Versi Online:
https://journal.ubm.ac.id/index.php/alu
DOI: http://dx.doi.org/10.30813/j-alu.v2i2. 3526

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 2) : 489 - 494. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

PERANCANGAN TOOLS KRIPTOGRAFI BERBASIS WEB MENGGUNAKAN ALGORITMA CAESAR, VIGENERE DAN STEGANOGRAFI EOF

[Design of Web-based Cryptogrphy Tools Using Caesar, Vigenere, and EOF Steganography Algorithm]

Jaeson Octavianus, s32180119@student.ubm.ac.id[1)], Lukman Hakim, lhakim2710@gmail.com[2)]
[1), 2)] Program Studi Informatika/Fakultas Teknologi dan Desain, Universitas Bunda Mulia

ABSTRACT

Cryptography is a science or art that is useful for maintaining the confidentiality of letters by converting messages into forms that are no longer understood (Simargolang, 2017). Many students feel that the dissemination of cryptographic information that is disseminated is still ineffective, because there are still many students who do not really understand cryptography so they have to surf the internet, read books, etc. to find additional information. The purpose of this research is to create applications that are effective and can be a medium for disseminating information for students about cryptography to develop their level of knowledge of cryptography and to disseminate additional information about cryptography through cryptography educational applications. The data collection technique used in this research is by conducting a literature study and collecting primary data. The data used is obtained from conducting a survey using google form and is used to determine decisions in making the "EduKripto" application. With the high level of student desire to learn cryptography, 41.2% enthusiasts and 11.8% tentative, it can be concluded that this application can help students learn cryptography coupled with the application accuracy level in running algorithms and getting the right output is 100% during trials on the "EduKripto" application, as well as the data obtained indicate that after using "EduKripto" the level of understanding of students with less understanding changed from 77.7% to 38.9% and the level of understanding of students with more than average understanding increased from 22.3% to 61.2%, so it can be concluded that the use of the "EduKripto" application can help in developing the level of understanding of cryptography.
Keywords: *Applications, Cryptography, Educational. EduKripto, Effective,*

ABSTRAK

Kriptografi merupakan ilmu atau seni yang berguna untuk menjaga kerahasiaan surat dengan cara mengubah pesan menjadi bentuk yang tidak dipahami lagi (Simargolang, 2017). Banyak pelajar merasakan bahwa penyebaran informasi kriptografi yang disebarkan masih kurang efektif, dikarenakan masih banyaknya siswa yang tidak terlalu memahami kriptografi sehingga harus menjelajah internet, membaca buku, dll untuk mencari informasi tambahan. Tujuan dari penelitian ini adalah untuk membuat aplikasi yang bersifat efektif dan dapat menjadi media penyebaran informasi bagi mahasiswa mengenai kriptografi untuk mengembangkan tingkat pengetahuan kriptografi serta menyebarkan informasi tambahan mengenai kriptografi melalui aplikasi edukasi kriptografi. Teknik pengumpulan data yang dilakukan dalam penelitian ini yaitu dengan melakukan studi literatur dan pengumpulan data primer, Data yang digunakan didapat dari melakukan survey dengan menggunakan google form dan digunakan untuk menentukan keputusan dalam membuat aplikasi “EduKripto”. Dengan tingginya tingkat keinginan siswa untuk mempelajari kriptografi, sebesar 41.2% peminat dan 11.8% tentatif , dapat disimpulkan bahwa aplikasi ini dapat membantu siswa dalam mempelajari kriptografi ditambah dengan tingkat akurasi aplikasi dalam menjalankan algoritma dan mendapatkan output yang tepat adalah 100% selama dilakukan uji coba pada aplikasi “EduKripto”, serta data yang didapat mengindikasikan bahwa setelah menggunakan “EduKripto” tingkat pemahaman mahasiswa dengan pemahaman kurang berubah dari 77,7% menjadi 38,9% dan tingkat pemahaman mahasiswa dengan pemahaman lebih dari rata-rata

meningkat dari 22,3% menjadi 61,2%, sehingga dapat disimpulkan bahwa penggunaan aplikasi "EduKripto" dapat membantu dalam pengembangan tingkat pemahaman kriptografi.
Kata Kunci: Aplikasi, Edukasi, EduKripto, Efektif, Kriptografi

