JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

E-LEARNING DALAM PENGEMBANGAN PEMBELAJARAN KRIPTOGRAFI

M. Syaifuddin[1*], Juniar Hutagalung[2] , Ganefri[3]
[1,2]Sistem Informasi, STMIK Triguna Dharma
[3]Fakultas Teknik, Universitas Negeri Padang
email: [*]msyaifuddins@gmail.com

Abstract: Cryptography is an important subject to study because it contains data security. In this course, there are algorithms where each algorithm has a different level of calculation process from one another. Testing has been done several times in the form of training on students and some of them still make mistakes in getting the results of the encryption and decryption process. These errors are caused by a lack of understanding of algorithms and calculations in cryptography. In cryptography, the accuracy of the calculation results is a top priority, because if one does the calculation which is called the encryption and decryption process it will result in an incorrect message/information. To anticipate these errors, this cryptography learning is assisted by a tool called crypTool. This tool is a companion in carrying out the encryption and decryption process to avoid errors in the calculation process.

Keywords: Cryptography; E-Learning

Abstrak: Kriptografi merupakan salah satu matakuliah yang penting untuk dipelajari, karena didalamnya memuat materi pengamanan data. Dalam matakuliah tersebut terdapat algoritma-algoritma dimana setiap algortima memiliki tingkat proses perhitungan yang berbeda satu dengan yang lainnya. Telah dilakukan beberapa kali pengujian dalam bentuk latihan terhadap mahasiswa dan dari sebagian dari mereka masih melakukan kesalahan dalam mendapatkan hasil proses enkripsi dan dekripsi. Kesalahan tersebut diakibatkan oleh kuranganya memahami algoritma dan perhitungan dalam kriptografi. Dalam kriptografi keakuratan hasil perhitungan menjadi prioritas utama, karena apabila salah dalam melakukan perhitungan yang disebut dengan proses enkripsi dan dekripsi maka akan menghasilkan sebuah pesan/informasi yang salah. Guna mengantisipasi kesalahan tersebut maka pembelajaran kriptografi ini dibantu dengan sebuah tools yang bernama cryptool. Tool ini bersifat pendamping dalam melakukan proses enkripsi dan dekripsi dengan maksud menghindari kesalahan didalam melakukan proses perhitungannya.

Kata kunci: E-Learning; Kriptografi

PENDAHULUAN

Saat ini begitu murah dan mudahnya mengakses sebuah informasi, hal ini menuntun sebuah perubahan arah pembelajaran.[1] Pada awalnya, pembelajaran hanya berpusat pada dosen/guru atau disebut pembelajaran satu arah (*teacher learnig center*)[2] [3]. Namun karena mudah dan berkembangan sebuah teknologi dan informasi mengakibatkan arah transfer ilmu pengetahuan ini berubah, yang awalnya berpusat pada guru/dosen maka pembelaja-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

ran abad 21 berubah menjadi *student center learning*[4][5]. Pembelajaran abad ke 21 pembelajaran yang bercirikan *learning skill, skill*, dan *literasi*. *Learning skill* yaitu kegiatan pembelajaran yang di dalamnya ditandai dengan adanya kerja sama, komunikasi, serta berpikir kritis dan kreatif [6] [7]

Pembelajaran (*instruction*) bermakna sebagai upaya untuk membelajarkan seseorang atau kelompok orang melalui berbagai upaya (*effort*) dan berbagai strategi, metode dan pendekatan ke arah pencapaian tujuan yang telah direncanakan[8]. Pembelajaran bertujuan membantu peserta didik memperoleh pengetahuan. Dengan pengetahuan yang didapat selama belajar akan menjadi bekal dalam menjalani kehidupannya dimasa kini dan yang akan datang [9]. Dalam proses pembelajaran terdapat beberapa komponen yang dapat mempengaruhi keberhasilan pembelajaran. Komponen yang dimaksud adalah (1) peserta didik, (2) guru ataupun pemandu berjalannya pembelajaran, (3) serta materi pembelajaran [10].

Untuk mengoptimalkan pembelajaran, diperlukan sebuah media pembelajaran yang baik dan relevan, karena media pembelajaran salah satu unsur yang mempengaruhi kualitas pelaksanaan pendidikan. Media pembelajaran sarana yang dapat membantu proses belajar mengajar dan berfungsi untuk memperjelas makna pesan yang disampaikan, sehingga dapat mencapai tujuan pembelajaran dengan lebih baik dan sempurna [11]. Dengan diperbantukan media pembelajaran, bahan-bahan pembelajaran mudah diakses sehingga memungkinkan peserta melakukan pembelajaran berulang kali agar peserta lebih mudah memahami materi tersebut.

