PERANAN MATRIK DALAM KRYPTOGRAFI

Slamet Boediono
STKIP PGRI JOMBANG
slamet.boediono@gmail.com

Abstract

Cryptography is a mathematical technique related to aspects of information security such as level of confidence, data integrity, entity authentication and data authenticity authentication. In principle, cryptography is the process of hiding information so that it cannot be read by anyone who is not interested so that data security is maintained. Security requires technique and art as well as data security. The security reliability of data depends on each individual's way of understanding the importance of the data. Various security fields in the world of communications cannot be separated from this. There are two processes in cryptography, namely encryption and description. One of the encryption and description processes can utilize operations on matrices. The aim of this research is the role of matrices in the encryption and decryption process of a text or sentence. The research results show that the cryptographic process of a sentence can use a square matrix and its operations. The greater the order of metrics used, the higher the level of security of the data. In this research, a square matrix of order 2x2 is used as the encryption and description key. Meanwhile, to speed up the encryption and description process, you can use the help of a programming language, one of which is the C programming language.

Keywords *: cryptography, data, matric*

Abstrak

Kriptografi merupakan teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data, autentikasi entitas dan autentikasi keaslian data. Pada prinsipnya kriptografi merupakan proses menyembunyikan suatu informasi agar tidak bisa dibaca oleh seseorang yang tidak berkepentingan sehingga keamanan data tetap terjaga. Keamanan membutuhkan membutuhkan teknik dan seni demikian pula dengan keamanan suatu data. Kehandalan keamanan suatu data tergantung dari cara masing-masing dalam memahami pentingnya data. Berbagai bidang keamanan dalam dunia komunikasi tidak terlepas dari hal tersebut. Pada proses kriptografi ada dua yaitu enkripsi dan deskripsi. Proses enkripsi dan deskripsi, salah satunya dapat memanfaatkan operasi pada matrik. Tujuan dari penelian ini adalah bagaimana peranan matrik dalam proses enkripsi dan dekripsi suatu teks atau suatu kalimat. Hasil penelitian menunjukkan bahwa proses kriptografi suatu kalimat, dapat menggunakan matrik bujursangkar berserta operasinya. Semakin besar ordo mtrik yang digunakan maka semakin tinggi tingkat keamanan suatu data. Pada penelitian ini digunakan matrik bujursangkar dengan ordo 2x2 sebagai kunci enkripsi dan deskripsi. Sedangkan untuk mempercepat proses enkripsi maupun deskripsi maka dapat menggunakan bantuan bahasa pemrograman salah satunya bahasa pemrograan C

Kata kunci *: kriptografi, data, matrik*

PENDAHULUAN

Perkembangan teknologi informasi semakin memudahkan masyarakat dalam berbagai bidang memberikan dampak pada segala aspek kehidupan manusia. Salah satu hal yang berkembang pesat dan menjadi pemicu dari

perkembangan yang ada adalah komunikasi. Komuniksi merupakan hal yang penting dalam kehidupan sehari-hari untuk interaksi manusia satu sama lain. Tidak bisa dipungkiri, terjadi banyak permasalahan yang muncul pada kkomunikasi khususnya keamanan informasi. Bagaimana cara memberikan dan memperoleh informasi dengan aman maka kerahasiaan merupakan elemen penting bagi keamanan suatu komunikasi. Salah satu teknik keamanan penyampaian maupun penerimaan data yang aman adalah melalui teknik kriptografi.

Kriptografi atau cryptography berasal dari bahasa Yunani, kripto dan graphia. Kripto memiliki arti menyembunyikan, sementar graphia berarti tulisan. Sehingga bisa dijabarkan kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi. misalnya keabsahan data, kerahasiaan data, kredibilitas data, integritas data, dan autentikasi data. Akan tetapi, tidak semua aspek keamanan informasi bisa diatasi dengan kriptografi. Kriptografi merupakan seni dan ilmu dalam menciptakan sebuah sistem crypto yang mampu menyediakan keamanan informasi. Kriptografi berkaitan erat dengan pengamanan data digital ilmu ini terdiri dari mekanisme-mekanisme perancangan yang didasarkan pada algoritma algoritma matematika yang menawarkan sejumlah layanan keamanan informasi fundamental. Kebalikan dari kriptografi adalah grip analisis yang merupakan seni dan ilmu dalam membongkar teks ciper nalisis seringkali dipakai untuk mempelajari kekuatan keamanan dari rancangan atas sebuah teknik kriptografi yang baru. (Siahaan,2019:1).

Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandian disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana teknik melindungi data dan informasi tersebut beserta seluruh ikutannya. Penerapan kriptografi membutuhkan operator crypto seperti penyampaian berita rahasia dari satu tempat ke tempat lain, penyimpanan data dan informasi rahasia ke dalam database atau pengoperasian mesin-mesin khusus crypto. Pemakaian bilangan sebagai pengganti abjad kerap dijumpai dalam kriptografi. Salah satu cara penggunaannya adalah dalam bentuk sebuah matriks. Hal ini disebabkan karena matriks memiliki operasi perkalian yang melibatkan beberapa elemen sekaligus sehingga penyidikan terhadap kunci sandinya juga berbentuk matrik

METODE PENELITIAN

Penelitian ini bersifat deskriptif analitis, yakni diawali dengan menggambarkan situasi yang ada yaitu penggunaan teknik kriptografi dalam pengamanan dalam suatu informasi. Selanjutnya berdasarkan data-data ini akan dilakukan analisis dan kemudian menghubungkan dengan teori-teori yang relevan. Metode yang digunakan dalam penelitian ini adalah experiment reasearc. Penelitian dimulai dengan studi kepustakaan yaitu pengumpulan bahan-bahan referensi baik dari buku, jurnal mengenai kriptografi, matrik dan konsep matematis yang mendasari dalam pengenkripsian suatu data dengan menggunakan matrik. Selanjutnya pada tahapan analisis masalah dilakukan terhadap kriptografi. Operasi matrik yaitu perkalian matrik kunci dengan suatu data yang akan disandikan (proses penyandian) dan pencarian invers matrik untuk proses

mendapatkan data yang original. Tahap selanjutnya adalah perancangan sistem dengan tujuan dapat menjamin keamanan data, perancangan struktur program dan perancangan procedural sistem. Data yang digunakan dalam penelitian ini adalah karakter A-Z beserta spasi. Tahap pengkodean digunakan untuk mengimplementasikan system yang telah dirancang kedalam bahasa pemrogaman agar proses lebih cepat dan akurat. Tahap akhir adalah pengujian system dengan tujuan apakah system yang telah dirancang dapat berjalan sesuai dengan yang diharapkan.

HASIL DAN PEMBAHASAN

Proses kriptografi pada penelitian ini akan digunakan data berupa karakter huruf A-Z beserta karakter spasi. Kumpulan dari karaktr tersebut dapat membentuk suatu kalimat yang mana kalimat tersebut akan kita lakukan proses kriptografi. Proses ini ada terdiri dari dua tahap yaitu Enkripsi (pengkodean atau penyandian) dan Deskripsi (proses penguraian penyandian).

Pada Proses enkripsi perlu dibuat aturan sesuai yang dikehendaki. Pada penelitian ini dibuat aturan sebagai berikut :

1. karater A-Z akan direlasikan kedalam angka 1-26 sedangankan spasi direlasikan dalam angka 0.

A	B	C	……	spasi
↕	↕	↕	……	↕
1	2	3		0

2. Tentukan matrik ordo 2x2 dengan syarat matrik tersebut mempunyai invers, matrik ini akan sebagai kunci penyandian.
3. Melakukan relasi data/kalimat perkarakter dengan angka yang berkesesuaian dan simpan hasilnya kedalam matrik M yang berordo 2 x n.
4. Lakukan perkalian matrik A. M simpan hasilnya dalam matrik P. Selanjutnya rubah matrik P kedalam modulus 27.
5. Setiap elemen matrik P yang sudah dalam modulus 27 direlasikan kedalam huruf-huruf yang telah ditentukan sehingga didapat susunan karakter hasil enkripsi.