PENDAHULUAN

Kriptografi merupakan ilmu atau seni yang berguna untuk menjaga kerahasiaan surat dengan cara mengubah pesan menjadi bentuk yang tidak dipahami lagi (Simargolang, 2017). Kriptografi juga dapat didefinisikan sebagai ilmu menutup/merekonstruksi pesan asli menjadi pesan yang tidak dapat dikenali atau tidak dapat dipahami (Limbong, 2015). Kriptografi merupakan salah satu mata pelajaran yang dipelajari oleh mahasiswa di perguruan tinggi. Banyak hal yang bisa disampaikan dalam mata kuliah kriptografi, karena biasanya dalam rapat-rapat kuliah kita membahas tata cara penerapan metode kriptografi. Ada banyak metode dan algoritma kriptografi berbeda yang terkait dengan metode kriptografi.[1]

Banyak pelajar merasakan bahwa penyebaran informasi kriptografi yang disebarkan masih kurang efektif, dikarenakan masih banyaknya siswa yang tidak terlalu memahami kriptografi sehingga harus menjelajah internet, membaca buku, dll untuk mencari informasi tambahan dikarenakan kekurangpahaman siswa dengan penjelasan yang diberikan dan rasa ingin tahu mengenai informasi tersebut. Berdasarkan penelitian terdahulu, tingkat motivasi siswa untuk melakukan pembelajaran diluar pendidikan formal dengan intensitas yang tinggi adalah sebesar 66,7%.[2]

Waktu pembelajaran dan kurang efisiennya tingkat pembelajaran secara formal, serta ide untuk menggabungkan edukasi dan efektivitas sebagai media pembelajaran kriptografi menjadi alasan utama penulis untuk membuat aplikasi *website*, ***"EduKripto"***, Aplikasi berbasis *web* yang merupakan media interaktif untuk pembelajaran kriptografi dasar.

Berdasarkan masalah tersebut, penelitian ini dapat diarahkan dengan beberapa pertanyaan:

1. Apakah dengan menggunakan aplikasi edukasi *"EduKripto"*, dapat meningkatkan pemahaman mahasiswa dalam kriptografi?
2. Bagaimana dengan tingkat akurasi penerapan algoritma kriptografi yang nantinya akan digunakan dalam kegiatan pembelajaran?
3. Lalu apakah tingkat pemahaman mahasiswa yang menggunakan aplikasi edukasi, *"EduKripto"* meningkat dengan signifikan?

Tujuan dan Manfaat dari penelitian ini dapat dijabarkan dengan seperti berikut:

1. Membuat aplikasi yang bersifat efektif dan dapat menjadi media penyebaran informasi bagi mahasiswa mengenai kriptografi untuk mengembangkan tingkat pengetahuan kriptografi.
2. Menyebarkan informasi tambahan mengenai kriptografi melalui aplikasi edukasi kriptografi.
3. Dengan dikembangkannya aplikasi edukasi kriptografi ini dapat membuktikan teori bahwa belajar dengan menggunakan aplikasi dapat memberikan suasana belajar yang unik serta dapat meningkatkan wawasan para mahasiswa dengan informasi yang disediakan.
4. Aplikasi dibuat untuk memberikan informasi mengenai kriptografi bagi mahasiswa dalam bentuk aplikasi yang bersifat unik dan efektif.

Metode Penyampaian Informasi merupakan sebuah faktor penting dalam proses memahami. Penyampaian informasi

yang tepat dapat menarik perhatian dari para pendengar, dengan menggunakan media interaktif, mahasiswa dapat mengurangi rasa bosan ketika mempelajari informasi-informasi yang ada.[3] Menurut penelitian terdahulu mengenai tingkat efektifitas pembelajaran menggunakan media interaktif, tingkat efektifitas media pembelajaran interaktif adalah 63,44%.[4]

Dalam pengembangannya, aplikasi edukasi *"EduKripto"* menggunakan 3 algoritma kriptografi, yaitu algoritma kriptografi *caesar cipher, vigenere cipher* dan *steganografi* metode *EOF*.

