JETBUS Journal of Education Transportation and Business
E-ISSN: 3062-8121 P-ISSN: 3062-813X
Vol. 1 No. 2 Desember 2024

Aplikasi Enkripsi dan Deskripsi Teks Menggunakan Vernam Chiper Berbasis Web

Hijka Listia[1] Sabina Wardaniah[2] Zulfahmi Indra[3]
Program Studi Ilmu Komputer, Universitas Negeri Medan, Kota Medan, Provinsi Sumatera Utara, Indonesia[1,2,3]
Email: hsbtia62@mhs.unimed.ic.id[1] sabinawardaniah@mhs.unimed.ac.id[2]
zulfahmi.indra@unimed.ac.id[3]

Abstrak

Dalam era digital yang berlangsung saat ini, keamanan data menjadi aspek yang sangat penting, khususnya untuk menjaga kerahasiaan sebuah informasi yang sensitif. Kriptografi adalah studi tentang menjaga data atau pesan tetap aman. Penelitian ini bertujuan untuk merancang dan membangun sebuah sistem enkripsi dan dekripsi berbasis web yang menggunakan teknik vernam cipher. Salah satu metode kriptografi untuk melindungi informasi adalah Vernam Cipher. Vernam Cipher adalah teknik enkripsi simetris yang menggunakan kunci acak dengan panjang yang sama dengan pesan asli untuk membuat ciphertext yang aman dan sulit untuk dibongkar. Dalam penelitian ini, telah dibuat aplikasi web untuk mengenkripsi dan mendeskripsi teks dengan menggunakan algoritma Vernam Cipher. Aplikasi ini memungkinkan pengguna untuk mengenkripsi teks menjadi kode rahasia serta mendekripsinya kembali menggunakan kunci yang sama. Teknologi berbasis web dipilih karena memiliki tingkat aksesibilitas yang tinggi dan mudah digunakan. Hasil uji menunjukkan aplikasi dapat berfungsi optimal dalam proses enkripsi dan dekripsi teks dengan cepat dan akurat. Diharapkan aplikasi ini dapat meningkatkan keamanan data dalam komunikasi digital.

Kata Kunci: Aplikasi Web, Deskripsi, Enkripsi, Kriptografi, Vernam Chiper

PENDAHULUAN

Kemajuan teknologi dan internet yang sangat pesat telah meningkatkan kebutuhan akan keamanan informasi, khususnya dalam pertukaran data. Salah satu teknik umum untuk menjaga kerahasiaan informasi adalah dengan menggunakan kriptografi. Kriptografi bertujuan melindungi pesan dari akses pihak yang tidak berwenang melalui proses enkripsi dan dekripsi. Kriptografi merupakan ilmu yang membahas teknik enkripsi, di mana data diacak dengan kunci enkripsi sehingga sulit dibaca tanpa kunci dekripsi. Kriptografi berasal dari Bahasa Yunani kuno, crypto yang berarti rahasia dan graph yang berarti tulisan. Oleh karena itu, kriptografi dapat diartikan sebagai tulisan rahasia. Kriptografi digunakan dalam dunia komputer untuk mengamankan file. Kriptografi memiliki dua komponen kunci, yakni enkripsi dan dekripsi. Enkripsi adalah proses penyandian data dengan memasukkan kunci agar data tersebut tidak mudah terbaca, Sedangkan deskripsi adalah proses mengartikan informasi atau mengubah informasi kembali ke bentuk aslinya untuk memahami maksud yang ingin disampaikan oleh pengirim.

