JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 90-93
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Kriptografi dan Penerapannya Dalam Sistem Keamanan Data

Nanda Amalya[1]*, Santa Maria Sopiana Silalahi[2], Della Fatricia Nasution[3], Melia Sari[4], Indra Gunawaan[5]

[1,2,3,4,5] Teknik Informatika, Stikom Tunas Bangsa Pematangsiantar, Pematangsiantar 21127, Indonesia
Email: [1*]nandaamalya2323@gmail.com, [2]santasilalahi14@gmail.com, [3]dellafatricianasution@gmail.com,
[4]meliasaari058@gmail.com, [5]indra@amiktunasbangsa.ac.id
Correspondence Writer's Email: [1]nandaamalya2323@gmail.com

Abstrak− Pemahaman tentang apa itu kriptografi, untuk memahami kriptografi dan bagaimana penerapannya dalam keamanan data, sehingga data akan lebih aman dan terlindungi dari spamming atau peretasan informasi secara ilegal. Pengamatan terhadap kriptografi dan penerapannya terhadap keamanan data dilakukan dengan menggunakan Pendekatan Studi Sastra. Studi Kepustakaan adalah teknik pengumpulan data dengan mempelajari berbagai buku referensi dan hasil penelitian sejenis sebelumnya, yang berguna untuk memperoleh landasan teori tentang masalah yang akan diteliti. Kriptografi adalah teknik penyampaian pesan secara tersembunyi dengan menggunakan fitur enkripsi data, yang berfungsi untuk mengamankan data, baik yang ditransfer melalui jaringan komputer maupun tidak, yang sangat berguna untuk melindungi, privasi, integritas data, otentikasi, dan non-repudiation . Saat ini penggunaan kriptografi sudah mulai banyak digunakan dalam kehidupan sehari-hari. Gunakan sistem kriptografi untuk keamanan data Anda saat mengakses informasi.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, Keamanan Data, Chiper

Abstract− An understanding of what cryptography is, to understand cryptography and how it is applied in data security, so that data will be safer and more protected from spamming or illegal hacking of information. Observations of cryptography and its application to data security are carried out using the Approach of Literary Studies. Library Studies is a data collection technique by studying various reference books and the results of previous similar research, which is useful for obtaining a theoretical foundation on the problem to be studied. Cryptography is a technique of conveying messages in a hidden manner by using data encryption features, which serve to secure data, whether transferred through a computer network or not, which is very useful for protecting, privacy, data integrity, authentication, and non-repudiation. Nowadays the use of cryptography has begun to be widely used in everyday life. Use cryptographic systems for the security of your data when accessing information.

Keywords: Cryptography, Encryption, Decryption, DataSecurity, Chiper

1. PENDAHULUAN

Menurut catatan sejarah kuno, aplikasi kriptografi pertama (yang telah ditemukan) adalah hieroglyphics yang diterapkan oleh orang Mesir kuno pada awal 3000 tahun SM. Mulai ada di masa kejayaan Yunani oleh spartan di Yunani sekitar 400 SM. Pada saat itu alat yang digunakan untuk membuat pesan tersembunyi disebut Scytale. Scytale memiliki bentuk batang silinder dengan kombinasi 18 huruf dan pita panjang yang terbuat dari bahan papirus, cara membaca pesannya adalah dengan menggulung pita pada batang silinder. Orang Cina dan Jepang mulai mengenali kriptografi pada abad ke-15 M.[1]

Di bawah pemerintahan Julius Caesar (zaman Romawi), teknik caesar cipher diciptakan untuk mengirim pesan rahasia kepada anggota militer yang berada di tengah-tengah perang. Penggunaan kriptografi juga semakin intens karena pertimbangan stabilitas negara. Meskipun teknik yang digunakan tidak serumit orang Yunani, untuk memahami pesan kriptografi dari periode Romawi cukup sulit untuk dikerjakan[2].

