

Pengembangan Algoritma Caesar Cipher dalam Game-Based Learning untuk Pendidikan Kriptografi pada Anak

Putu Arya Dharma Kesuma^{a1}, I Gede Surya Rahayuda^{a2}

^aProgram Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
¹aryadharmakesuma@gmail.com
²igedesuryarahayuda@unud.ac.id

Abstract

The decline in children's interest in learning due to easy access to games is the main reason I designed game-based learning. To make learning more engaging, presenting materials in an interactive way is essential. Game-based learning addresses this issue by packaging educational content attractively, increasing children's interest in learning. This game will introduce the world of IT to children, particularly cyber security. One key concept is cryptography, using the Caesar cipher algorithm due to its simplicity and suitability for children. The Caesar cipher enables both encryption and decryption processes, making it perfect for teaching cryptography basics. By designing the game as an interactive mystery, it aims to enhance children's learning interest and introduce them to cyber security effectively, making learning both fun and educational.

Keywords: Game-Based Learning, Caesar Cipher, Cryptography

1. Pendahuluan

Dalam era digital yang terus berkembang dan mudahnya akses alat elektronik, anak-anak cenderung lebih tertarik untuk menghabiskan waktu mereka dengan bermain game daripada fokus pada proses belajar. Fenomena ini tidaklah mengejutkan. Game online mempunyai daya tarik yang membuat para siswa lebih senang bermain ketimbang belajar. Game online juga dapat menyebabkan ketagihan ketika sedang bermain, kemudian kalah anak-anak akan mencoba lagi sampai menang [1]. Game Based Learning merupakan metode pembelajaran yang menggunakan aplikasi permainan atau game yang telah dirancang khusus untuk membantu proses belajar dan membantu meningkatkan minat siswa dalam belajar [2]. Dengan berkembangnya zaman tentu cara penyajian materi pembelajaran harus berubah menjadi lebih menarik, salah satunya yaitu menyajikan materi pembelajaran melalui game. Pada game yang akan dikembangkan membahas mengenai pengenalan dunia IT kepada anak-anak salah satu konsep yang akan diimplementasikan adalah kriptografi, kriptografi merupakan bagian ilmu yang mempelajari tentang cara menjaga agar data atau pesan tetap aman [3], algoritma yang kriptografi yang akan digunakan adalah caesar cipher, alasan dipilihnya algoritma ini adalah mudahnya dipahami maka dari itu algoritma ini dipilih untuk membantu pengembangan game yang bertujuan untuk memperkenalkan dunia IT kepada anak-anak. Caesar cipher adalah salah satu algoritma enkripsi yang cukup mudah untuk dipahami, cara kerja dari algoritma tersebut adalah menggeser setiap huruf dalam pesan untuk menjaga keamanan data yang dikirim [4], seberapa jauh pergeseran huruf yang akan terjadi tergantung dari key yang digunakan. Diharapkan dengan dikembangkannya game-based learning ini nantinya dapat menarik minat anak-anak terhadap dunia IT dan memberikan sedikit pembelajaran tentang bagaimana dunia IT terkhususnya pada bagian cyber security. Cyber security adalah konsep dimana memproteksi informasi dari serangan cyber salah satunya adalah dengan metode kriptografi [5], dengan menggunakan kriptografi kita dapat menyamarkan pesan yang sebenarnya menjadi pesan yang sulit dibaca dan hanya dapat diubah kembali ke pesan yang dapat dibaca jika sudah mengetahui key dari pesan tersebut.

2. Metode Penelitian

2.1. Game Based Learning

Game Based Learning merupakan metode pembelajaran yang menggunakan aplikasi permainan atau game yang telah dirancang khusus untuk membantu proses belajar dan membantu meningkatkan minat siswa dalam belajar. Dalam rancangan ini akan memperkenalkan siswa tentang dunia keamanan digital, salah satu bidang ilmu yang diterapkan adalah kriptografi.

2.2. Algoritma Caesar Cipher

Dengan key yang telah ditentukan cara kerja algoritma yang digunakan pada penulisan ini adalah dengan menggeser huruf awal menjadi cipher. Jika Key yang digunakan adalah angka 2 maka pergeseran huruf yang terjadi adalah sebagai berikut:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Gambar 1. Pergeseran Huruf

Pada gambar 1 terjadi pergeseran 2 huruf dari A menjadi C, dari B menjadi D dan seterusnya, pergeseran 2 huruf ini terjadi dikarenakan penggunaan angka 2 pada key yang digunakan untuk melakukan enkripsi, jadi seberapa jauh pergeseran terjadi tergantung pada key yang digunakan nantinya.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	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

Gambar 2. Konversi Huruf

Pada gambar 2 dapat dilihat konversi huruf menjadi angka, tujuan huruf diubah menjadi angka ini adalah agar mempermudah pergeseran huruf pada saat implementasi menggunakan code. berikut adalah perhitungan manual menggunakan rumus sebelum diimplementasikan dengan code.