Media pembelajaran yang disajikan dalam pembelajaran menjadi *suplemen* (tambahan) terhadap sebuah materi yang disampaikan dikelas[12][13] Dengan *tools* yang digunakan dalam media pembelajaran pembelajaran kriptografi, pembelajaran ini akan terasa lebih mudah. Karena *tools* ini memiliki fitur yang *user freindly* untuk digunakan, mulai dari proses pengisian plainteks, hingga proses selanjutknya, yakni proses enkripsi dan dekripsi.

Kriptografi salah satu caabang ilmu yang mempelajari bagaimana menjaga keamananan suatu pesan (*plaintext*) [14]. Dalam kajian ilmu kriptografi, terdapat dua proses yang sangat penting, proses tersebut adalah enkripsi dan dekripsi. Enkripsi secara sederhana bermakna mengubah pesan jelas (*clear text*) menjadi pesan acak yang tidak bermakna (*cipher text*) [15]. Sementara dekripsi merupakan mengembalikan pesan tidak bermakna (*cipher text*) menjadi pesan jelas (*plaintext*) [16]. Bidang ilmu ini digunakan untuk menyampaikan pesan kepada pihak lain melalui sebuah media, dengan harapan pesan yang disampaikan terjaga kerahasiannya.

Keakuratan dalam proses enkripsi dan dekripsi hal yang utama dalam bidang kriptografi. Jika terjadi kesalahan dalam proses enkripsi, maka akan menghasilkan pesan yang salah pula. Jika terjadi kesalahan dari hasil enkripsi maka hasil dekripsi juga akan terjadi kesalahan.

Untuk meminimalisir kesalahan dalam melakukan proses enkripsi dan dekripsi, digunakan sebuah *tools* bantu bernama *CrypTools.* Dengan tools yang ditawarkan ini nantinya, para mahasiswa tidak lagi merasa kesulitan dalam mempelajari dan melakukan proses enkripsi-dekripsi, karena dengan bantuan *tools* ini kedua proses tersebut mudah dilakukan dan keakuratan hasilnya lebih handal jika dibandingkan dengan perhitungan manual.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

METODE

Mengamankan data/informasi merupakan salah satu capaian dalam ilmu kriptografi yang harus terselesaikan. Pada awalnya penggunaan kriptografi hanya sebagai ilmu yang mempelajari bagaimana mengamanan pesan/informasi dari pengirim ke penerima pesan. Namun saat ini, ilmu kriptografi tidak hanya sebatas mengamankan pesan saja, namun merambah kepada bagaimana menjaga keutuahan, otoritasasi data/validasi data.

Dalam mengamankan data/informasi, kriptografi memiliki 2 (dua) jenis metode, yakni metode klasik dan modern**.**[7] Kriptografi klasik merupakan pengamanan data yang dimana sistem operasinya menggunakan abjad alphabet (A s.d Z) yang berjumlah 26 huruf. Sedangkan kriptografi modern pengamanan data dengan sistem operasinya menggunakan bilangan biner.

Didalam kriptografi terdiri dari komponen yang disebut plainteks, cipherteks, kunci dan algoritma [15]. *Plaintext* (plainteks), yaitu informasi awal sebelum pesan dikirim, sehingga pesan ini masih dapat dibaca dan pahami maksud dan tujuannya;

1. *Ciphertext* (cipherteks), yaitu pesan tersandikan, dimana pesan ini tidak lagi dapat dipahami isi dan maksudnya;
2. Key (kunci), yaitu sebuah parameter untuk proses enkripsi dan dekripsi;
3. Algorithm (algoritma), yaitu cara yang digunakan untuk proses enkripsi dan dekripsi.

Istilah pemrosesan kriptografi disebut enkripsi dan dekripsi

1. *Encryption* (enkripsi) yaitu cara merubah pesan yang dapat dibaca (plainteks) menjadi pesan yang tidak dapat dibaca. Hasil dari proses ini disebut *ciphertext* (cipherteks)
2. *Decription* (dekripsi) yaitu proses mengembalikan pesan tidak bisa dibaca (*ciphtertext*) menjadi bisa terbaca (*plaintext*).

Ada beberapa teknik dalam mengamankan data menggunakan metode klasik, teknik itu diataranya adalah:

1. *Substitution* (subtitusi) yaitu teknik pengamanan pesan dengan cara mengganti deretan huruf ataupun angka lama menjadi sebuah deretan baru yang tercak. Algoritma subtitusi ini contohnya adalah Caesar cipher, vigenere cipher;
2. *Transposition* (transposisi) yaitu teknik pengamanan data dengan cara memindahkan/menggeser deretan huruf atau angka plainteks keposisi yang lain.
3. Super encryption (super enkripsi) yaitu menggabungkan dua metode, yakni metode subtitusi dangan transposisi. Tujuan dari pengabungan ini adalah menyulitkan seorang *cryptanalyst t* dalam mendapatkan pesan yang terkandung didalamnya apabila tidak mendapatkan kunci.