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, cipher yang lebih kompleks menjadi sangat mungkin untuk dihasilkan. Tidak seperti kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisional), kriptografi modern beroperasi pada string biner. Cipher yang kompleks seperti DES (Data Encryption Standard) dan penemuan algoritma RSA adalah algoritma kriptografi modern yang paling dikenal di dalam sejarah kriptografi modern[3].

Di Indonesia kriptografi dikenal atau bisa juga disebut dengan kriptologi ataupun sandisastra. Salah satu tujuan dari kriptografi adalah melakukan berbagai upaya komunikasi antar individu ataupun kelompok secara aman tanpa kehadiran pihak-pihak yang tidak diinginkan, serta menganalisis komunikasi yang sulit dipahami.[4],[5]

2. METODOLOGI PENELITIAN

Pada penelitian jurnal ini, menggunakan metode internet searching yang merupakan teknik pengumpulan data melalui bantuan teknologi yang berupa alat atau mesin pencari di internet dimana segala informasi dari berbagai era tersedia didalamnya[6],[7].

Submited: **01/03/2023**; Acepted: **11/04/2023** ; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 90-93
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Selain intenet searching, pengamatan tentang kriptografi dan penerapannya terhadap keamanan data juga dilakukan dengan metode pendekatan Studi Pustaka. Studi Pustaka [8] yaitu merupakan teknik pengumpulan data dengan mempelajari berbagai buku referensi serta hasil penelitian yang sudah ada sebelumnya yang sejenis, yang berguna untuk mendapatkan landasan teori mengenai masalah-masalah yang akan diteliti. [9],[10])

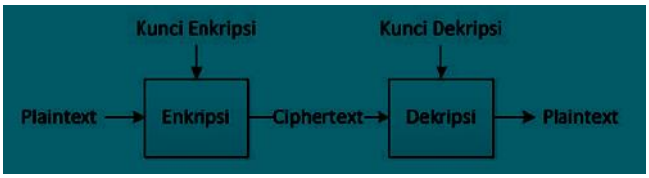
3. HASIL DAN PEMBAHASAN

Kata kriptografi (cryptography) berasal dari bahasa Yunani yaitu Kryptos (tersembunyi atau rahasia) dan Graphein (menulis atau tulisan). Sehingga dapat dijabarkan bahwa secara harfiah makna kriptografi adalah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya.

Kriptografi memiliki arti lain, yaitu suatu ilmu yang mempelajari tentang teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi data atau keamanan pesan dengan menggunakan dua proses dasar kriptografi yaitu enkripsi dan deskripsi.

Enkripsi dapat diartikan sebagai cipher atau kode, merupakan proses penyembunyian sebuah data pesan, dengan cara mengubah plaintext (Pesan yang bisa dibaca) menjadi ciphertext (Pesan acak yang tidak bisa dibaca). Sedangkan Deskripsi merupakan kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Proses Enkripsi/Dekripsi :



Gambar 1. Proses enkripsi/dekripsi

Kriptografi terbagi menjadi dua jenis yaitu Kriptografi Klasik dan Kriptografi Modern.

a) Kriptografi Klasik
Merupakan kriptografi yang digunakan sebelum atau sesudah penemuan komputer, tapi tidak sepopuler saat ini.. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z dan tidak disarankan untuk mengamankan informasi penting karena mudah dipecahkan dalam kurun waktu yang singkat, Penggunaan kriptografi klasik memberikan prinsip untuk menjaga keamanan kunci itu sendiri.
Ciri-ciri :
- Berbasis karakter
- Menggunakan pena dan kertas
- Termasuk kedalam kiptografi kunci simetris

Algoritma kriptografi klasik :

1. Substitution Ciphers
Merupakan penggantian setiap karakter dari plaintext dengan karakter lain dalam susunan abjad (alfabet). Substitusi pertama kali ada dalam dunia persandian pada masa pemerintahan yulius caesar dan dikenal dengan sebutan caesar cipher.
Misalnya pada Caesar Chiper, setiap huruf di substitusi dengan tiga huruf berikutnya. Maka dalam hal ini, kuncinya adalah pergeseran tiga huruf (kunci = 3).

