Issues in Distributed Database System Model. *An International Journal of Advanced Computer Technology (Compusoft)*. 2(12): 396-399.

Rathi, D. & P. Astya. 2014. Extended Hill Cipher Decryption by Using Transposed Interweaved Shifting. *International Journal of Computer Science and Information Technologies* (*IJCIT*). 5(2): 1147-1151.\

Ratnasari, D. & Sejati, H. P. 2017. Enkripsi Citra Digital Menggunakan Kombinasi Algoritme Hill Cipher dan Chaos Map dengan Penerapan Teknik Selektif pada Bit MSB. *Jurnal Teknologi Technoscientia*. 1(10): 110-117.

Ravan, R. R & A. R. Nigavekar. 2013. Secured Data Communication using Novel Modification to Hill Cipher Algorithm with Self Repetitive Matrix. *International Journal of Science and Research* (*IJSR*). 2(4): 392-395.

Rinartha, K. 2010. Pengaman Citra Digital dengan Menggunakan Pengembangan Kriptografi Kunci Publik Elgamal. *Proseding Seminar Nasional*

Teknologi Informasi dan Aplikasinya. Vol.2 . Malang: Politeknik Negeri Malang.

Rohmanu, A. 2017. Implementasi Kriptografi dan Steganografi dengan Metode Algoritma Des dan Metode End Of File. *Jurnal Informatika SIMANTIK*. 2(1): 1-11.

Rosen, K.H. 1986. *Elementary Number Theory and Its Applications*. United States of America: Addison-Wesle.

Stinson, D. R. 2006. *Criptography Theory and Practice* 3^{th}. United Statis of America: Chapman & Hall/CRC.

Suryadilaga, M. K. S. 2007. *The Balance Ways*. Jakarta: PT Mizan Publika.

Thangarasu, N. & SelvaKumar, A. L. 2015. Encryption Using Lester Hill Cipher Algorithm. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*. 12(2): 13-17.