Pada Proses Deskripsi :

Pada proses ini merupakan proses pembalikan yaitu proses pengubahan data yang sudah dienkripsi menjadi data original atau data asli. Pada proses ini dibutuhkan langkah-langkah sebagai berikut :

1. Cari invers matrik dari matrik kunci yang telah ditetapkan.
2. Tentukan data atau kalimat hasil enkripsi yang telah diterima.
3. Konversikan data yang diterima kedalam angka-angka sesuai aturan yang telah ditetapkan dan susun sebagai bentuk matrik P yang berukuran 2 x n.
4. Hitung hasil perkalian matrik invers dengan matrik P yaitu M= A^(-1).P
5. Ubah matrik M kedalam modulus 27
6. Konversikan hasil modulus dengan huruf-huruf yang bersesuaian sehingga didapat suatu data asli atau kalimat awal.

HASIL PENELITIAN

Pada penelitian ini akan diakukan kriptografi pada data atau kalimat sebagai berikut :

KESUKSESAN BERMULA DARI KEGAGALAN

Berdasarkan kalimat tersebut, bisa dikonversi menjadi deretan angka-angka berikut :

11 5 19 21 11 19 1 14 0 2 5 18 13 21 12 1 0 4 1 18 9 0 11 5 7 1 7 1 12 1 14 0

Deretan angka-angka tersebut disusun dalam bentuk matrik :

$$M = \begin{bmatrix} 11 & 19 & 11 & 5 & 1 & 0 & 5 & 13 & 12 & 0 & 1 & 9 & 11 & 7 & 7 & 12 & 14 \\ 5 & 21 & 19 & 19 & 14 & 2 & 18 & 21 & 1 & 4 & 18 & 0 & 5 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Selanjutnya ditentukan matrik kunci ordo 2x2 yang mempunyai invers sebagai matrik kunci

$$A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$$

Cari matrik P dengan mengalikan matrik A dengan matrik M

$$P = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 11 & 19 & 11 & 5 & 1 & 0 & 5 & 13 & 12 & 0 & 1 & 9 & 11 & 7 & 7 & 12 & 14 \\ 5 & 21 & 19 & 19 & 14 & 2 & 18 & 21 & 1 & 4 & 18 & 0 & 5 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$P = \begin{bmatrix} 47 & 143 & 117 & 105 & 72 & 10 & 100 & 131 & 29 & 20 & 92 & 18 & 47 & 19 & 19 & 2 & 1 \\ 26 & 82 & 68 & 62 & 43 & 6 & 59 & 76 & 15 & 12 & 55 & 9 & 26 & 10 & 10 & 15 & 4 \end{bmatrix}$$

Mengubah bentuk matrik P menjadi matrik modulus 27

$$P = \begin{bmatrix} 20 & 8 & 9 & 24 & 18 & 10 & 19 & 23 & 2 & 20 & 11 & 18 & 20 & 19 & 19 & 2 & 1 \\ 26 & 1 & 14 & 8 & 16 & 6 & 5 & 22 & 15 & 12 & 1 & 9 & 26 & 10 & 10 & 15 & 14 \end{bmatrix}$$

Dengan mengkonversikan matrik P kedalam huruf yang bersesuaian akan didapat :

$$P = \begin{bmatrix} T & H & I & X & R & J & S & W & B & T & K & R & T & S & S & B & A \\ Z & A & N & H & P & F & E & V & O & L & A & I & Z & J & J & O & N \end{bmatrix}$$

Sehingga didapat data atau kalimat yang dienkripsi sebagai berikut :
TZHAINXHRPJFSEWVBOTLKARITZSJSJBOAN

Untuk mengubah data atau kalimat yang sudah terenkeripsi maka diperlukan tahapan-tahapan sebagai berikut :

1. Carilah invers matrik kunci yang telah ditetapkan
   $A = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$ invers dari matrik adalah $A^{-1} = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$
2. Konversikan data atau kalimat yang tenkripsi
   TZHAINXHRPJFSEWVBOTLKARITZSJSJBOAN
   dengan angka sesuai aturan konversi dan susun kedalam matrik P sebagai berikut :
   $$P = \begin{bmatrix} 20 & 8 & 9 & 24 & 18 & 10 & 19 & 23 & 2 & 20 & 11 & 18 & 20 & 19 & 19 & 2 & 1 \\ 26 & 1 & 14 & 8 & 16 & 6 & 5 & 22 & 15 & 12 & 1 & 9 & 26 & 10 & 10 & 15 & 14 \end{bmatrix}$$
3. Kalikan matrik A^{-1} dengan matrik P
   $$M = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}.$$
   $$\begin{bmatrix} 20 & 8 & 9 & 24 & 18 & 10 & 19 & 23 & 2 & 20 & 11 & 18 & 20 & 19 & 19 & 2 & 1 \\ 26 & 1 & 14 & 8 & 16 & 6 & 5 & 22 & 15 & 12 & 1 & 9 & 26 & 10 & 10 & 15 & 14 \end{bmatrix}$$