Penelitian oleh mengembangkan aplikasi berbasis web untuk pengamanan data menggunakan metode RSA dan AES, yang menunjukkan bahwa aplikasi kriptografi berbasis web dapat diimplementasikan secara efisien untuk komunikasi jarak jauh. Namun, metode modern seperti AES dan RSA lebih kompleks dan memerlukan sumber daya komputasi yang lebih tinggi dibandingkan dengan kriptografi klasik seperti Vernam Cipher. Menurut Stallings, kriptografi klasik seperti Vernam Cipher meskipun sudah berusia tua, tetap relevan dalam pembelajaran dasar kriptografi. Penelitian ini melakukan penerapan metode Vernam Cipher

sebagai solusi untuk mengatasi tantangan keamanan dan kebutuhan enkripsi sederhana pada aplikasi berbasis web. Vernam Cipher terkenal karena tingkat keamanannya yang tinggi, yang tidak dapat ditembus asalkan kunci yang digunakan benar-benar acak. Vernam Cipher adalah sebuah metode enkripsi simetris, terkenal dengan konsep "One-Time Pad" yang menggunakan kunci acak unik sepanjang pesan untuk memberikan keamanan maksimum. Dalam proses enkripsi, algoritma ini menggunakan stream cipher dengan melakukan XOR antara bit plaintext dan bit kunci. Pada metode ini, teks biasa diubah menjadi kode ASCII, kemudian di-XOR dengan kunci yang juga telah diubah menjadi kode ASCII.

Penggunaan metode ini diharapkan dapat menghasilkan aplikasi yang mudah digunakan untuk menyandikan dan mendekripsi teks, dengan tingkat keamanan yang lebih baik daripada metode sederhana lainnya. Aplikasi ini dibuat agar bisa diakses secara real-time dan memungkinkan pengguna untuk langsung mengenkripsi dan mendekripsi pesan melalui antarmuka web yang sederhana. Penelitian ini ingin mengembangkan aplikasi web yang dengan menginplementasikan algoritma Vernam Cipher dalam proses enkripsi dan dekripsi teks. Dengan aplikasi ini maka pengguna dapat dengan mudah mengenkripsi dan mendekripsi pesan secara online, tanpa memerlukan instalasi perangkat lunak tambahan. Selain itu, diharapkan aplikasi ini dapat berguna kepada yang membutuhkan.

Metode penelitian

Pada penelitan ini peneliti menggunakan 5 tahapan yaitu Studi literatur, Identifikasi masalah, Perancangan aplikasi, Pembuatan aplikasi dan Pengujian system.

Gambar 1. Alur Penelitian

Studi Literatur

Dalam proses ini peneliti melakukan pengumpulan informasi dan beberapa referensi yang berkaitan dengan teknik enkripsi dan deskripsi teks, khususnya tentang algoritma Vernam Cipher. Penelitian literatur juga mencakup kajian tentang aplikasi berbasis web yang relevan untuk penerapan sistem enkripsi dan deskripsi.