Dikarenakan didalam kriptografi memiliki banyak algoritma, maka dalam penelitian ini algoritma yang digunakan hanyalah Caesar cipher dan vigenere cipher.

Algortima Caesar Cipher

Algoritma Caesar cipher tergolong pada kriptografi clasik yang menerapkan metode substitusi abjad-tunggal. [17]Maksud dari abjad tunggul tesebut adalah semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama. Algoritma ini menggunakan huruf alphabet yang berjumlah 26 karakter.

Persamaan yang bisa digunakan dalam proses enkripsi dan dekripsi adalah sebagai berikut

a.persamaan enkripsi

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

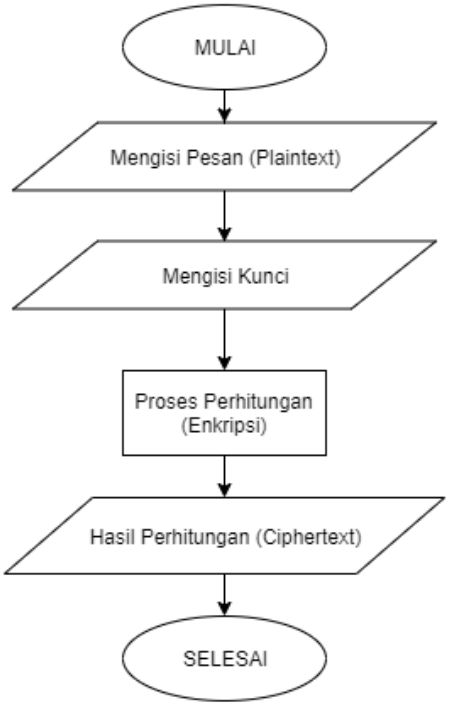
E = C= P + K mod 26 (1)

b.persamaan dekripsi

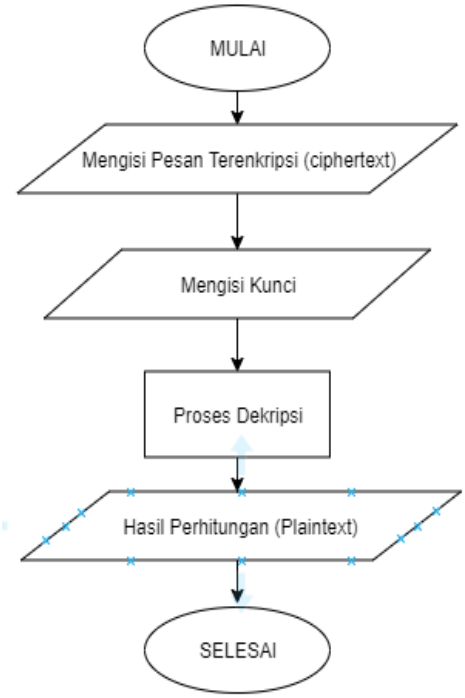
D = P= C – K mod 26 (2)

Keterangan :
E = Enkripsi
C = Ciphertext
K = Kunci
P = Plaintext
D = Dekripsi
Mod = modulus 26

Tahapan proses enkripsi dan dekripsi dapat dilihat pada gambar diagram dibawah



Gambar 1. tahapan proses enkripsi



Gambar 2 tahapan proses dekripsi

Contoh *plaintext* yang akan dilakukan proses enkripsi adalah : **STMIK TRIGUNA DHARMA** dengan kunci 3. Maka langkah penyelesainnya adalah sebagai berikut:

1. Melakukan konversi pada setiap abjad kedalam angka seperti tabel dibawah ini

Tabel 1. Abjad dan Angka

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

2. Menjumlahkan setiap angka dengan kunci yang dibuat menggunakan persamaan enkripsi yang telah dijelaskan diatas.
   Pada contoh ini kunci yang diberikan adalah 3.
   E = C= P + 3 mod 26 (3)