Keterangan:

PT = Plain Text
 CT = Cipher Text
 K = key

Enkripsi:

PT = Arya
 K = 2

CT = (PT + K) mod 26
 = 0 + 2
 = 2 mod 26
 = 2 (C)
 = C

CT = (PT + K) mod 26

$$\begin{aligned} &= 17 + 2 \\ &= 19 \text{ mod } 26 \\ &= 19 \text{ (T)} \\ &= \mathbf{T} \end{aligned}$$

$$\begin{aligned} \text{CT} &= (\text{PT} + \text{K}) \text{ mod } 26 \\ &= 24 + 2 \\ &= 26 \text{ mod } 26 \\ &= 0 \text{ (A)} \\ &= \mathbf{A} \end{aligned}$$

$$\begin{aligned} \text{CT} &= (\text{PT} + \text{K}) \text{ mod } 26 \\ &= 0 + 2 \\ &= 2 \text{ mod } 26 \\ &= 2 \text{ (C)} \\ &= \mathbf{C} \end{aligned}$$

Cipher Text = CTAC

Dekripsi:

$$\begin{aligned} \text{CT} &= \mathbf{CTAC} \\ \text{K} &= 2 \end{aligned}$$

$$\begin{aligned} \text{PT} &= (\text{CT} - \text{K}) \text{ mod } 26 \\ &= 2 - 2 \\ &= 0 \text{ mod } 26 \\ &= 0 \text{ (A)} \\ &= \mathbf{A} \end{aligned}$$

$$\begin{aligned} \text{PT} &= (\text{CT} - \text{K}) \text{ mod } 26 \\ &= 19 - 2 \\ &= 17 \text{ mod } 26 \\ &= 17 \text{ (R)} \\ &= \mathbf{R} \end{aligned}$$

$$\begin{aligned} \text{PT} &= (\text{CT} - \text{K}) \text{ mod } 26 \\ &= 0 - 2 \\ &= -2 \text{ mod } 26 \\ &= 24 \text{ (Y)} \\ &= \mathbf{Y} \end{aligned}$$

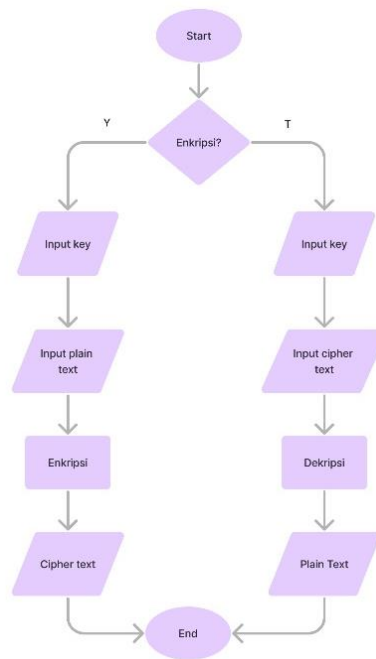
$$\begin{aligned} \text{PT} &= (\text{CT} - \text{K}) \text{ mod } 26 \\ &= 0 \text{ mod } 26 \\ &= 0 \text{ (A)} \\ &= \mathbf{A} \end{aligned}$$

Plain Text = Arya

3. Hasil dan Diskusi

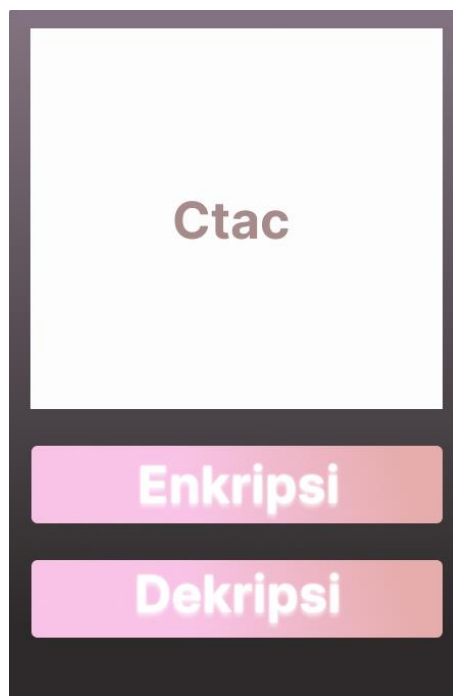
3.1. Rancangan Sistem

Pada perancangan sistem ini akan menggambarkan bagaimana flow dari program nantinya dan gambaran bagaimana rancangan sistem pada game.