TINJAUAN PUSTAKA

Caesar Cipher

Dalam kriptografi, Caesar cipher adalah salah satu teknik kriptografi yang paling sederhana dan paling terkenal. Sandi yang terdiri dari sandi alternatif dimana setiap huruf dalam teks biasa diganti dengan huruf lain yang posisinya berbeda dalam huruf alfabet. Misalnya, jika menggunakan pergeseran 3 huruf, B akan menjadi E, U akan menjadi X dan K akan menjadi N sehingga plaintext dari "BOOK" akan menjadi "EXNX" dalam teks terenkripsi.[5]

Vigenere Cipher

Jenis sandi polifabetik yang menarik ini ditemukan oleh Blaise de Vigenère, seorang matematikawan Prancis abad keenam belas. Ini dikenal sebagai sandi Vigenere. Ini telah menjadi salah satu sandi paling populer di masa lalu karena kesederhanaan dan ketahanannya terhadap tes analisis frekuensi huruf yang dapat memecahkan sandi sederhana seperti sandi Caesar.

Dalam sandi Vigenere, tabel alfabet dapat digunakan untuk enkripsi dan dekripsi, yang disebut tabel lurus, kisi Vigenre, atau tabel Vigenre. Ini terdiri dari alfabet yang ditulis 26 kali pada baris yang berbeda, setiap alfabet secara siklis bergeser ke kiri alfabet sebelumnya, sesuai dengan 26 kemungkinan sandi Caesar, yang dikenal sebagai sandi pelengkap. Setiap cipher diidentifikasi dengan huruf kunci, yaitu huruf ciphertext yang menggantikan huruf plaintext. Masing-masing dari 26 digit disajikan secara horizontal, dengan huruf kunci untuk setiap digit.[6]

Steganografi & Metode EOF

Steganografi berasal dari bahasa Yunani *steganos*, yang berarti "tersembunyi atau terselubung," dan *graphein*, "untuk menulis." Dengan demikian, steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan berbagai cara. Steganografi membutuhkan penyembunyian dua properti, yaitu *container* dan data rahasia. Lanskap digital adalah media digital sebagai wadah, seperti gambar, *audio*, teks, dan *video*. Data sensitif yang tersembunyi juga dapat berupa gambar, *audio*, teks, atau *video*.[7]

Metode *End Of File* (EOF) adalah metode yang dapat digunakan untuk menyisipkan *file* di akhir *file* agar wadah penyimpanan atau gambar tidak berubah secara kasat mata saat metode ini menyisipkan atau menyisipkan bagian akhir file. *file* yang digunakan, gambar yang terlihat akan diperbesar secara bertahap, sehingga mungkin mencurigakan.[8][9]

METODE PENELITIAN

Studi Pustaka

Tahapan penelitian studi pustaka dilaksanakan dengan menghimpun sumber kepustakaan, baik primer juga sekunder. Penelitian ini melakukan klasifikasi data sesuai formula penelitian. Pada tahap lanjut dilakukan pengolahan data serta atau pengutipan surat keterangan buat ditampilkan sebagai temuan penelitian, diabstraksikan buat mendaptakan gosip yg utuh, dan dinterpretasi sampai membuat

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 2) : 489 - 494. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

pengetahuan buat penarikan konklusi. Aadapun pada termin interpretasi dipergunakan analisis atau pendekatan, contohnya, filosofis, teologis, sufistik, tafsir, syarah, serta lain-lain.[10]

Pengumpulan Data Primer

Data Primer (primary data) yaitu data yang dikumpulkan sendiri oleh perorangan/ suatu organisasi secara langsung dari objek yang diteliti dan untuk kepentingan studi yang bersangkutan yang dapat berupa interviu, observasi.[11]

HASIL DAN PEMBAHASAN

Hasil

Pengumpulan data menggunakan data *primer*, yang merupakan data yang didapatkan dari kuisioner menggunakan *google form* sebagai medi untuk mengumpulkan data yang digunakan. Kuisioner pertama mendapatkan *total* 51 responden dengan hasil data *primer* sebagai berikut:

Tabel 1 Data Mahasiswa yang Mengetahui Kriptografi

Pilihan	Ya	Tidak	Mungkin
Responden	16	30	5

Dari tabel diatas, terdapat 16 mahasiswa yang mengetahui kriptografi, dan 35 mahasiswa yang tidak benar-benar mengetahui kriptografi.