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Gambar 2. Proses Enkripsi

C1 : S + 3 mod 26 : 18 + 3 mod 26 : 21 mod 26 : 21 > V **C2** : T + 3 mod 26 : 19 + 3 mod 26 : 22 mod 26 : 22 > W **C3** : M + 3 mod 26 : 12 + 3 mod 26 : 15 mod 26 : 15 > P	**C4** : I + 3 mod 26 : 8 + 3 mod 26 : 11 mod 26 : 11 > L **C5** : K + 3 mod 26 : 10 + 3 mod 26 : 13 mod 26 : 13 > N **C6** : T + 3 mod 26 : 22 + 3 mod 26 : 22 mod 26 : 22 > W	**C7** : R + 3 mod 26 : 17 + 3 mod 26 : 20 mod 26 : 20 > U **C8** : I + 3 mod 26 : 8 + 3 mod 26 : 11 mod 26 : 1 > L **C9** : G + 3 mod 26 : 6 + 3 mod 26 : 9 mod 26 : 9 > J
C10 : U + 3 mod 26 : 20+ 3 mod 26 : 23 mod 26 : 23 > X **C11** : N + 3 mod 26 : 13 + 3 mod 26 : 16 mod 26 : 16 > Q **C12** : A + 3 mod 26 : 0+ 3 mod 26 : 3 mod 26 : 3 > D	**C13** : D+ 3 mod 26 : 3 + 3 mod 26 : 6 mod 26 : 6 > G **C14** : H + 3 mod 26 : 7 + 3 mod 26 : 10 mod 26 : 10 > K **C15** : A + 3 mod 26 : 0 + 3 mod 26 : 3 mod 26 : 3 > D	**C16** : R + 3 mod 26 : 17 + 3 mod 26 : 20 mod 26 : 20 > U **C17** : M + 3 mod 26 : 12 + 3 mod 26 : 15 mod 26 : 15 > P **C18** : A + 3 mod 26 : 0 + 3 mod 26 : 3 mod 26 : 3 > D
Plainteks **STMIK TRIGUNA DHARMA** menghasilkan ciphertext **VWPLN WULJXQD GKDUPD**		

Untuk mengembalikan pesan yang tersembunyi (*ciphertext*) maka perlu dilakukan proses dekripsi. Dekripsi adalah proses mengembalikan pesan terenkripsi (*ciphtertext*) kepesan semula (*plaintext*). Tahapan proses dekripsi adalah sebagai berikut:

1. Melakukan konversi pada setiap abjad kedalam angka;
2. Mengurangkan setiap angka dengan kunci yang dibuat menggunakan persamaan dekripsi . Pada contoh ini kunci yang dibuat adalah 3.

   D = P= C – 3 mod 26

Gambar 3. Proses Dekripsi

P1 : V - 3 mod 26 : 21 - 3 mod 26 : 21 mod 26 : 18 > S **P2** : W - 3 mod 26 : 22 - 3 mod 26 : 22 mod 26 : 19 > T **P3** : P - 3 mod 26 : 15 - 3 mod 26 : 12 mod 26 : 12 > M	**P4** : L - 3 mod 26 : 11 - 3 mod 26 : 8 mod 26 : 8 > I **P5** : N - 3 mod 26 : 13 - 3 mod 26 : 10 mod 26 : 10 > K **P6** : W - 3 mod 26 : 22 - 3 mod 26 : 19 mod 26 : 19 > T	**P7** : U - 3 mod 26 : 20 - 3 mod 26 : 17 mod 26 : 17 > R **P8** : L- 3 mod 26 : 11 - 3 mod 26 : 8 mod 26 : 8 > I **P9** : J - 3 mod 26 : 9 - 3 mod 26 : 6 mod 26 : 6 > G
P10 : X - 3 mod 26 : 23- 3 mod 26 : 20 mod 26 : 20 > U **P11** : Q - 3 mod 26 : 16 - 3 mod 26 : 13 mod 26 : 13 > N **P12** : D - 3 mod 26 : 0- 3 mod 26 : 3 mod 26 : 3 > A	**P13** : G- 3 mod 26 : 6 - 3 mod 26 : 3 mod 26 : 3 > D **P14** : K - 3 mod 26 : 10 - 3 mod 26 : 7 mod 26 : 7 > H **P15** : D - 3 mod 26 : 3 - 3 mod 26 : 0 mod 26 : 0 > A	**P16** : U - 3 mod 26 : 20 - 3 mod 26 : 17 mod 26 : 17 > R **P17** : P - 3 mod 26 :15 - 3 mod 26 : 12 mod 26 : 12 > M **P18** : D - 3 mod 26 : 3 - 3 mod 26 : 0 mod 26 : 0 > A
Plaintext dari **VWPLN WULJXQD GKDUPD** adalah **STMIK TRIGUNA DHARMA**		

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

2.Algoritma *Vigenere Cipher*

Vigenere merupakan perluasan dari algoritma Caesar cipher. Yang membedakan antara diantara kedua algoritma ini adalah terletak pada kunci.

