 ISSN: XXXX-XXXX

Analisis Perbandingan *Known Plaintext* dan *Chosen Plaintext* Pada Metode Hill Chiper

Abdul Rauf Tuasikal

Universitas Muslim Indonesia, Jalan Urip Sumoharjo, Makassar, 90231, Makassar
arnifattah@gmail.com

INFORMASI ARTIKEL

Diterima : xx – xx – 20xx
Direvisi : xx – xx – 20xx
Diterbitkan : xx – xx – 20xx

Kata Kunci:
Hill Cipher
Kriptanalisis
Known Plaintext
Chosen Plaintext

ABSTRAK

Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher karena teks yang akan diproses akan 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 merupakan salah satu algoritma kriptografi kunci simetris. Algoritma Hill Cipher menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Tujuan penelitian ini adalah untuk melakukan proses kriptanalisis atau membongkar suatu cipherteks tanpa mengetahui kunci pada metode hill cipher. Hasil pengujian yang dilakukan kriptanalisis pada algoritma hill cipher dengan melakukan known plaintext dan chosen plaintext untuk mencari kunci. Hasil penelitian memperlihatkan bahwa dari dua perbandingan tersebut cukup baik dalam mencari kunci, dan tingkat akurasi dalam mencari kunci tergantung menggunakan ordo yang gunakan.

I. Pendahuluan

Proses yang paling sering dilakukan oleh para pengguna computer dalam menggunakan komputer adalah melakukan pertukaran informasi atau data. Seringkali data atau informasi yang dapat dipertukarkan adalah data penting yang tidak boleh diketahui oleh orang lain. Berdasarkan fakta tersebut, maka dikembangkan suatu bidang ilmu yang berisi metode atau cara untuk melindungi data yang akan dipertukarkan dari akses – akses illegal. Kriptologi merupakan ilmu yang menekuni dua bidang yaitu kriptografi dan kriptanalisis. Kriptografi merupakan seni untuk mengacak sebuah pesan dengan teorema tertentu sehingga pesan tidak bisa dimengerti maknanya atau disebut dengan cipherteks. Kriptanalisis merupakan seni untuk memecahkan cipherteks tanpa mengetahui kunci yang digunakan(Nurkifli et al. 2013). Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher karena teks yang akan diproses akan 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 (Hasugian 2017).

Dalam implementasiannya ada saja kesalahan atau kecerobohan pada saat melakukan enkripsi, seperti kunci matriks yang digunakan pada proses enkripsi hilang karena tidak disimpan atau bahkan lupa. Oleh sebab itu diperlukan teknik kriptanalisis untuk mendapatkan kembali kunci yang hilang tersebut. Salah satu teknik kriptanalisis untuk pencarian variabel matriks kunci pada kriptografi Hill Cipher yang telah diketahui, yaitu dengan menggunakan perkalian matriks. pada perkalian matriks, proses pencarian variabel matriks kunci hanya dapat dilakukan jika matriks yang merepresentasikan plaintext memiliki invers. Jika matriks yang merepresentasikan plaintext tidak memiliki invers maka pencarian kunci tidak dapat dilakukan. Hal tersebut disebabkan karena nilai determinan pada matriks yang merepresentasikan plaintext tidak sama dengan satu(Azhar, dkk, 2017). Dalam ilmu kriptanalisis terdapat beberapa enkripsi diantaranya ciphertext only, known-plaintext, chosen-plaintext, adaptive-chosen-plaintext, chosen-ciphertext, dalam penelitian ini penulis akan menggunakan dua algoritma enkripsi yaitu chosen-plaintext dan known-plaintext. Sehingga dengan alasan tersebut penulis berharap bahwa dengan menggunakan metode dari hasil penelitian ini maka ukuran data akan lebih kecil, begitu juga keamanan data dari hasil enkripsi data bisa lebih terjamin Tujuan penelitian adalah melakukan kriptanalisis tanpa mengetahui kunci pada metode hill cipher dengan batasan masalah penggunaan panjang kunci maksiman 20 karakter dan karakter plaintext merupakan data teks *lowercase.* Manfaat dari penelitian ini dapat diuraikan sebagai berikut yaitu menambah pengetahuan dan wawasan dalam hal menganalisis metode hill cipher dalam masalah pengamanan data teks, menawarkan penyelesaian yang lebih mudah dalam pengamanan data teks menggunakan metode hill cipher dengan pilihan matriks yang lebih aman,

dan dapat memberikan suatu referensi yang berguna bagi dunia akademik khususnya dalam penelitian-penelitian yang akan dilaksanakan oleh para peneliti yang akan datang dalam hal pengamanan data teks atau berkaitan dengan metode yang penulis gunakan.