1. Kriptografi. Enkripsi merupakan proses mengubah data dari format yang dapat dibaca menjadi kode yang sulit dipahami. Fungsi utama enkripsi adalah untuk melindungi data. Enkripsi digunakan untuk melindungi data dari ancaman di dunia maya. Contohnya termasuk peretasan email, phishing, pencurian data, dan pencurian kartu kredit. Enkripsi dilakukan dengan mengacak data sensitif sehingga tidak dapat dengan mudah diakses oleh pihak yang tidak berwenang. Hal ini bertujuan untuk mencegah upaya peretasan data, mereka tidak dapat menggunakannya dengan mudah karena proses enkripsi ini. Enkripsi dibuat untuk melindungi data atau menjaga kerahasiaannya. Data terenkripsi juga dapat didekripsi artinya dapat diubah menjadi teks seperti data aslinya.
2. Pesan. Pesan merupakan informasi yang mudah dibaca dan dipahami yang artinya pesan tersebut berupa teks biasa teks biasa. pesan dalam kriptografi disebut plaintext, Plaintext adalah pesan bermakna yang diproses secara instan menggunakan algoritma kriptografi dan pesan yang akan dikirimkan yang berisi data asli.
3. Chipertext. Chiperteks adalah jenis pesan yang telah dienkripsi dan harus dapat didekripsi kembali menjadi teks biasa agar pesan yang diterima dapat terbaca. Chiperteks tidak bisa dibaca tanpa kunci enkripsi yang sesuai.
4. Enkripsi. Enkripsi merupakan proses mengubah data dari format yang dapat dibaca menjadi kode yang sulit dipahami. Fungsi utama enkripsi adalah untuk melindungi data. Enkripsi digunakan untuk melindungi data dari ancaman di dunia maya. Contohnya termasuk peretasan email, phishing, pencurian data, dan pencurian kartu kredit. Enkripsi dilakukan dengan mengacak data sensitif sehingga tidak dapat dengan mudah diakses oleh pihak yang tidak berwenang. Hal ini bertujuan untuk mencegah upaya peretasan data, mereka tidak dapat menggunakannya dengan mudah karena proses enkripsi ini. Enkripsi dibuat untuk melindungi data atau menjaga kerahasiaannya. Data terenkripsi juga dapat didekripsi artinya dapat diubah menjadi teks seperti data aslinya.
5. Deskripsi. Dekripsi yaitu proses mengembalikan ciphertext yang diubah menjadi plaintext dengan cara yang sama seperti awal yang disebut dengan penguraian kode. Setelah pesan sampai ke pihak yang ditentukan maka dekripsi dilakukan.
6. Kunci (key). Kunci adalah parameter untuk enkripsi dan dekripsi. Kunci dibagi dua, yaitu kunci privat dan kunci publik. Kunci privat digunakan untuk proses deskripsi, dan kunci publik untuk enkripsi. Tujuan kriptografi bukan hanya melindungi data, tetapi juga memastikan keaslian dan integritasnya. Kriptografi terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik menggunakan satu kunci untuk melindungi data. Metode ini digunakan beberapa abad yang lalu. Pada prose enkripsi karakter akan diacak menjadi plaintext/teks biasa. Enkripsi ini tidak disarankan untuk melindungi informasi sensitif karena ini hanya susunan huruf acak dari A sampai Z dan dapat dibobol dalam waktu singkat. Meskipun kriptografi klasik kini sudah ditinggalkan, kriptografi klasik masih disertakan dalam seluruh pelajaran kriptografi sebagai pengantar kriptografi modern. Sedangkan kriptografi modern lebih baik dibandingkan dengan kriptografi klasik. Beberapa contoh algoritma enkripsi yang umum digunakan adalah MD5, RC4, dan AES. Algoritma ini memiliki tingkat kesulitan kompleks, sehingga sulit bagi cryptanalyst untuk memecahkan ciphertext tanpa kunci. Ada tiga jenis kunci dalam enkripsi modern: simetris, asimetris, dan hibrida.
7. Keamanan Data. Keamanan merupakan kondisi bebas dari bahaya dan ancaman. Keamanan merupakan elemen penting dalam sistem informasi. Masalah keamanan sering diabaikan oleh perancang dan pengelola sistem informasi. Masalah keamanan sering diposisikan setelah tampilan atau bahkan di urutan terakhir dalam daftar hal yang dianggap penting. Keamanan data kini menjadi sangat penting dalam transaksi komersial dan perdagangan

tradisional. Contohnya ketika menggunakan media transmisi data elektronik, seperti email atau media lain yang sering digunakan dalam bisnis. Terdapat berbagai jenis data yang dikirim melalui email, seperti data umum dan sensitif. Berdasarkan situasi dan kenyataan tersebut, ahli dan peneliti IT sedang mencoba berbagai cara untuk membangun sistem keamanan data. Salah satu cara untuk melindungi data sensitif yaitu dengan menggunakan metode kriptografi. Hal ini bertujuan agar data tersebut tidak dapat diakses oleh pihak yang tidak berhak.

8. Vernam Chiper. Vernam Cipher adalah sebuah algoritma enkripsi kunci simetris. Vernam Cipher merupakan salah satu algoritma block cipher yang paling cepat. Proses enkripsi Vernam Cipher melibatkan operasi XOR yang menggabungkan bit plaintext dengan bit keystream. Keunggulan algoritma cipher Vernam dibandingkan cipher lainnya adalah penggunaan kunci pseudo-Rand yang panjangnya sama dengan fungsi XOR. Namun, kelemahan algoritma Vernam cipher adalah bahwa hasil enkripsi masih jelas terlihat oleh manusia, sehingga dapat mudah diidentifikasi sebagai data yang asli setelah proses enkripsi selesai.
9. Aplikasi. Aplikasi artinya pelaksanaan atau kegunaan. Menurut konsep ini, aplikasi yaitu sebuah program yang siap digunakan. Singkatnya Aplikasi adalah program komputer yang dibuat untuk melaksanakan tugas-tugas khusus bagi pengguna. Aplikasi adalah kumpulan aktivitas atau perintah yang dieksekusi oleh komputer.
10. Web. Web merupakan sistem informasi yang mendukung interaksi pengguna melalui antarmuka berbasis Web. Fitur-fitur Web umumnya mencakup persistensi data, transaksi, dan komposisi halaman Web dinamis yang menggabungkan hypermedia dan sistem informasi.

