Instal : Jurnal Komputer

E-ISSN: 2808-683X
Edisi : Volume 16 Nomor 04 | 2024

Available online at https://journalinstal.cattleyadf.org/index.php/Instal/index

Optimizing Cryptography Teaching Using E-Learning Approaches

M.Syaifuddin[1], Zulfi Azhar[2], Saidi Ramadan Siregar[3], Eferoni Ndururu[4]
[1,2,3,4] Universitas Budi Dharma

ARTICLE INFO

Keywords:

Cryptography
E-Learning

ABSTRACT

Cryptography plays a critical role in safeguarding data, making it an essential subject in information security education. Within this course, various algorithms are introduced, each requiring different levels of computational complexity. However, instructional practice has revealed frequent student errors in executing encryption and decryption processes, primarily due to limited understanding of cryptographic algorithms and mathematical procedures. Since accuracy is fundamental in cryptography, miscalculations can lead to incorrect message interpretation. To mitigate these issues, the learning process is supported by CrypTool, a digital aid designed to guide students through encryption and decryption tasks and minimize computational errors.

Corresponding Author:
M. Syaifuddin
Universitas Budi Dharma
Email:msyaifuddin@gmail.com

INTRODUCTION

In the current digital era, the affordability and ease of accessing information have significantly influenced the direction of educational practices. Traditionally, learning was predominantly teacher-centered, where the flow of knowledge occurred in a one-way manner from instructor to student [1][2][3]. However, the rapid advancement of technology and information systems has transformed the educational paradigm into a more student-centered approach, particularly in the context of 21st-century learning [4][5].

Twenty-first-century education is characterized by the emphasis on learning skills, practical competencies, and literacy. Learning skills refer to activities within the educational process that foster collaboration, communication, critical thinking, and creativity [6][7]. Instruction, in this context, is defined as a structured effort aimed at facilitating the learning of individuals or groups through various strategies, methods, and approaches to achieve specific educational goals [8].

The primary goal of instruction is to assist learners in acquiring knowledge that can serve as a foundation for both present and future life challenges [9]. Several key components influence the effectiveness of the learning process, including (1) the learner, (2) the instructor or facilitator, and (3) the learning materials [10].

To enhance the effectiveness of instruction, the use of appropriate and relevant learning media is essential. Instructional media play a vital role in supporting teaching and learning activities

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

by clarifying messages and helping learners better understand the content, thereby facilitating the achievement of learning objectives [11]. Moreover, instructional media allow learners to access materials repeatedly, which enhances comprehension and retention.

In practice, instructional media also serve as supplementary tools that reinforce the materials delivered in class [12][13]. In the context of cryptography instruction, the use of digital tools makes the learning experience more accessible and efficient. These tools are typically designed with user-friendly interfaces that guide learners through the stages of plaintext input, encryption, and decryption processes.

Cryptography is a field of study that focuses on securing messages (plaintext) from unauthorized access [14]. It involves two critical processes: encryption and decryption. Encryption is the transformation of readable data (clear text) into an unintelligible format (cipher text), while decryption is the reverse process of converting cipher text back into readable plaintext [15][16][17]. The primary aim of cryptography is to ensure the confidentiality of messages transmitted across various media.

Accuracy is crucial in both encryption and decryption. Any error in the encryption process will lead to incorrect cipher text, which in turn results in erroneous decryption outcomes. To minimize such errors, a support tool known as CrypTools can be utilized. This tool simplifies the cryptographic process, enabling students to perform encryption and decryption more efficiently and accurately compared to manual calculations. The use of CrypTools thus helps learners grasp cryptographic concepts more effectively and with greater confidence.

METHODS

The equation that can be used in the encryption and decryption process is as follows:

Encryption

$$E = C = P + K \bmod 26$$

E : Encryption
C : Ciphertext (the encrypted message)
P : Plaintext (the original message)
K : Key (used for the encryption process)
mod : Modulo operation
26 : Number of letters in the alphabet

Decryption

$$D = P = C - K \bmod 26$$

Encryption

As an illustration, the plaintext **"STMIK TRIGUNA DHARMA"** will be encrypted using a key of **3**. The encryption process can be carried out through the following steps:

1 Convert each letter in the plaintext into its corresponding numerical value based on the table provided below.

Table 1. Letters and Their Corresponding Numerical Values

A	B	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

2. Add each numerical value with the given key using the encryption formula explained previously. In this example, the key used is **3**.

$$E = C = P + 3 \bmod 26$$

C1: S
- *S*+3mod26
- 18+3mod26
- 21mod26
- 21>*V*

C2: T
- *T*+3mod26
- 19+3mod26
- 22mod26
- 22>*W*

C3: M
- *M*+3mod26
- 12+3mod26
- 15mod26
- 15>*P*

C4: I
- *I*+3mod26
- 8+3mod26
- 11mod26
- 11>*L*

C5: K
- *K*+3mod26
- 10+3mod26
- 13mod26
- 13>*N*

C6: (space)

