https://tunasbangsa.ac.id/abdimas

Pelatihan Teknik Caesar Cipher Terhadap Keamanan Informasi

Caesar Chiper Technique Training on Information Security

Asbon Hendra Azhar[1*]

Ratih Adinda Destari[2]

Wahyu Sapta Negoro[3]

Ardansyah [4]

[1,2]Universitas Potensi Utama, Medan, Sumatera Utara, Indonesia.

*email: asbon.upu@gmail .com

Abstrak

Konsep kriptografi telah digunakan sejak zaman dahulu oleh Julius Caesar dan terus berkembang sampai saat ini. Berdasarkan era-nya kriptografi terbagi menjadi dua bagian, yaitu kriptografi klasik dan kriptografi modern. Persamaan dari keduanya adalah sama-sama menggunakan konsep matematika dalam teknik pembuatan dan pemecahan suatu pesan. Tetapi dalam kriptografi klasik, konsep matematika yang dipakai masih sangat sederhana, seperti substitusi, permutasi dan transpos. Sedangkan dalam kriptografi modern konsep matematika yang digunakan sudah tidak sederhana lagi, seperti polinom, bilangan prima, grup, ring dan lapangan. Kelebihan dari kriptografi klasik adalah kemudahannya dalam mengenkripsi pesan, tetapi beberapa teknik pengenkripsiannya juga memiliki kelemahan yang cukup fatal yaitu sangat mudah untuk dipecahkan. Contoh kriptografi klasik yang sangat mudah dibuat dan dipecahkan adalah Caesar Cipher yang hanya memiliki kunci yang mungkin sebanyak 26 buah. Caesar Cipher termasuk kedalam enkripsi Substitution Cipher, dimana kode atau naskah acak didapatkan dengan mengganti setiap karakter pada naskash asli.

Kata Kunci:
Caesar Cipher
Pelatihan
Keamanan Nasional

Keywords:
Caesar Cipher
Training
National Security

Abstract

The concept of cryptography has been used since ancient times by Julius Caesar and continues to develop today. Based on the era, cryptography is divided into two parts, namely classical cryptography and modern cryptography. The similarity between the two is that they both use mathematical concepts in the technique of creating and breaking a message. But in classical cryptography, the mathematical concepts used are still very simple, such as substitution, permutation and transpose. Meanwhile, in modern cryptography the mathematical concepts used are no longer simple, such as polynomials, prime numbers, groups, rings and fields. The advantage of classical cryptography is that it is easy to encrypt messages, but some encryption techniques also have a fatal weakness, namely that they are very easy to crack. An example of classic cryptography that is very easy to create and solve is the Caesar Cipher which only has 26 possible keys. Caesar Cipher is included in the Substitution Cipher encryption, where a random code or script is obtained by replacing each character in the original text..

 DOI: http://dx.doi.org/10.30645/.v1i1.

PENDAHULUAN

Caesar Cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Caesar chiper pertama kali digunakan oleh Julius Caesar. Caesar mengkodekan informasi dengan menggubah setiap huruf dalam informasi menjadi tiga huruf di setelah informasi asli dalam urutan alfabet. Caesar Cipher termasuk kedalam enkripsi Substitution Cipher, dimana kode atau naskah acak didapatkan dengan mengganti setiap karakter pada naskash asli. Salah satu teknik enkripsi sederhana yang masih digunakan hingga hari ini adalah algoritma Caesar Cipher, yang dibuat oleh Julius Caesar pada era Romawi kuno. Prinsip dasar algoritma ini adalah mengubah setiap huruf dalam pesan dalam urutan alfabet sebanyak langkah tertentu.Caesar Cipher merupakan salah satu jenis cipher substitusi yang