Identifikasi Masalah

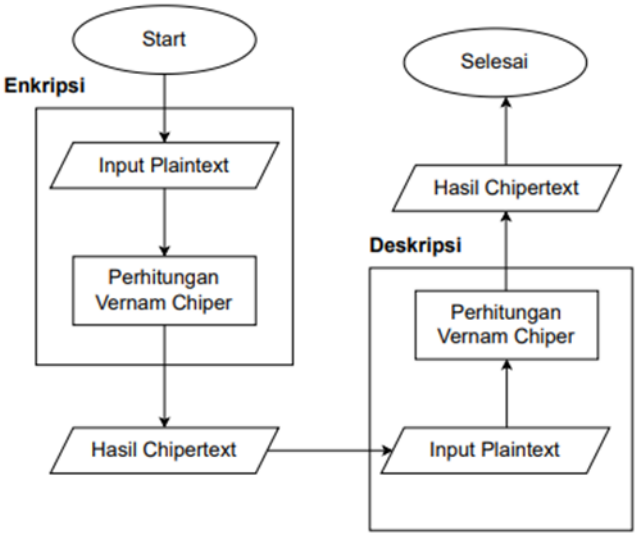
Dalam proses ini peneliti melakukan identifikasi masalah terkait keamanan data dalam bentuk teks pada sistem berbasis web. Dari identifikasi masalah tersebut diputuskan bahwa diperlukan sebuah sistem yang dapat mengamankan teks dengan menggunakan metode enkripsi dan deskripsi yang tepat yaitu Vernam Cipher.

Perancangan Aplikasi

Tahap ini meliputi proses perancangan sistem aplikasi yang akan dikembangkan. Desain dari aplikasi berbasis web untuk enkripsi dan deskripsi teks disusun pada tahap ini, termasuk perancangan arsitektur sistem, antarmuka pengguna, dan alur enkripsi/deskripsi menggunakan Vernam Cipher.

Pembuatan Aplikasi

Pada tahap ini aplikasi akan dikembangkan sesuai dengan desain yang telah dibuat. Pembuatan aplikasi ini melibatkan pengkodean program berbasis web yang memanfaatkan algoritma Vernam Cipher untuk mengenkripsi dan mendeskripsi teks sesuai masukan pengguna.



Gambar 2. Cara Kerja Sistem

Pengujian Sistem

Pengujian dilakukan setelah pembuatan aplikasi selesai, ini bertujuan untuk memastikan aplikasi mampu berjalan dengan baik dan sesuai fungsinya. Pengujian pada system ini akan meliputi verifikasi apakah proses enkripsi dan deskripsi teks berjalan dengan benar serta apakah aplikasi berbasis web tersebut memiliki performa yang optimal. Setelah aplikasi berhasil diuji dan semua masalah teratasi, penelitian dianggap selesai. Aplikasi enkripsi dan deskripsi teks berbasis Vernam Cipher siap digunakan atau diimplementasikan sesuai dengan tujuan awal.