Pada algoritma Caesar cipher setiap plaintext ataupun ciphertext akan dijumlahkan dengan kunci yang sama, mulai dari huruf awal hingga akhir. Tentunya hal ini menjadi titik lemah dari algoritma ini, karena seorang *cryptanylisys* tidak perlu mengetahui kuncinya, cukup melakukan ujicoba kunci 0 sampai dengan 25. Apabila kunci 0 sampai 25 ini diujikan, maka hasil ataupun plaintetxnya akan didapat.

Kelemahan pada algoritma *caesar cipher* ini bisa diatasi dengan algoritma *vigenere cipher*, dimana *vigenere cipher* tidak lagi menjumlahkan setiap huruf dengan kunci yang sama pada proses enkripsi melainkan menggunakan kunci yang berbeda. Tentu dengan menggunakan kunci yang berbeda, akan lebih menyulitkan seorang *cryptanylisys* dalam memecahkan pesan yang di enkripsi. Contoh plaintext yang akan dilakukan proses enkripsi adalah STMIK TRIGUNA DHARMA dengan kunci LANGKAH SUKSES.

Tahapan penyelesaiannya adalah sebagai berikut:

1. Memasangkan setiap huruf plaintext dengan kunci dan apabila kunci telah habis dan huruf pada plaintext belum mendapatkan kunci, maka kunci akan diulang sampai setiap huruf *plaintext* mendapatkan pasangan kunci. Persamaan yang digunakan sama dengan algoritma *Caesar cipher*, baik proses enkripsi dan dekripsi

Gambar 4**.** Memasangkan Kunci dengan plaintext

Plaintext	S	T	M	I	K	T	R	I	G	U	N
Kunci	L	A	N	G	K	A	H	S	U	K	S

Plaintext	A	D	H	A	R	M	A
Kunci	E	S	L	A	N	G	K

2. Menjumlahkan setiap huruf pada plaintext dengan kunci yang telah dipasangkan.

Gambar 5. Proses Enkripsi

C1 : S + L mod 26 : 18 + 11 mod 26 : 29 mod 26 : 3 > D C2 : T + A mod 26 : 19 + 0 mod 26 : 19 mod 26 : 19 > T C3 : M + N mod 26 : 12 + 13 mod 26 : 25 mod 26 : 25 > Z	C4 : I + G mod 26 : 8 + 6 mod 26 : 14 mod 26 : 14 > O C5 : K + K mod 26 : 10 + 10 mod 26 : 20 mod 26 : 20 > U C6 : T + A mod 26 : 19 + 0 mod 26 : 19 mod 26 : 19 > T	C7 : R + H mod 26 : 17 + 7 mod 26 : 24 mod 26 : 24 > Y C8 : I + S mod 26 : 8 + 18 mod 26 : 26 mod 26 : 0 > A C9 : G + U mod 26 : 6 + 20 mod 26 : 26 mod 26 : 0 > A
C10 : U + K mod 26 : 20+ 10 mod 26 : 30 mod 26 : 4 > E C11 : N + S mod 26 : 13 + 18 mod 26 : 31 mod 26 : 5 > F C12 : A + E mod 26 : 0+ 4 mod 26 : 4 mod 26 : 4 > E	C13 : D + S mod 26 : 3 + 18 mod 26 : 21 mod 26 : 21 > V C14 : H + L mod 26 : 7 + 11 mod 26 : 18 mod 26 : 18 > S C15 : A + A mod 26 : 0 + 0 mod 26 : 0 mod 26 : 0 > A	C16 : R + N mod 26 : 17 + 13 mod 26 : 30 mod 26 : 4 > E C17 : M + G mod 26 : 12 + 6 mod 26 : 18 mod 26 : 18 > S C18 : A + K mod 26 : 0 + 10 mod 26 : 10 mod 26 : 10 > K
plainteks **STMIK TRIGUNA DHARMA** menghasilkan ciphertext **DTZOUTYAAEFEVSAESK**		

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Untuk mengembalikan pesan yang tersembunyi (*ciphertext*) maka perlu dilakukan proses dekripsi. Dekripsi adalah proses mengembalikan pesan terenkripsi (*ciphtertext*) kepesan semula.