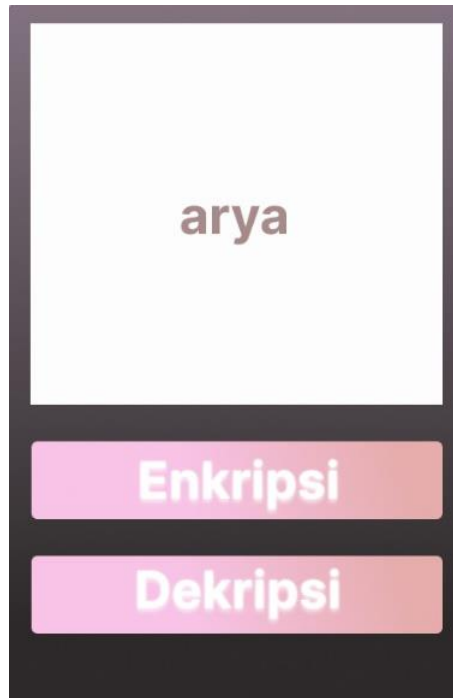
Gambar 3. Alur Sistem

Pada gambar 3 dijelaskan bagaimana alur sistem, ketika user memilih enkripsi user pertama harus memilih angka berapa yang digunakan sebagai key, lalu memasukan plain text kemudian sistem akan melakukan enkripsi kemudian memberikan output ciphertext, begitupun sebaliknya ketika user memilih dekripsi, pertama user akan memilih key kemudian memasukan ciphertext kemudian proses lainnya sama seperti bagian enkripsi.



Gambar 4. Design Input

Pada gambar 4 dapat dilihat "Text field" merupakan tempat user mengetikkan kalimat lalu dibawahnya adalah opsi yang dapat dipilih oleh user untuk melakukan enkripsi ataupun dekripsi.

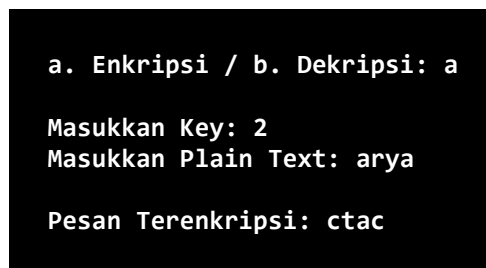


Gambar 5. Design Output

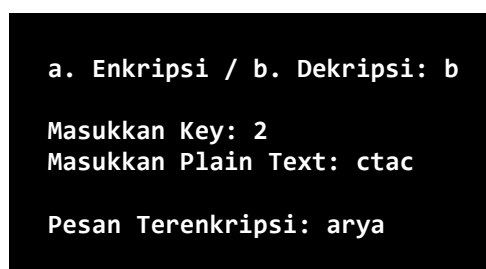
Pada gambar 5 dapat dilihat itu merupakan tempat hasil dari proses yang dipilih oleh user.

3.2. Pengujian Sistem

Pengujian sistem bermaksud untuk memastikan keakuratan output yang diberikan oleh sistem.



Gambar 6. Enkripsi



Gambar 7. Dekripsi

Pada gambar 6 dan 7 dapat dilihat bahwa sistem enkripsi dan dekripsi dapat berjalan dengan baik dan menghasilkan output yang akurat.

4. Kesimpulan

Dari percobaan yang telah dilakukan, dapat disimpulkan bahwa algoritma Caesar cipher mudah untuk dipahami. Oleh karena itu, pemilihan algoritma ini dalam rancangan game berbasis edukasi sangat tepat, karena kesederhanaannya memungkinkan pengguna mempelajarinya dengan mudah dan dapat digunakan untuk pengembangan game yang berbasis pembelajaran.

Daftar Pustaka

- [1] N. Nisrinafatin, "Pengaruh Game Online Terhadap Motivasi Belajar Siswa", JENFOL, vol. 1, no. 1, pp. 135-142, Mar. 2020.
- [2] R. Oktavia, "Game Based Learning Meningkatkan Efektivitas Belajar Siswa," Center for Open Science, Jun. 2022. Accessed: May 10, 2024. [Online]. Available: <http://dx.doi.org/10.31219/osf.io/6aeuy>
- [3] Yhopi Suhelna, "Perancangan Aplikasi Penyandian Pesan Teks dengan Menggunakan Algoritma Digraph Cipher", JUKI, vol. 2, no. 1, pp. 25–34, May 2020.
- [4] M. A. F. Rachman, "Perancangan Aplikasi Memo Menggunakan Algoritma Kriptografi Caesar Cipher Dan Rsa Berbasis Android," Semin. Nas. Inov. dan Apl. Teknol. di Ind., pp. 121–127, 2018.
- [5] F. Indah, A. Sidabuntar, and N. Anissa, "Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)", Jurnal Bidang Penelitian informatika, vol.1,no.1, pp. 1-8,2022.