Tabel 1. Substitusi Caesar Cipher

Plainteks	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chiperteks	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Contoh :
Plainteks : **STIKOM TUNAS BANGSA PEMATANGSIANTAR**
Dengan menggunakan caesar cipher, maka pesan tersebut akan dienkripsi menjadi,

Submited: **01/03/2023**; Acepted: **11/04/2023** ; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 90-93
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Chiperteks : **VWLNRP WXQDV EDQJVD SHPDWDQJVLDQWDU**

Agar kriptanalis menjadi lebih sulit, Cipherteks dapat dikelompokkan kedalam kelompok n-huruf, misal kelompok 4-huruf :

VWLN RPWX QDVE DQJV DSHP DWDQ JVLD QWDU

Atau dengan membuang semua spasi :

VWLNRPWXQDVEDQJVDSHPDWDQJVLDQWDU

Dan jika dilakukan dekripsi pesan, akan kembali ke pesan aslinya.

Mengkodekan setiap huruf abjad dengan bilangan bulat (integer) ; A = 0, B = 1, …, Z = 25.

Menyandikan Plainteks (P) menjadi Chiperteks (C) :

$$C = E(P) = (pi + k) \bmod 26$$

Menyandikan Chiperteks (C) menjadi Plainteks (P) :

$$P = D(P) = (ci - k) \bmod 26$$

* pi : karakter ke-i dari Plainteks (P)
* ci : karakter ke-i dari Chiperteks (C)

Jenis-jenis substitution ciphers :

a) Monoalphabetic Cipher
Cipher yang mengubah tiap huruf nya pada plainteks dengan huruf yang bersesuaian.
Jumlah kemungkinan susunan huruf yang dapat dibuat adalah
26! = 403.291.461.126.605.635.584.000.000

b) Homophonic Substitution Cipher
Pada tiap huruf plainteks dihubungkan kedalam salah satu huruf cipherteks.

c) Polyalphabetic Substitusion Cipher
Pensubstitusian setiap huruf menggunakan kunci yang berbeda.

d) Polygram Substitution Cipher
Blok karakter disubstitusikan dengan blok cipherteks.

2. Transpotition Chiper
Teknik ini menggunakan permutasi karakter, dimana teknik ini memungkinkan pesan yang asli tidak dapat dibaca kecuali memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula atau disebut deskripsi.

Contoh :
Plainteks : **TUNAS BANGSA PEMATANGSIANTAR**
Enkripsi : **TUNASB**
ANGSAP
EMATAN
GSIANT
ARZZZZ
Chiperteks (baca secara vertikal)
TUAEGAUNMSRNGAIZASTAZSAANZBPNTZ
TUAE GAUN MSRN GAIZ ASTA ZSAA NZBP NTZ

b) Kriptografi Modern
Merupakan kriptografi yang cukup rumit. Dibutuhkan pengetahuan matematika untuk menguasainya. Oleh karena itu kriptografi modern berkembang bersamaan dengan berkembangnya komputer hingga jaman sekarang.
Terdiri dari 3 bagian, yaitu :
1) Algoritma Simetris
Menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu.

Submited: **01/03/2023**; Acepted: **11/04/2023** ; Published: **01/06/2023**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 4, Nomor 2, Juni 2023, Page 90-93
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

2) Algoritma Asimetris
Pasangan kunci kriptografi yang salah satunya digunakan sebagai proses enkripsi dan deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya guna mengenkripsi suatu pesan, dan hanya satu orang saja yang memiliki rahasia itu dimana dalam hal ini, kunci rahasia digunakan untuk melakukan pembongkaran terhadap kode yang dikirim untuknya.
3) Algortima Hibrida
Memanfaatkan dua tingkatan kunci, yaitu kunci rahasia (simetri) yang disebut juga session key (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia – kunci publik untuk pemberian tanda tangan digital serta melindungi kunci simetri.