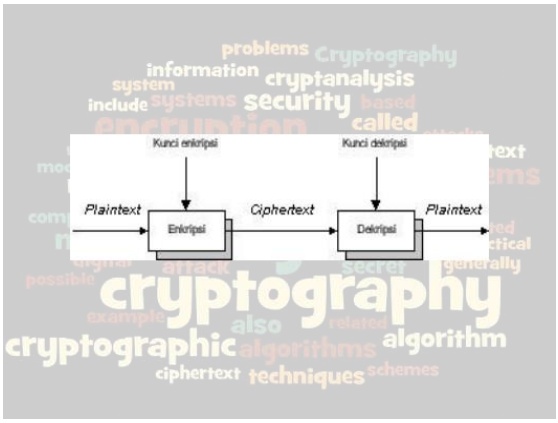
membentuk cipher dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya.Seiring berkembangnya teknologi dan kebutuhan manusia yang semakin meningkat dapat dimanfaatkan untuk menciptakan suatu keamanan. Salah satu contohnya adalah keamanan pesan dalam berkomunikasi, keamaan merupakan hal yang diinginkan semua orang untuk menjaga privasi. Agar pesan yang dikirim 2 aman dari orang yang tidak bertanggung jawab, maka pesan tersebut disembunyikan menggunakan algoritma kriptografi (Ariyus, 2008). Kriptografi dibagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Di dalam kriptografi ada beberapa teknik dalam menyandikan pesan yaitu: teknik substitusi, teknik permutasi, teknik blocking, teknik ekspansi, dan teknik perampatan. Dengan beberapa teknik ini dapat dilakukan beberapa proses penyandian untuk merahasiakan sebuah pesan. Dalam pesan rahasia, kriptografi lebih mengarah ke pesan yang dienkripsi sementara steganografi lebih mengarah pada pesan tersembunyi. Namun, kedua metode tersebut memiliki tujuan yang sama, yaitu upaya untuk menyembunyikan pesan. Di sisi lain, ternyata penggunaan kriptografi seringkali dapat diselesaikan atau diterjemahkan oleh orang lain atau kriptoanalis. Hal ini dimungkinkan karena biasanya pesan teks yang tidak dapat dibaca memberikan kecurigaan seseorang bahwa pesan teks tersebut mengandung arti tertentu bagi pemilik pesan. Seiring berkembangnya teknologi dan ilmu pengetahuan, maka ancaman penyerangan atau pemecahan terhadap sandi kriptografi juga semakin berkembang. Caesar cipher sebagai salah satu jenis kriptografi klasik tentunya mengalami ancaman yang sama. Dengan teknik penyandian yang digunakan dalam Caesar cipher masih bersifat sederhana yakni menggunakan teknik substitusi dan transposisi, maka hasil penyandian tersebut akan mudah mengalami ancaman pemecahan atau penyerangan. Sehingga atas dasar tersebut maka diperlukan modifikasi terhadap teknik penyandian Caesar cipher agar tidak mudah terpecahkan oleh kriptanalis. Proses modifikasi yang dapat digunakan dalam penyandian ini sangat beragam sebagaimana telah disebutkan sebelumnya, yakni 3 dapat menggunakan teknik substitusi, permutasi, blocking, ekspansi, dan teknik perampatan.