Data selanjutnya adalah data mengenai tingkat keinginan mahasiswa yang tidak mengetahui kriptografi untuk mempelajari kriptografi setelah diberikan penjelasan secara singkat, *total* mahasiswa yang setuju mengikuti kuisioner ini adalah 34 orang.

Tabel 2 Data Mahasiswa yang Ingin Belajar Kriptografi Tanpa Pengetahuan Dasar

Pilihan	Ya	Tidak	Mungkin
Responden	14	16	4

Dari data diatas, terhitung sebanyak 18 orang memiliki niat untuk mempelajari kriptogarfi, dan 16 orang tidak berniat untuk mempelajari kriptografi,

Data selanjutnya merupakan data dari tingkat pemahaman mahasiswa yang mempelajari kriptografi, yang berjumlah 16 orang.

Tabel 3 Data Tingkat Pemahaman Mahasiswa Terhadap Kriptografi

Tingkat Pemahaman	Total Responden
1	2
2	4
3	5
4	4
5	1

Dari data yang dikumpulkan, dapat dihitung terdapat 11 mahasiswa yang pengetahuannya masih rata-rata dan dibawahnya, dan terdapat 5 mahasiswa yang tingkat pemahaman mengenai kriptografinya diatas rata-rata.

Data selanjutnya adalah data yang didapatkan dari melakukan uji coba terhadap aplikasi untuk mengetes tingkat akurasi dari algoritma kriptografi yang diterapkan dalam aplikasi “EduKripto”

Tabel 4 Pengujian Akurasi Algoritma Kriptografi Aplikasi EduKripto

Algoritma Kriptografi	Jumlah Uji Coba	Uji Berhasil	Uji Gagal
Caesar	50	50	0
Vigenere	50	50	0
Steganografi	50	50	0

Dari tabel diatas, tingkat akurasi dari algoritma kriptografi *caesar cipher, vigenere cipher* dan *steganografi* metode *eof,* adalah 100%.

Data selanjutnya adalah data yang didapat dari mahasiswa yang telah menggunakan aplikasi EduKripto. Data berikut menghitung mahasiswa yang bersedia dan ingin meningkatkan pemahamannya mengenai kriptografi dan bersedia untuk melakukan uji coba aplikasi *“EduKripto”.*

Tabel 5 Tingkat Pemahaman Kriptografi Mahasiswa Sebelum Menggunakan EduKripto

Tingkat Pemahaman	Algoritma Kriptografi
1	8
2	3
3	3
4	3
5	1

Berikut data mengenai tingkat pemahaman mahasiswa-mahasiswi tersebut setelah menggunakan "EduKripto".

Tabel 6 Tingkat Pemahaman Kriptografi Mahasiswa Setelah Menggunakan EduKripto

Tingkat Pemahaman	Algoritma Kriptografi
1	0
2	3
3	4
4	10
5	1

Dari data tabel diatas, terlihat terjadi peningkatan pada pemahaman kriptografi mahasiwa dan mahasiswi yang menggunakan *"EduKripto"*.

Pembahasan

Dari data-data yang sudah dikumpulkan sebelumnya, dapat dilihat bahwa semua rumusan masalah yang ditemukan dapat terselesaikan. Mulai dari tingkat keinginan untuk mempelajari kriptografi dengan aplikasi edukasi kriptografi berbasis *web*, Tingkat akurasi penerapan algoritma kriptografi dan tingkat peningkatan pemahaman mengenai kriptografi.