Tabel 6. Proses Dekripsi

C1 : D - L mod 26 : 3 - 11 mod 26 : -8 mod 26 : 18 > S C2 : T - A mod 26 : 19 - 0 mod 26 : 19 mod 26 : 19 > T C3 : Z - N mod 26 : 25 - 13 mod 26 : 12 mod 26 : 12 > M	C4 : O - G mod 26 : 14 - 6 mod 26 : 8 mod 26 : 8 > I C5 : U - K mod 26 : 20 - 10 mod 26 : 10 mod 26 : 10 > K C6 : T - A mod 26 : 19 - 0 mod 26 : 19 mod 26 : 19 > T	C7 : Y - H mod 26 : 24 - 7 mod 26 : 17 mod 26 : 17 > R C8 : A - S mod 26 : 0 - 18 mod 26 : -18 mod 26 : 8 > I C9 : A - U mod 26 : 0 - 20 mod 26 : -20 mod 26 : 6 > G
C10 : E - K mod 26 : 4 - 10 mod 26 : -6 mod 26 : 20 > U C11 : F - S mod 26 : 5 - 18 mod 26 : -13 mod 26 : 13 > N C12 : E - E mod 26 : 4 - 4 mod 26 : 0 mod 26 : 0 > A	C13 : V - S mod 26 : 21 - 18 mod 26 : 3 mod 26 : 3 > D C14 : S - L mod 26 : 18 - 11 mod 26 : 7 mod 26 : 7 > H C15 : A - A mod 26 : 0 - 0 mod 26 : 0 mod 26 : 0 > A	C16 : E - N mod 26 : 6 - 13 mod 26 : -7 mod 26 : 17 > R C17 : S - G mod 26 : 18 - 6 mod 26 : 18 mod 26 : 12 > M C18 : K - K mod 26 : 10 - 10 mod 26 : 0 mod 26 : 0 > A
Ciphertext **DTZOUTYAAEFEVSAESK** menghasilkan plaintext **STMIK TRIGUNA DHARMA**		

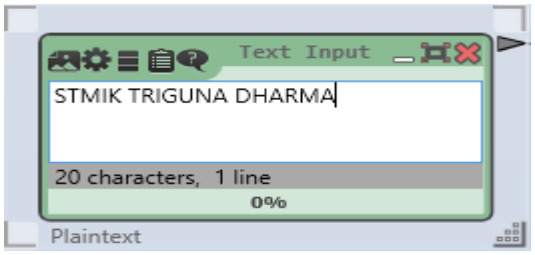
HASIL DAN PEMBAHASAN

Pada pengujian ini proses enkripsi dan dekripsi menggunakan sebuah tools yang bernama cryptool versi 2.1.

Contoh plaintext yang akan dilakukan proses enkripsi adalah STMIK TRIGUNA DHARMA menggunakan metode Caesar Cipher dan Vigenere Cipher.

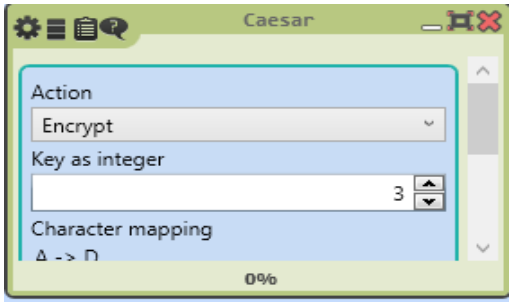
Tahapan penggunaan tools untuk proses enkripsi

1. Mengisi *plaintext* yang akan disembunyikan. Pengisian *plaintext* diletakkan pada lembar yang berjudul Text Input



Gambar 6. Mengisi Plaintext

2. Setelah plaintext terisi, maka langkah selanjutknya memilih *action*: *encrypt* dan mengisikan kunci 3.

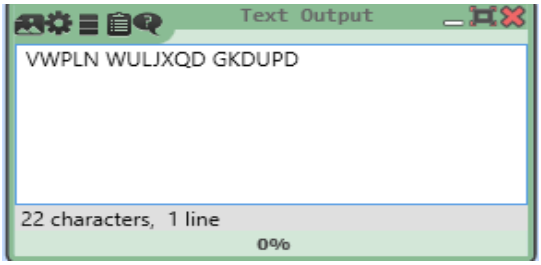


Gambar 7. Mengisi kunci

3. Setelah mengisikan kunci maka selanjutnya adalah melakukan proses enkripsi dengan cara klik pada *icon play*

Gambar 8. Proses Enkripsi

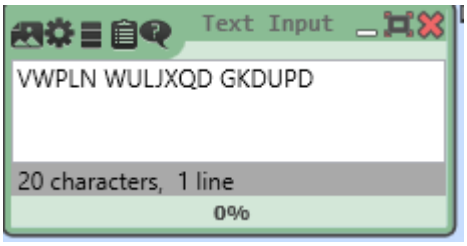
4. Setelah diklik icon play, maka akan akan menghasilkan pesan tersembunyi (*ciphtertext*)