Kriptografi berfungsi mengamankan data, baik yang ditransfer melalui jaringan komputer maupun tidak, dimana hal tersebut sangat berguna untuk melindungi,privasi, integritas data, authentication, dan non-repudiation.

a. Confidentiality (Kerahasiaan)
Informasi yang dilindungi tidak akan bisa diakses oleh siapa pun yang tak memiliki wewenang.
b. Integrity Data (Integritas Data)
Data yang akan diterima dan dikirim tidak dapat diubah tanpa sepengetahuan kedua belah pihak.
c. Authentication (Autentikasi)
Pihak penerima dan pengirim dapat mengetahui identitas masing-masing serta sumber data yang sedang mereka gunakan.
d. Non-Repudiation
Pihak penerima atau pengirim tidak akan bisa menyangkal tujuannya menciptakan atau mengubah suatu data.

4. KESIMPULAN

Penggunaan kriptografi sudah mulai banyak di gunakan dalam kehidupan sehari-hari. Saat mengakses informasi di Internet, gunakan sistem enkripsi untuk memastikan keamanan data. Hasilnya, data lebih terlindungi dari spam dan peretas ilegal. Saat ini Kriptografi bukan hanya dipakai untuk menulis atau pun menyelesaikan kode, tetapi kriptografi sudah berkembang ke berbagai macam fungsi seperti enkripsi/dekripsi untuk pengamanan data, otentikasi identitas dan pesan, tanda tangan dan sertifikat digital, protokol pertukaran kunci, uang digital, dan lain sebagainya.

REFERENSI

[1] R. Dea Mustika, A. Zakir, and A. Rizmi, "IMPLEMENTASI ALGORITMA K-MEANS UNTUK CLUSTERING JUDUL SKRIPSI UNIVERSITAS HARAPAN MEDAN," *J. Media Inform.*, vol. 4, no. 1, pp. 40–47, Nov. 2022, doi: 10.55338/jumin.v4i1.405.
[2] S. P. Lestari, H. N. Fadlan, R. Angelia Purba, and I. Gunawan, "REALISASI KRIPTOGRAFI PADA FITUR ENKRIPSI END-TO-END PESAN WHATSAPP," *J. Media Inform.*, vol. 4, no. 1, pp. 1–8, Nov. 2022, doi: 10.55338/jumin.v4i1.423.
[3] J. H. Sinaga, M. Pangaribuan, I. Rivaldo, and I. Gunawan, "Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Data Encryption Standart (DES) Dengan Pemograman Matlab," vol. 4, 2022.
[4] P. A. M. Z. R.W.P.P.Zer and I. Gunawan, "Penerapan Data Mining Naïve Bayes Dalam Klasifikasi Kepuasan Mahasiswa Berlangganan WiFi Indihome," *J. Media Inform.*, vol. 3, no. 2, pp. 112–118, Jun. 2022, doi: 10.55338/jumin.v3i2.488.
[5] N. D. Farhanah, "Optimalisasi Penentuan Kinerja Perawat Terbaik di Klinik Amanah dengan Sistem Pendukung Keputusan dan Metode Simple Additive Weighting," vol. 2, 2023.
[6] B. Sapriatin and F. A. Sianturi, "Penerapan Teorema Bayes Mendeteksi Stunting pada Balita," vol. 3, 2021.
[7] A. Suaib and I. I. Tritosmoro, "Perbandingan Performa Metode Local Binary Pattern dan Random Forest dalam Identifikasi COVID-19 pada Citra X-ray Paru-paru.," vol. 2, 2023.
[8] D. E. Frans, "Peningkatan Produksi Budidaya Perikanan dengan Penerapan Algoritma Apriori dan Association Rule," vol. 2, 2023.
[9] N. Hafizar, E. R. Syahputra, and D. Irwan, "Desain Dan Penerapan Sistem Informasi Untuk Pemasaran Biji Kopi Dan Bubuk Kopi Arabika Berbasis Android," vol. 4, 2022.
[10] A. Simangunsong, R. M. Simanjorang, and H. Fahmi, "Penerapan Metode Composite Performance Index Dalam Seleksi Penerimaan Calon Laboran," vol. 1, 2022.

Submited: **01/03/2023**; Acepted: **11/04/2023** ; Published: **01/06/2023**