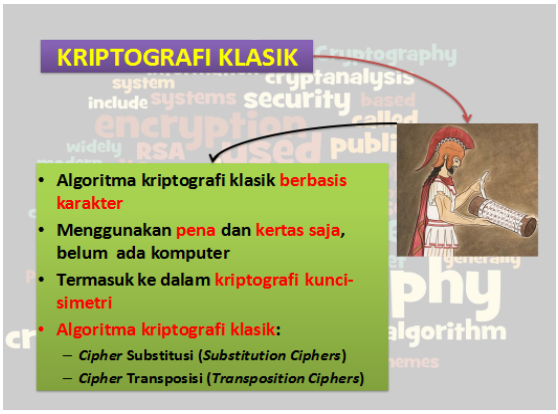
METODE

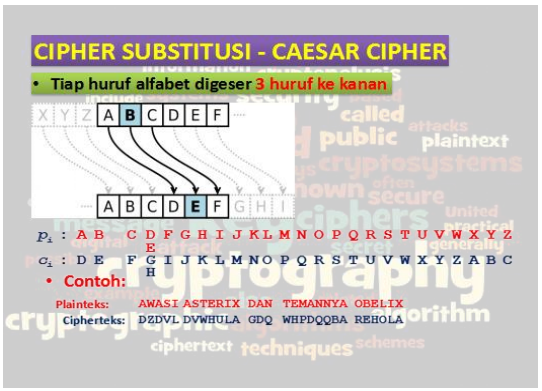
Adapun persiapan dan metode dalam kegiatan kepada masyarakat sebelum kegiatan dilaksanakan maka dilakukan persiapan sebagai berikut:

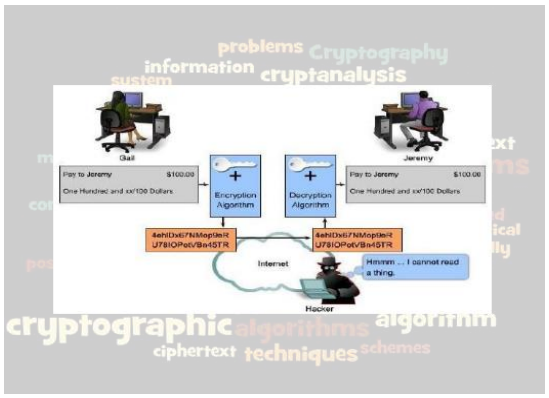
a) Melakukan studi pustaka tentang Caesar Cipher.
b) Melakukan persiapan alat dan bahan untuk pembuatan Caesar Cipher.
c) Menentukan waktu pelaksanaan dan lamanya kegiatan pengabdian bersama-sama tim pelaksana.
d) Menentukan dan mempersiapkan materi yang akan disampaikan dalam kegaitan pengabdian masyarakat.
e) Dalam Pelaksanaan Pelatihan ini tim pelaksana akan mengumpulkan para siswa sekolah tersebut dimana akan dilakukan dulu perkenalan baik dari tim pelaksana maupun siswa sekolah tersebut. Setelah itu pelatihan akan dimulai dengan memberikan penjelasan apa yang itu Caesar cipher dan kegunaannya apa –apa saja baik bagi siswa saat proses belajar mengajar maupun diluar proses belajar mengajar. Tim Pelaksana selanjutnya memberikan materi tentang bagaimana Penggunaan Caesar Cipher yang mana akan diberikan juga contoh pembuatannya kepada siswa tersebut sehingga menghasilkan hasil yang baik dan bagus:

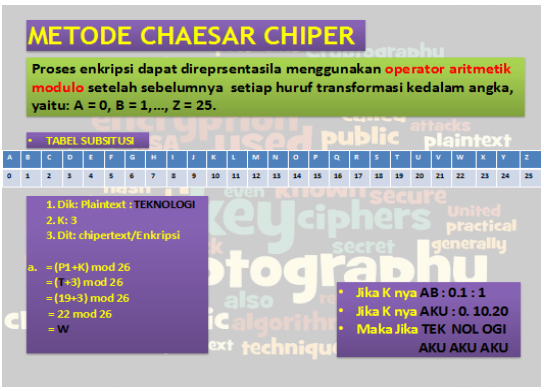
HASIL DAN PEMBAHASAN

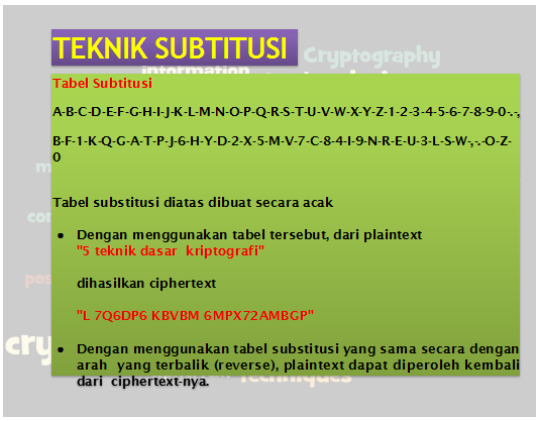


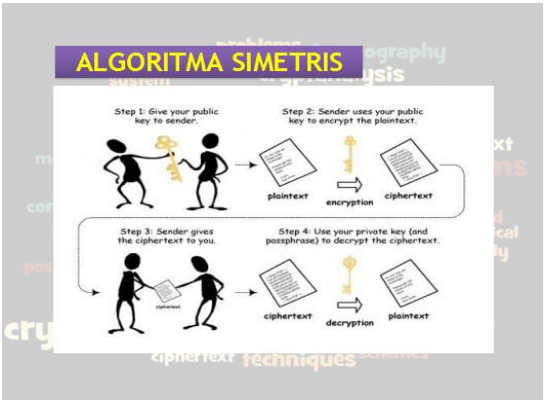


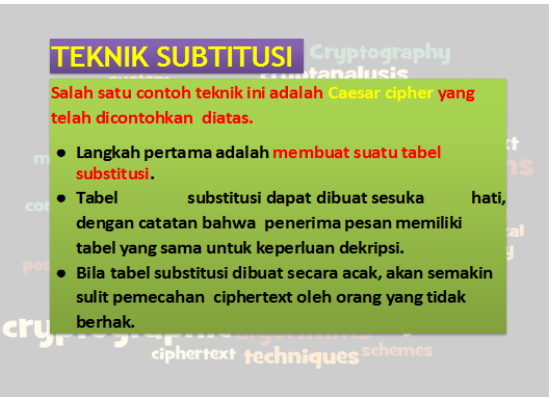












Gambar 1. Materi

Hasil yang didapat dalam Pengabdian Masyarakat ini adalah:

a) Meningkatnya pengetahuan dan pemahaman siswa dalam Caesar Cipher

b) Meningkatkan keterampilan siswa dalam penggunaan Caesar Cipher.

Gambar 2. Pelatihan Teknik Caesar Chiper Terhadap Keamanan Informasi di SMK Tritech Indonesia

SIMPULAN

Pelatihan yang telah di analisis maka dapat hasil yang dapat disimpulkan bahwa minat, semangat serta keingintahuan para Siswa/i peserta Pelatihan Caesar Cipher begitu tinggi setelah terlaksananya Pelatihan ini. Dengan Pelatihan ini dapat meningkatkan motivasi para Siswa/i dalam meningkatkan minat belajar untuk Mengenal Caesar Cipher sebagai materi belajar bagi Siswa/i tersebut. Pengetahuan dan pemahaman Siswa/i dalam Caesar Cipher menjadi meningkat..

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama dan SMK Tritech Indonesia yang telah membantu penulis dalam penelitian ini.

REFERENSI

Faisal, 2014, Penerapan Kombinasi Sandi Caesar Dan Vigenere Untuk Pengamanan Data Pesan Pada Surat Elektronik, Jakarta.

Rachmawati, Dian dan Candra, Ade., 2015, Implementasi Kombinasi Caesar dan Affine Cipher untuk keamanan Data Teks, Jurnal Edukasi dan Penelitian Informatika (JEPIN), Nomor 2, Volume(1):60-63.

Basuki, A., Paranita, U., & Hidayat, R. 2016. Perancangan Aplikasi Kriptografi Berlapis menggunakan Algoritma Caesar, Transposisi, Vigenere, dan Blok Chiper Berbasis Mobile. Seminar Nasional Teknologi Informasi Dan Multimedia 2016, 1(2), 31–35.

Gurning, R. R. A. (2014). Perancangan aplikasi pengamanan pesan dengan algoritma caesar chiper. Pelita Informatika Budi Darma, VI(April), 106–110.

R. Febrianingsih and A. Hafiz, 2019 Implementasi Kriptografi Berbasis Caesar Chiper Untuk Keamanan Data," J. Inf. Dan Komput., vol. 7, no. 2, pp. 81–86.