Gambar 9. Hasil Enkripsi

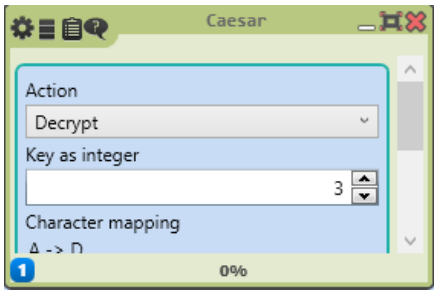
JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Untuk mengembalikan pesan yang tersembunyi (*ciphertext*) maka perlu dilakukan proses dekripsi, tahapan penggunaan tools untuk proses dekripsi:
1. Mengisi *ciphertext* yang akan kembalikan ke awal (*plaintext*). Pengisian *ciphertext* diletakkan pada lembar yang berjudul Text Input



Gambar 10. Mengisi Ciphertext

2. Memilih *action*: *Decrypt* dan mengisikan kunci 3.

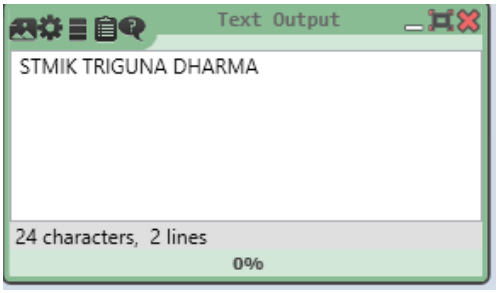


Gambar 11. Mengisi kunci

3. Setelah mengisikan kunci maka selanjutnya adalah melakukan proses dekripsi dengan cara klik pada *icon play*

Gambar 12. Proses Dekripsi

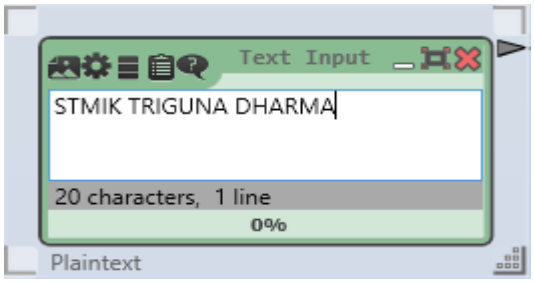
4. Setelah diklik icon play, maka textoutput akan menghasilkan pesan awal (*plaintext*)



Gambar 13. Hasil Dekripsi

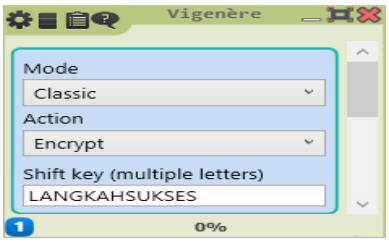
Tahapan penggunaan *tools* untuk proses enkripsi menggunakan metode *vigerene cipher*

1. Mengisi *plaintext* yang akan disembunyikan. Pengisian *plaintext* diletakkan pada lembar yang berjudul Text Input dengan isian STMIK TRIGUNA DHARMA



Gambar 14. Input Plaintext

2. Setelah *plaintext* terisi, maka langkah selanjutknya memilih *action*: *encrypt* dan mengisikan kunci LANGKAHSUKSES.



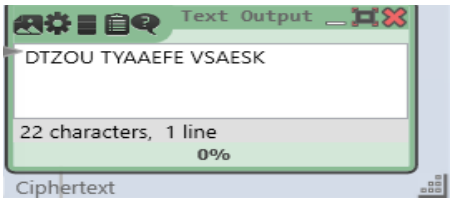
Gambar 15**.** Mengisi Kunci

3. Setelah mengisikan kunci maka selanjutnya adalah melakukan proses enkripsi dengan cara klik pada *icon play*

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. VII No. 2, April 2021, hlm. 117 - 126 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v7i2.914
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Gambar 16. Proses Enkripsi

4. Setelah diklik icon play, maka akan akan menghasilkan pesan tersembunyi (*ciphtertext*)



Gambar 17. Hasil Enkripsi

SIMPULAN

Dengan menggunakan *CrypTool* dalam pembelajaran kriptografi, hasil yang didapat lebih akurat dan lebih cepat. Disamping itu juga penggunaan *Cryp-Tool* dianggap sangat membantu untuk mengetahui hasil perhitungan manual enkripsi dan dekripsi, sehingga dengan kata lain *tools* ini bisa meminimalisir kesalahan dalam menghasilkan pesan.

UCAPAN TERIMA KASIH

Ucapan terimakasih kepada DRPM Deputi Bidang Penguatan Riset Dan Pengembangan Kementerian Riset Dan Teknologi/Badan Riset Dan Inovasi Nasional Sesuai dengan Kontrak Penelitian Tahun Anggaran 2020.