$$M = \begin{bmatrix} -70 & 19 & -43 & 32 & -26 & 0 & 32 & -41 & -69 & 0 & 28 & 9 & -70 & 7 & 7 & -69 & -67 \\ 32 & -6 & 19 & -8 & 14 & 2 & -9 & 21 & 28 & 4 & -9 & 0 & 32 & 1 & 1 & 28 & 27 \end{bmatrix}$$

4. Mengubah matrik M menjdi matrik modulu 27

$$M = \begin{bmatrix} 11 & 19 & 11 & 5 & 1 & 0 & 5 & 13 & 12 & 0 & 1 & 9 & 11 & 7 & 7 & 12 & 14 \\ 5 & 21 & 19 & 19 & 14 & 2 & 18 & 21 & 1 & 4 & 18 & 0 & 5 & 1 & 1 & 1 & 1 \end{bmatrix}$$

5. Mengkonversi matrik M dengan huruf yang bersesuaian, akan didapat KESUKSESAN BERMULA DARI KEGAGALAN

SIMPULAN DAN SARAN

SIMPULAN

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa kriptografi dapat dibuat dengan memanfaatkan matrik bujur sangkar ordo 2x2 atau lebih dengan syarat matrik tersebut mempunyai invers. Matrik yang ditentukan sebagai kunci pengkodean berperan sebagai pengubah data atau kalimat dengan cara perkalian matrik. Sedangkan invers matrik dari matrik kunci digunakan untuk proses mendapatkan data atau kaliat asli. Pada kriptografi terjadi dua proses yaitu enkripsi dan deskripsi. Pada enkripsi data atau kalimat terjadi suatu proses penyandian atau pengkoden dari data asli sehingga data atau kalimat tidak akan bermakna. Sedangkan pada proses deskripsi merupakan proses untuk merubah data atau kalimat yang tak bermakna menjadi data atau kalimat yang bermakna.
Simpulan dapat bersifat generalisasi temuan sesuai permasalahan penelitian, dapat pula berupa rekomendatif untuk langkah selanjutnya

SARAN

Berdasarkan hasil penelitian maka peneliti memberikan saran sebagai berikut :

1. Hasil penelitian ini dapat dikembangkan dengan menggunakan matrik kunci dengan ordo lebih dari 2x2 sehingga akan didapatkan penyandian yang mempunyai tingkat keamanan yang lebih tinggi.
2. Untuk mempercepat proses kriptografi baik enkripsi maupun deskripsi bisa menggunakan bantuan bahasa pemrogaman komputer yang ada.
3. Penelitian dapat dilanjutkan untuk hasil enkripsi yang berupa barcode maupun gambar.

DAFTAR PUSTAKA

[1]. Anna, Deffi, Ika, 2017, *Matrik dan Ruang Vektor*, Malang : Media Nusa Kreatif

[2]. Indriati, Kumala, 2019. *Matrik, Vektor dan Program Linear.* Jakarta: Universitas Katolik Indonesia Atma Jaya.

[3]. Khowarsimi, al, 2021, *Pengantar TEknologi Informasi (Dalam Perkembangan Data Scient)* , Medan: UMSU

[4]. Ruminta, 2009, *Matrik Persamaan Lineardan Pemrogaman Linear*, Bandung : Rekayasa Sains.

[5]. Siahaan, Vivian dan Rismon Hasiholan Sianipar, 2019, *Database dan kriptografi menggunakan java/mysql* : Sparta Publising

[6]. Taufik, Marhan, 2000, *Pengantar Teori Bilangan.* Malang: Universitas Muammadiyah Malang.