HASIL PENELITIAN DAN PEMBAHASAN

Peneliti akan menggunakan beberapa aplikasi seperti XAMPP, Chrome, dan Visual Studio Code untuk menampilkan hasil kerja pada web. Bahasa pemrograman yang digunakan pada penelitian yaitu Javascript. Hasil ini program akan melakukan proses enkripsi dan dekripsi menggunakan kunci atau key. Pada rancangan ini peneliti mengunakan kasus untuk mengenkripsi dan mendeskripsi yaitu:
Plaintext: MUSIK
Key: 3

Proses Enkripsi

Proses enkripsi dalam metode ini yaitu sebagai berikut:
Plaintext: MUSIK
Key: 3

Tabel 1. Plaintext

Plaintext	Nilai Biner
M	01001101
U	01010101
S	01010011
I	01001001
K	01001011

Tabel 2. Key

Key	Nilai Biner
3	00110011

Kemudian dilakukan proses enkripsi menggunakan logika XOR yaitu:

Tabel 3. Enkripsi

Nilai Biner Plaintext	Nilai Biner Key	Hasil XOR	Karakter
01001101	00110011	01111110	**~**
01010101	00110011	01100110	**f**
01010011	00110011	01100000	**`**
01001001	00110011	01111010	**z**
01001011	00110011	01111000	**x**

Jadi, chipertext dari kata MUSIK adalah ~ f ` z x.

Proses Dekripsi

Sedangkan pada proses deskripsi itu sama seperti proses enkripsi yaitu dengan melakukan proses logika XOR pada chipertext dan key.

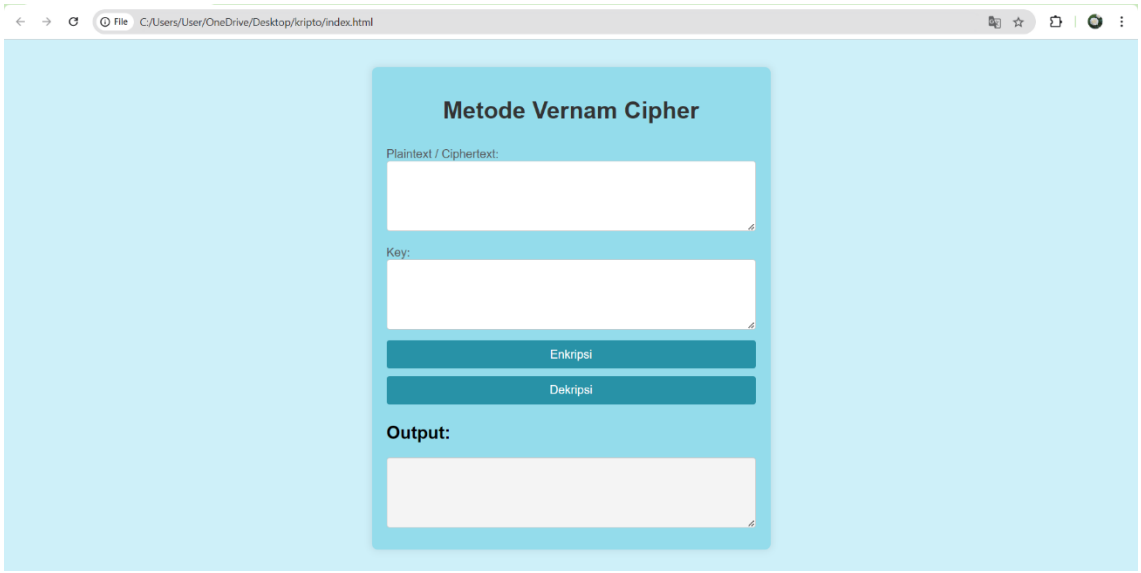
Table 4. Dekripsi

Nilai Biner Chipertext	Nilai Biner Key	Hasil XOR	Karakter
01111110	00110011	01001101	M
01100110	00110011	01010101	U
01100000	00110011	01010011	S
01111010	00110011	01001001	I
01111000	00110011	01001011	K

Jadi, didapatlah plaintext dari kata ~ f ` z x adalah MUSIK.