II. Metodologi Penelitian

A. Kriptografi

Menurut(Rio et al. 2016) Ilmu kriptografi berawal dari kriptologi yang kemudian ilmunya terbagi menjadi dua yaitu kriptografi dan kriptanalisis. Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Sedangkan kriptanalisis sendiri merupakan sebuah usaha mendapatkan teks terang dari suatu teks sandi yang tidak diketahui sistem serta kunci-kunci-nya. Kriptografi bertujuan untuk memberi layanan keamananofana (2010). (Sulistyo 2009), kriptografi mempunyai beberapa layanan keamanan antara lain, Confidentiality (kerahasaian), yaitu aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang mempunyai kewenangan atau kunci rahasia untuk membuka informasi, data Integritas (keutuhan data), adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah, dan *authentication* (otentikasi), yaitu aspek yang berhubungan dengan identifikasi atau pengenalan baik secara kesatuan sistem maupun informasi itu sendiri.Pihak yang saling berkomunikasi harus saling memperkenalkan diri Jaringan komputer (*computer network*) merupakan himpunan interkoneksi sejumlah komputer autonomous. Dalam bahasa populernya dapat dijelaskan bahwa jaringan komputer merupakan kumpulan beberapa komputer yang saling terhubung dengan lain melalui media perantara seperti media kabel ataupun media tanpa kabel (nirkabel). Berdasarkan skala atau area, jaringan komputer dapat dibagi menjadi 4 bagian yaitu

B. Kriptanalisis

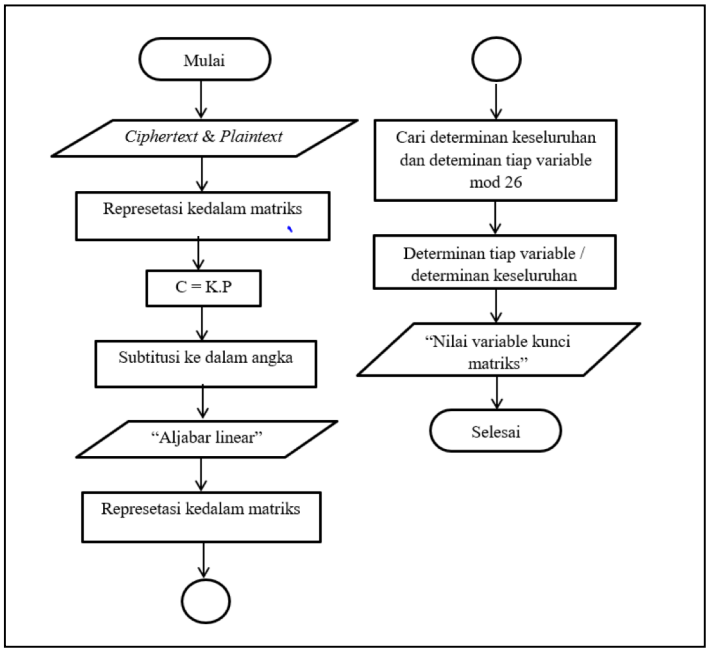
Kriptanalisis adalah sebuah studi mengenai cipher, ciphertext atau cyrptosystems yang bertujuan menemukan kelemahan dalam sistem penyandian, sehingga dimungkinkan untuk memperoleh plaintext dari ciphertext yang ada, tanpa perlu mengetahui kunci ataupun algoritma pembangun ciphertext tersebut. Cara ini disebut dengan memecahkan cipher, ciphertext atau cryptosystem. Dalam memecahkan cipher, dilakukan pencarian kesalahan dalam desain atau implementasi dari cipher itu sendiri sehingga dapat mengurangi jumlah kunci yang harus dicoba ketika melakukan brute force attack (mencoba memecahkan cipher dengan menggunakan semua kunci yang mungkin sampai akhirnya ditemukan satu kunci yang benar). Contohnya, jika kunci yang digunakan untuk mengenkripsi sepanjang 2128, maka brute force attack akan mencoba semua kunci yang mungkin , yaitu sebanyak 2128 (atau rata-rata 2127) kali untuk menemukan kunci yang tepat. Iterasi sebesar itu masih belum dapat dilakukan secara cepat oleh sistem komputasi saat ini. Dengan adanya studi kriptanalisis, telah ditemukan cara pengekstraksian plaintext hanya dalam 240 kali iterasi. Walaupun belum sepenuhnya terpecahkan, namun plaintext telah dapat diekstrak dari cipher dengan menggunakan sumberdaya komputasi yang relatif jauh lebih kecil.