DAFTAR PUSTAKA

[1] H. Ibda, "Penguatan Literasi Baru Pada Guru Madrasah Ibtidaiyah Dalam Menjawab Tantangan Era Revolusi Industri 4.0," *J. Res. Thought Islam. Educ.*, vol. 1, no. 1, pp. 1–21, 2018, doi: 10.24260/jrtie.v1i1.1064.

[2] Y. Kristanti, S. Subiki, and R. Handayani, "Model Pembelajaran Berbasis Proyek (Project Based Learning Model) Pada Pembelajaran Fisika Di SMA," *J. Pembelajaran Fis. Univ. Jember*, vol. 5, no. 2, p. 116319, 2016.

[3] M. A. Kurniawan, A. Miftahillah, and N. M. Nasihah, "Pembelajaran Berbasis Student-Centered Learning Di Perguruan Tinggi: Suatu Tinjauan Di Uin Sunan Kalijaga Yogyakarta," *Lentera Pendidik. J. Ilmu Tarb. dan Kegur.*, vol. 21, no. 1, pp. 1–11, 2018, doi: 10.24252/lp.2018v21n1i1.

[4] I. wayan Santyasa, "Student centered learning : Alternatif pembelajaran inovatif abad 21 untuk menyiapkan guru profesional," *Pros. Semin. Nas. Quantum*, vol. 25, pp. xix–xxxii, 2018.

[5] I. Emaliana, "Teacher-centered or Student-centered Learning Approach to Promote Learning ?," *J. Sos. Hum.*, vol. 10, pp. 59–70, 2017

[6] R. D. Prayogi and R. Estetika, "Kecakapan Abad 21 : Kompetensi Digital Pendidik Masa Depan," *J. Manaj. Pendidik.*, vol. 14, no. 2, pp. 144–151, 2019,

[7] R. Akbar, Z. Arifin,) Dyna, and M. Khairina, "Rancang Bangun Multifile Locker Application Menggunakan Metode Data Encryption Standard," *J. Inform. Mulawarman*, vol. 9, no. 2, 2014.

[8] U. M. K. Abdullah and A. Azis, "Efektifitas Strategi Pembelajaran Analisis Nilai Terhadap

Pengembangan Karakter Siswa pada Mata Pelajaran Sejarah Kebudayaan Islam," *J. Penelit. Pendidik. Islam*, vol. 7, no. 1, p. 51, 2019, doi: 10.36667/jppi.v7i1.355.

[9] "pembelajaran efektif 2," *KONSEP DAN Indik. PEMBELAJARAN Ef.*, vol. 1, p. 2, 2018,

[10] P. Sonang Siregar, L. Wardani, R. Genesa Hatika, S. Rokania, and U. Pasir Pengaraian, "PENERAPAN PENDEKATAN PEMBELAJARAN AKTIF INOVATIF KREATIF EFEKTIF DAN MENYENANGKAN (PAIKEM) PADA PEMBELAJARAN MATEMATIKA KELAS IV SD NEGERI 010 RAMBAH," *J. Pemikir. dan Pengemb. SD*, vol. 5, no. 2, 2017.

[11] M. S. M. Rahmi, M. A. Budiman, and A. Widyaningrum, "Pengembangan Media Pembelajaran Interaktif Macromedia Flash 8 pada Pembelajaran Tematik Tema Pengalamanku," *Int. J. Elem. Educ.*, vol. 3, no. 2, p. 178, 2019,

[12] S. R. Nurhalimah, S. Suhartono, and U. Cahyana, "Pengembangan Media Pembelajaran Mobile Learning Berbasis Android pada Materi Sifat Koligatif Larutan," *JRPK J. Ris. Pendidik. Kim.*, vol. 7, no. 2, pp. 160–167, 2017

[13] L. Choirun Nisa, "PENGARUH PEMBELAJARAN E-LEARNING TERHADAP HASIL BELAJAR MATA KULIAH STATISTICS MAHASISWA TADRIS BAHASA INGGRIS FAKULTAS TARBIYAH IAIN WALISONGO," 2012.

[14] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020

[15] Y. Efrand, Asnawati, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher," *J. Media Infotama*, vol. 10, no. 2, pp. 120–128, 2014.

[16] S. T. C. Kurniawan, D. Dedih, and S. Supriyadi, "Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android," *J. Online Inform.*, vol. 2, no. 2, p. 102, 2018

[17] A. Halimatusadiah, U. Sunan, and G. Djati Bandung, "IMPLEMENTASI KRIPTOGRAFI METODE CAESAR CHIPER PADA CHATING.