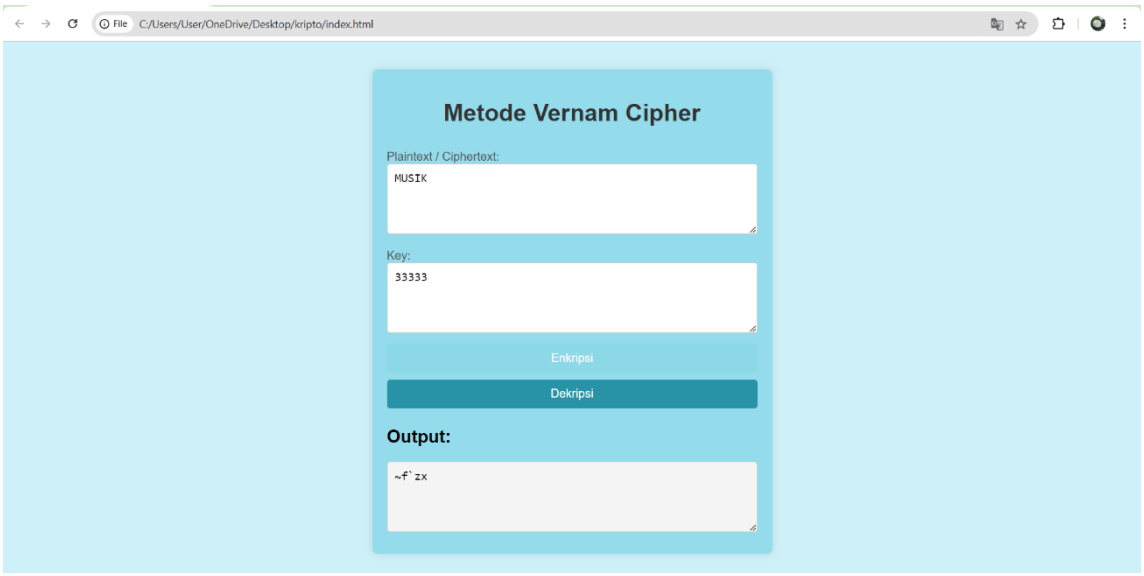
Dibawah ini merupakan tampilan utama untuk melakukan proses enkripsi dan deskripsi pada metode vernam chiper, yang mana terdapat beberapa kolom yaitu:

1. Kolom Plaintext/Ciphertext sebagai area teks yang memungkinkan pengguna untuk memasukkan teks yang akan dienkripsi (plaintext) atau teks terenkripsi yang akan didekripsi (ciphertext).
2. Kolom Key yaitu pengguna memasukkan kunci yang digunakan untuk proses enkripsi atau dekripsi. Dalam metode Vernam Cipher, kunci harus sepanjang teks yang dienkripsi/didekripsi.
3. Tombol Enkripsi dan Dekripsi yang digunakan untuk mengubah teks biasa (plaintext) menjadi teks terenkripsi (ciphertext).
4. Output adalah Area yang akan menampilkan hasil dari proses enkripsi atau dekripsi.



Gambar 3. Tampilan Sistem

Sebagai contoh pada gambar dibawah ini peneliti ingin mengenkripsikan sebuah teks atau pesan sehingga peneliti langsung memasukkan teks atau pesan pada kolom plaintekt yaitu MUSIK, sedangkan pada kolom key adalah 3 (sebanyak 5 digit angka 3). Maka output yang dihasilkan adalah ~ f ` z x.



Gambar 4. Proses Enkripsi

Dan sebaliknya jika dideskripsikan menggunakan chipertext ~ f ` z x dengan kunci 3 akan menghasilkan output yaitu MUSIK.

Gambar 5. Proses Deskripsi

KESIMPULAN

Penelitian ini berhasil menciptakan dan menerapkan aplikasi web untuk melakukan proses enkripsi maupun dekripsi teks dengan menggunakan algoritma Vernam cipher. Algoritma vernam cipher, dikenal sebagai metode enkripsi simetris menggunakan XOR, efektif dalam menjaga kerahasiaan data jika kunci dan teks sama panjang. Aplikasi web memungkinkan pengguna melakukan enkripsi dan dekripsi dengan mudah melalui antarmuka yang ramah pengguna dan efisien. Implementasi web juga memungkinkan aksesibilitas yang luas tanpa perlu instalasi perangkat lunak tambahan. Hasil pengujian aplikasi menunjukkan bahwa aplikasi ini mampu bekerja dengan stabil dan mampu mengamankan teks dengan baik. Sesuai dengan karakteristik dasar Vernam cipher, yaitu menjaga keamanan tinggi jika kunci bersifat acak dan tidak diulang.