Sebuah algoritma kriptografi dikatakan aman (computationally secure) bila ia memenuhi tiga kriteria berikut: persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik, biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut, waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya (2013).

C. Known-Plaintext Analysis

Dengan prosedur ini, kriptanalis mengetahui sebagian isi plaintext dari ciphertext yang berhasil didapatkan. Menggunakan informasi yang ada ini, kriptanalis berusaha untuk mencari kunci yang digunakan untuk menghasilkan ciphertext. Pesan-pesan yang memiliki format terstruktur memberikan peluang kepada kriptanalis untuk menebak plaintext dari ciphertext yang bersesuaian. Contoh dari pesan-pesan terstruktur ini adalah email dengan kolom from, to, subject, kemudian salam penutup dan pembuka pada surat seperti ”dengan hormat”, salam, dan lainnya. Dimiliki 9): C1=Ek(P1) dan P1, C2=Ek(P2) dan P2 ..., Ci=Ek(Pi) dan Pi, Deduksi : kunci. Linear Cryptanalysis adalah salah satu algoritma yang termasuk ke dalam serangan known-plaintext. Linear Cryptanalysis diperkenalkan oleh Mitsuru Matsui pada tahun 1993. Pada algoritma ini penyerang akan mempelajari fungsi linear yang merepresentasikan hubungan antara ciphertext dan plaintext untuk mendapatkan kunci. Untuk algoritma yang menggunakan fungsi XOR, suatu fungsi linier sederhana dapat dibentuk dan dipecahkan dengan probabilitas sebesar 1 (pasti dipecahkan). Sedangkan untuk fungsi yang lebih kompleks seperti S-Box, akan dicari suatu fungsi linear, yang memiliki probabilitas sebesar p, dengan memaksimalkan |p-½|. Untuk seluruh teks cipher akan didapatkan fungsi, fungsi ini didapatkan melalui

konkatenasi satu siklus fungsi linier. Suatu fungsi linier dikatakan cukup tepat apabila memiliki p≠½. Sebagai contoh, fungsi linear untuk mendekati kunci yang dibangun menggunakan algoritma DES memiliki probabilitas sebesar ½+2-24. Algoritma berbasis XOR, termasuk ke dalam algortima enkripsi/dekripsi yang tidak aman karena dapat dipecahkan menggunakan linear cryptanalysis.



Gambar 1. Flowchart

D. Chosen-Plaintext Analysis

Kriptanalis telah dapat menghasilkan plaintext dari ciphertext yang ada, namun kuncinya sendiri belum ditemukan. Pada serangan jenis ini kriptanalis dapat memilih plaintext tertentu untuk dienkripsikan, yaitu plaintext yang lebih mengarahkan penemuan kunci. Kriptanalis berusaha untuk menemukan kunci pembangun ciphertext dengan membandingkan keseluruhan ciphertext dengan plaintext yang ada. Teknik enkripsi RSA (Rivest-Shanir-Adleman) telah terbukti dapat dipecahkan menggunakan teknik analisis ini. Dimiliki 9): C1=Ek(P1) dan P1 C2=Ek(P2) dan P2 .... Ci=Ek(Pi) dan Pi Deduksi : kunci. Differential Analysis adalah sebuah teknik yang dikembangkan oleh Eli Biham dan Adi Shamir. Teknik ini memberikan suatu cara untuk menemukan beberapa bit kunci dari plaintext dan ciphertext yang tersedia, dengan begitu jumlah kemungkinan kunci yang akan dicoba pada exhaustive key search atau brute force attack dapat berkurang drastis, mengurangi waktu kalkulasi. Differential Analysis secara garis besar membahas pola lengkap dari bit-bit mana saja yang berubah dan tidak berubah pada proses pengubahan input menjadi output. Prinsip dasar dari Differential Analysis adalah 2): Suatu ciphertext memiliki karakteristik dimana terdapat suatu konstanta X sehingga untuk banyak pasangan plaintext A dan B dimana B=(A xor X), jika sebuah pernyataan bernilai benar tehadap kunci, E(B,k) = (E(A,k) xor Y) untuk beberapa konstanta Y akan benar dengan probabilitas diatasnya (kemungkinan acak).