C7: T
- *T*+3mod26
- 19+3mod26
- 22mod26
- 22>*W*

C8: R
- *R*+3mod26
- 17+3mod26
- 20mod26
- 20>*U*

C9: I
- *I*+3mod26
- 8+3mod26
- 11mod26
- 11>*L*

C10: G

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

- *G*+3mod26
- 6+3mod26
- 9mod26
- 9>*J*

C11: U
- *U*+3mod26
- 20+3mod26
- 23mod26
- 23>*X*

C12: N
- *N*+3mod26
- 13+3mod26
- 16mod26
- 16>*Q*

C13: A
- *A*+3mod26
- 0+3mod26
- 3mod26
- 3>*D*

C14: (space)
- *D*+3mod26
- 3+3mod26
- 6mod26
- 6>*G*

C16: H
- *H*+3mod26
- 7+3mod26
- 10mod26
- 10>*K*

C17: A
- *A*+3mod26
- 0+3mod26
- 3mod26
- 3>*D*

C18: R
- *R*+3mod26
- 17+3mod26
- 20mod26
- 20>*U*

C19: M
- *M*+3mod26
- 12+3mod26
- 15mod26
- 15>*P*

C20: A
- *A*+3mod26
- 0+3mod26
- 3mod26

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

- 3>*D*

As a result, the ciphertext generated from the plaintext "STMIK TRIGUNA DHARMA" is "**VWPLN WULJXQD GKDUPD"**

Decryption
To retrieve the hidden message (ciphertext), a decryption process must be carried out. Decryption is the process of converting an encrypted message (ciphertext) back to its original form (plaintext). The steps involved in the decryption process are as follows:

1. Convert each letter of the ciphertext into its corresponding numerical value
2. Subtract each numerical value by the given key using the decryption formula. In this example, the key used is **3**

C1: V
- *V*−3mod26
- 21−3mod26
- 18mod26
- 18>*S*

C2: W
- *W*−3mod26
- 22−3mod26
- 19mod26
- 19>*T*

C3: P
- *P*−3mod26
- 15−3mod26
- 12mod26
- 12>*M*

C4: L
- *L*−3mod26
- 11−3mod26
- 8mod26
- 8>*I*

C5: N
- *N*−3mod26
- 13−3mod26
- 10mod26
- 10>*K*

C6: (space)

C7: W
- *W*−3mod26
- 22−3mod26
- 19mod26
- 19>*T*

C8: U
- *U*−3mod26
- 20−3mod26

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

- 17mod26
- 17>*R*

C9: L

- *L*−3mod26
- 11−3mod26
- 8mod26
- 8>*I*

C10: J

- *J*−3mod26
- 9−3mod26
- 6mod26
- 6>*G*

C11: X

- *X*−3mod26
- 23−3mod26
- 20mod26
- 20>*U*

C12: Q

- *Q*−3mod26
- 16−3mod26
- 13mod26
- 13>*N*

C13: D

- *D*−3mod26
- 3−3mod26
- 0mod26
- 0>*A*

C14: (space)

C15: G

- *G*−3mod26
- 6−3mod26
- 3mod26
- 3>*D*

C16: K

- *K*−3mod26
- 10−3mod26
- 7mod26
- 7>*H*

C17: D

- *D*−3mod26
- 3−3mod26
- 0mod26
- 0>*A*

C18: U

- *U*−3mod26
- 20−3mod26
- 17mod26
- 17>*R*

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

C19: P

- $P-3 \bmod 26$
- $15-3 \bmod 26$
- $12 \bmod 26$
- $12>M$

C20: D

- $D-3 \bmod 26$
- $3-3 \bmod 26$
- $0 \bmod 26$
- $0>A$

RESULTS AND DISCUSSION

In this experiment, the encryption and decryption processes are performed using a tool called CrypToolversion2.1.The plaintext used for the encryption example is "STMIK TRIGUNA DHARMA", which will be encrypted using both the Caesar Cipher. Steps for using the tool in the encryption process

1. Enter the plaintext to be encrypted. The plaintext should be placed in the sheet labeled **"Text Input"**

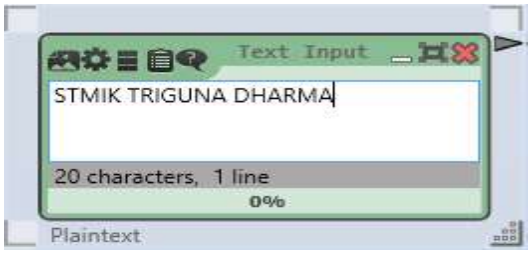

Figure 1. Encryption Process

2. Once the plaintext is entered, the next step is to select the action "Encrypt" and enter the key 3

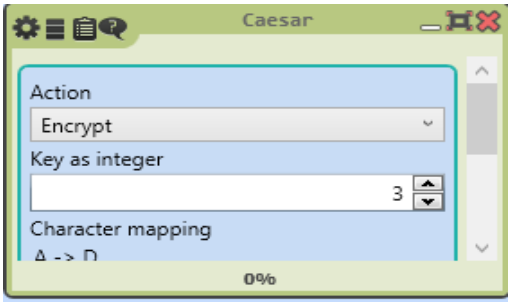

Figure 2. Key Process

3. After entering the key, proceed with the encryption process by clicking the Play icon.

Figure 3. Encryption Process

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

4. Once the Play icon is clicked, the hidden message (ciphertext) will be generated.

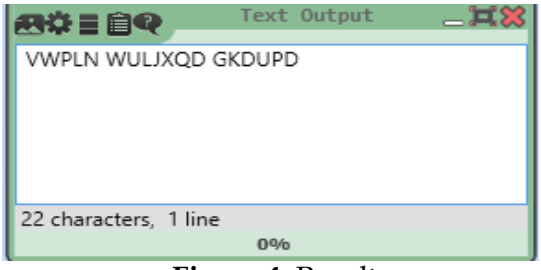

Figure 4. Result

CONCLUSION

By using CrypTool in cryptography learning, the results obtained are more accurate and faster. In addition, CrypTool is considered highly beneficial for verifying manual encryption and decryption calculations. In other words, this tool helps minimize errors in generating messages.

REFERENCES

[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, D. Y. 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

Page : 89-97
doi.org/10.54209/jurnalinstall.v16i04.397

(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 And 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."