DAFTAR PUSTAKA

A. Setiawan and T. Fatimah, “Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia,” Skanika, vol. 4, no. 1, pp. 66–71, 2021, doi: 10.36080/skanika.v4i1.2044.

A. Z. F. Rangkuti and H. Fahmi, “Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5,” J. Nas. Komputasi dan Teknol. Inf., vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

D. Adhar, “Implementasi Algoritma DES (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android.,” J. Tek. Inform. Kaputama, vol. 3, no. 2, pp. 53–60, 2019.

D. Alfiani Fauzan and A. Fathurrozi, “Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web,” J. Inf. Inf. Secur., vol. 4, no. 1, pp. 2722–4058, 2023, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

D. Melanda, A. Surahman, and T. Yulianti, “Pengembangan Media Pembelajaran IPA Kelas IV Berbasis Web (Studi Kasus : SDN 02 Sumberejo),” J. Teknol. Dan Sist. Inf., vol. 4, no. 1, pp. 28–33, 2023

E. Ndururu, M. Sayuthi, and A. H. Hasugian, “Proteksi Database dengan Algoritma Vernam Cipher,” J. Armada Inform., vol. 6, no. 2, pp. 606–611,2022,[Online].Available:https://scholar.google.com/citations?view_op=view_citatio

n&hl=en&user=5M9hHjkAAAAJ&pagesize=100&citation_for_view=5M9hHjkAAAAJ:-f6ydRqryjwC

F. Febrian and A. Hastuty, "Penerapan Algoritma Vernam Chiper Pada File Transfer Protocol Server Berbasis Php," J. Sintaks Log., vol. 3, no. 3, pp. 45–52, 2023, doi: 10.31850/jsilog.v3i3.2590.

Indri Widya Wulandari and Hwihanus Hwihanus, "Peran Sistem Informasi Akuntansi Dalam Pengaplikasian Enkripsi Terhadap Peningkatan Keamanan Perusahaan," J. Kaji. dan Penal. Ilmu Manaj., vol. 1, no. 1, pp. 11–25, 2023, doi: 10.59031/jkpim.v1i1.46.

L. Silalahi and A. Sindar, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," J. Nas. Komputasi dan Teknol. Inf., vol. 3, no. 2, pp. 182–186, 2020, doi: 10.32672/jnkti.v3i2.2413.

L., "Penyandian Teks Dengan Kombinasi Vernam Cipher Dan Caesar Cipher 220," J. Mahajana Inf., vol. 5, no. 1, pp. 22–28, 2020, doi: 10.51544/jurnalmi.v5i1.1193.

M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," J. Pendidik. Sains dan Komput., vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

M. Harun Alfirdaus et al., "Perancangan Aplikasi Enkripsi Deskripsi Mengunakan Metode Caesar Chiper Berbasis Web," Jtmei), vol. 2, no. 2, pp. 64–76, 2023.

S. Andika, "Implementasi Algoritma Freivlds Untuk Pembangkitan Kunci AlgoritmaRSA Pada Pengamanan Data Video," Pelita Inform. Inf. dan Inform., vol. 10, no. 2, pp. 70–77, 2021.

S. Aripin and M. Syahrizal, "Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakan Algoritma Blum-Micali Generator," J. Sains Komput. Inform. (J-SAKTI, vol. 6, no. 1, pp. 136–147, 2022.

S. P. Ananda and S. Lukman, "Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital," J. Ilm. Komputasi, vol. 21, no. 3, pp. 333–344, 2022, doi: 10.32409/jikstik.21.3.2973.

T. S. Permana, C. A. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and E. R. Subhiyakto, "Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher," Techno.Com, vol. 16, no. 4, pp. 337–347, 2017, doi: 10.33633/tc.v16i4.1267.

V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," J. Educ., vol. 5, no. 3, pp. 8563–8573, 2023, doi: 10.31004/joe.v5i3.1647.

Y. C. Milian and W. Sulistyo, "Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher," J. JTIK (Jurnal Teknol. Inf. dan Komunikasi), vol. 7, no. 2, pp. 208–216, 2023, doi: 10.35870/jtik.v7i2.716.