SIMPULAN

Kesimpulan yang didapat dari dijalankannya penelitian ini: Dengan tingginya tingkat keinginan siswa untuk mempelajari kriptografi, sebesar 41.2% peminat dan 11.8% tentatif , dapat disimpulkan bahwa aplikasi ini dapat membantu siswa dalam mempelajari kriptografi, tingkat akurasi aplikasi dalam menjalankan algoritma dan mendapatkan output yang tepat adalah 100% selama dilakukan uji coba pada aplikasi "EduKripto" dan setelah menggunakan "EduKripto" tingkat pemahaman mahasiswa dengan pemahaman kurang berubah dari 77,7% menjadi 38,9% dan tingkat pemahaman mahasiswa dengan pemahaman lebih dari rata-rata meningkat dari 22,3% menjadi 61,2%.

Data-data akhir yang digunakan merupakan data-data yang didapat dari campuran mahasiswa yang mengetahui kriptografi dan tidak mengetahuinya sama sekali, sehingga dapat disimpulkan bahwa peningkatan pemahaman kriptografi bagi mahasiswa secara acak memiliki tingkat yang jauh lebih tinggi daripada sebelum menggunakan aplikasi *"EduKripto"*, sehingga jika dapat di-aplikasikan kepada mahasiswa dalam kegiatan belajar mengajar dan sekaligus diberikan penerapan konsep oleh dosen, maka peningkatan pemahaman mahasiswa bisa jauh lebih besar daripada data yang dimiliki sekarang.

DAFTAR PUSTAKA

[1] H. Hendy and H. Akbar, "Pengembangan Aplikasi Android Belajar Kriptografi Sebagai Media Pembelajaran Mata Kuliah Kriptografi," J. Inform., vol. 8, no. 1, pp. 17–25, 2021, doi: 10.31294/ji.v8i1.9420.

[2] E. Khoerunnisa and G. A. Grafiyana, "Motivasi Siswa Mengikuti Bimbingan Belajar," Psisula Pros. Berk. Psikol., vol. 1, no. April, 2020, doi: 10.30659/psisula.v1i0.7687.

[3] B. O. Samekto, "Rancang Bangun Game Edumatika Berbasis

Android," J. Ilm. Teknol. Inf. Asia, vol. 14, no. 1, 2020, doi: 10.32815/jitika.v14i1.402.

[4] U. N. Medan, U. Haji, and S. Utara, "= 2,01, t," vol. 9, no. 1, pp. 1–8, 2022.

[5] F. I. Lubis, H. F. S. Simbolon, T. P. Batubara, and R. W. Sembiring, "Combination of caesar cipher modification with transposition cipher," Adv. Sci. Technol. Eng. Syst., vol. 2, no. 5, pp. 22–25, 2017, doi: 10.25046/aj020504.

[6] T. M. Aung, H. H. Naing, and N. N. Hla, "A complex transformation of monoalphabetic cipher to polyalphabetic cipher: (Vigenère-Affine Cipher)," Int. J. Mach. Learn. Comput., vol. 9, no. 3, pp. 296–303, 2019, doi: 10.18178/ijmlc.2019.9.3.801.

[7] J. Rosmiyati and T. M. S. Mulyana, "Watermark Dengan Gabungan Steganografi Dan Visible Watermarking," J. Algoritm. Log. dan Komputasi, vol. 1, no. 1, pp. 36–43, 2018, doi: 10.30813/j-alu.v1i1.1109.

[8] B. V. Indriyono, "Implementasi Sistem Keamanan File dengan Metode Steganografi EOF dan Enkripsi Caesar Cipher," Sisfo, vol. 06, no. 01, pp. 1–16, 2016, doi: 10.24089/j.sisfo.2016.09.001.

[9] Hermansa, R. Umar, and A. Yudhana, "Pangamanan Pesan Menggunakan Kriptografi," J. Sains Komput. Mat. , vol. Vol 4, pp. 1–13, 2020.

[10] W. Darmalaksana, "Metode Penelitian Kualitatif Studi Pustaka dan Studi Lapangan," Pre-print Digit. Libr. UIN Sunan Gunung Djati Bandung, pp. 1–6, 2020.

[11] [11] S. Helmi, Analisis data, no. July. 2021.