E. Hill Cipher

(Widyanarko, n.d. 2007), Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris. Algoritma Hill Cipher menggunakan matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Kunci pada hill cipher adalah matriks n x n dengan n merupakan ukuran blok. Jika matriks kunci kita sebut dengan K, maka matriks K. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki multiplicative inverse K-1. Kunci harus memiliki invers karena matriks K-1 tersebut adalah kunci yang digunakan untuk melakukan dekripsi. Proses enkripsi pada hill cipher dilakukan per blok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum membagi teks menjadi deretan blok-blok, plainteks terlebih dahulu dikonversi menjadi angka, secara sistematis, proses enkripsi pada hill cipher. Proses dekripsi pada hill cipher pada dasarnya sama dengan proses enkripsinya, Namun matriks kunci harus dibalik (invers) terlebih dahulu, secara sistematis.

F. Cryptool

Cryptool adalah perangkat lunak e-learning yang menggambarkan konsep kriptografi dan kriptanalitik. Cryptool digunakan untuk tools/alat sebagai generator hill cipher dalam melakukan enkripsi dan dekripsi.

III. Hasil dan Pembahasan

1) Enkripsi dan Dekripsi dengan metode Hill Cipher

a) Langkah 1. Plainteks dikonversi menjadi angka

b) Langkah 2. Merubah plainteks menjadi matriks yang sesuai dengan ordo Key. Matriks kunci K berukuran ordo 3x3, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 3 karakter.

c) *Langkah 3. Enkripsi* antara matriks plainteks dengan matriks key.

IV. Kesimpulan

Dari hasil penelitian yang telah dilakukan, kesimpulan yang bias ditarik adalah : hasil analisis perbandingan membuktikan bahwa dari kedua metode untuk melakukan pencarian key, dari beberapa karakter yang telah teruji pada known plaintext teruji kurang baik karena hasil key pada ordo 3x3 sulit untuk di temukan sedangkan bila ordo 2x2 hasilnya cukup baik namun hasil key tidak sepenuhnya di dapatkan, kemudian hasil dari chosen plaintext lebih baik dari metode pertama karena hasil key yang didapatkan teruji cukup baik karena yang di dapatkan dari ordo 2x2 dan ordo 3x3 dapat menemukan key namun tidak sepenuhnya, jika ingin melakukan penelitian lebih lanjut dengan melakukan dan dikembangkan menjadi chaining hill cipher untuk membuat proses kriptanalis menjadi lebih sulit.

Daftar Pustaka

[1] Azhar, Wafiqah Yasmin, Supriyadi Supriyadi, and Yessy Yanitasari. 2017. "Kriptanalisis Hill Cipher Terhadap Known Plaintext Attack Menggunakan Metode Determinan Matriks Berbasis Android." Simetris : Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer 8(2):579.

[2] Gupta, I., Singh, J., & Chaudhary, R. (2007). Cryptanalysis of an extension of the HillCipher.Cryptologia,31(3),246–253.

[3] Hasugian, Abdul Halim. 2017. "Implementasi Algoritma Hill Cipher." (August 2013):115–22.

[4] Hidayat, A., & Alawiyah, T. (2013). Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. Jurnal MatematikaIntegratif, 9(1), 39. https://doi.org/10.24198/jmi.v9.n1.10196.39-52.

[5] Levine, J., & Chandler, R. (1989). The hill cryptographic system with unknown cipher alphabet but known plaintext. Cryptologia, 13(1), 1–28. https://doi.org/10.1080/0161-118991863736.

[6] Li, C. Q., Zhang, D., & Chen, G. R. (2008). Cryptanalysis of an image encryption scheme based on the Hill cipher. Journal of Zhejiang University: Science A, 9(8), 1118–1123. https://doi.org/10.1631/jzus.A0720102.

[7] Nurkifli, E. Haodudin, Deden Wahidin, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang, Stastical Attack, and Tinjauan Pustaka. 2013. "Analisis Cryptanalys Exhaustive Search Dan Statistical Attack Pada Algoritma Playfair Cipher." (2012):6–9.

[8] Putera, A., & Siahaan, U. (2016). Algoritma Genetika Untuk Pembentukan Kunci Matriks 3 X 3 Pada Kriptografi Hill Cipher. Jurnal UMJ 2016, 1(November), 1–6.

[9] Valens. (2005). Membuat Jaringan. http://mikrotik.co.id/artikel_lihat.php?id=5, diakses pada tanggal 21 November 2019.

[10] Rio, Hernata, Cahyo Bawono, Program Studi, Teknik Informatika, Jurusan Teknik Informatika, Fakultas Sains, D. A. N. Teknologi, and Universitas Sanata Dharma. 2016. "Kriptanalisis Pada Algoritma Cipher Algorithm."

[11] Sulistyo, Budi. 2009. "Kriptanalisis Cipher Blok Berdasarkan Permainan Kaotik." 33204013.