MATHunesa
Jurnal Ilmiah Matematika
e-ISSN : 2716-506X | p-ISSN : 2301-9115

Volume 13 No 01
Tahun 2025

SUATU SKEMA ENKRIPSI BERBASIS GRAF

Ni Putu Permatasari
Jurusan Matematika, FMIPA, Universitas Pendidikan Ganesha
e-mail : permatasari@undiksha.ac.id

I Nengah Suparta
Jurusan Matematika, FMIPA, Universitas Pendidikan Ganesha
e-mail : nengah.suparta@undiksha.ac.id

Putu Kartika Dewi
Jurusan Matematika, FMIPA, Universitas Pendidikan Ganesha
e-mail : kartika.dewi@undiksha.ac.id

Abstrak

Abstrak: Kriptografi adalah ilmu dan seni mengamankan informasi dengan mengubahnya menjadi format yang tidak dapat dibaca oleh orang yang tidak berwenang, menggunakan teknik dan algoritma untuk menyandikan (enkripsi) dan mengembalikan (dekripsi) data. Penelitian ini bertujuan untuk membandingkan dua metode kriptografi yang dikembangkan oleh peneliti, yaitu metode 1 dan metode 2. Evaluasi metode yang dikembangkan ini mencakup aspek keamanan data, efisiensi , dan kualitas enkripsi-dekripsi. Penelitian dilakukan melalui uji coba kedua metode dengan menggunakan plainteks yang sama dan bantuan program untuk mencatat waktu yang dibutuhkan dalam melakukan enkripsi maupun dekripsi. Hasil evaluasi menunjukkan bahwa metode 1 lebih efisien dari segi waktu, tetapi tidak cocok untuk data yang membutuhkan keamanan tinggi. Sementara itu, metode 2 lebih unggul dalam hal keamanan, namun dengan biaya waktu yang lebih besar dan kompleksitas yang lebih tinggi. Kesimpulan dari penelitian ini adalah bahwa pemilihan pada metode kriptografi harus mempertimbangkan kebutuhan spesifik dari pengguna, terutama terkait dengan keseimbangan antara efisiensi dan keamanan. Untuk penelitian selanjutnya, disarankan untuk mengembangkan metode kriptografi yang dapat menggabungkan keunggulan dari kedua metode ini, sehingga dapat menawarkan keamanan yang tinggi dengan efisiensi yang lebih baik.
***Kata Kunci**:* kriptografi, enkripsi, dekripsi, kompleksitas algoritma, keamanan data

Abstract

Abstract: Cryptography is the science and art of securing information by converting it into a format that cannot be read by unauthorized persons, using techniques and algorithms to encode (encryption) and restore (decryption) data. This research aims to compare two cryptographic methods developed by researchers, namely method 1 and method 2. Evaluation of this research includes aspects of data security, efficiency and quality of encryption-decryption. The research was carried out by testing both methods using the same plaintext and the help of a program to record the time needed to carry out encryption and decryption. The evaluation results show that method 1 is more efficient in terms of time, but less suitable for data that requires high security. Meanwhile, method 2 is superior in terms of security, but at the cost of greater time and higher complexity. The conclusion of this research is that the choice of cryptographic method must consider as specific need of the user, especially regarding the balance between efficiency and security. For further research, it is recommended to develop a cryptographic method that can combine the advantages of these two methods, so that it can offer high security with better efficiency.
***Keywords**: cryptography, encryption, decryption, algorithm complexity, data security*

PENDAHULUAN

Kriptografi telah menjadi praktik penyandian yang digunakan oleh tentara Sparta di Yunani pada tahun 400 SM. Salah satu alat sederhana yang digunakan dalam praktik ini adalah *cipher disk*, *cipher disk* ini merupakan alat sederhana yang memungkinkan untuk mengenkripsi dan mendekripsi pesan dengan cara memutar cakram dengan huruf-huruf di atasnya, sehingga menghasilkan teks terenkripsi. Pada tahun 1467, arsitek Florentine Alberti menciptakan salah satu versi awal *cipher disk*, yang kemudian menjadi landasan untuk perkembangan teknologi penyandian selanjutnya.

Salah satu pengembangan terkenal dari *cipher disk* adalah Mesin Enigma. Mesin Enigma diciptakan pada tahun 1918 oleh Arthur Scherbius seorang insinyur Jerman. Mesin Enigma merupakan salah satu pencapaian terbesar dalam sejarah kriptografi dan merupakan puncak dari penggunaan graf dalam kriptografi pada masa itu. Mesin Enigma bekerja dengan cara mengubah seluruh huruf pesan menjadi karakter lain melalui serangkaian putaran. Penggunaan mesin enigma oleh Jerman selama Perang Dunia II menimbulkan tantangan besar bagi pihak Sekutu dalam memecahkan kode-kode yang dihasilkan oleh mesin ini. Hal inilah yang menjadi cikal bakal dalam sejarah kriptografi *modern* dengan memperkenalkan konsep kunci dan proses otomatis untuk enkripsi dan dekripsi (Frode dkk., 2019).

Dalam era *modern* ini, kriptografi berperan sebagai pelindung informasi sensitif dan menjaga integritas serta autentikasi data. Dengan demikian, kehidupan kita semakin terhubung secara digital, seperti komunikasi *online*, transaksi keuangan dan penyimpanan data. Penelitian ini menilai beberapa indikator untuk memastikan efektivitas metode kriptografi, yaitu keamanan data, efisiensi metode, dan kualitas enkripsi serta dekripsi (Ghazaly, 2023 & Watrianthos, 2021).

Peneliti meneliti tentang suatu skema enkripsi berbasis graf karena skema ini menggunakan struktur graf untuk melakukan proses enkripsi dan dekripsi data, memberikan keunggulan dalam memvisualisasikan hubungan antara kata kunci, dan hasil enkripsi. Graf dalam penelitian ini adalah representasi visual dari himpunan simpul (*nodes*) yang terhubung oleh sisi-sisi (*edges*), dan untuk graf yang digunakan dalam penelitian ini yaitu graf bipartit. Dengan menggunakan graf, analisis sistem kriptografi menjadi lebih mudah, memungkinkan untuk mengidentifikasi kelemahan dan kekurangan yang mungkin ada dalam skema kriptografi. Penggunaan graf juga dapat membantu dalam mengelola dan menguji algoritma metode kriptografi baru dan metode kriptografi berbasis graf ini telah dikaji dalam beberapa penelitian terdahulu yang disusun oleh (Hongbo dkk., 2021 & Ni, B., 2021).

Mengingat pentingnya menjaga keamanan data, sehingga kita harus memilih metode kriptografi yang efektif dalam menjaga keamanan data dan memiliki efisiensi yang bagus. Ada berbagai macam metode kriptografi seperti penggunaan *XOR* (*Exclusive OR*) yang telah dikaji dalam penelitian sebelumnya seperti yang terdokumentasikan dalam studi oleh dan penelitian terdahulu yang disusun oleh. Tabel konversi *ASCII* bertujuan untuk mengubah plainteks menjadi nilai atau nilai biner, *equation* (perhitungan matematika) yang dapat ditemukan pada penelitian terdahulu yang dikaji oleh (Hidayatuloh dkk., 2021 & Suriadi, 2020).

Penelitian ini bertujuan untuk membandingkan 2 metode kriptografi dalam upaya untuk meningkatkan keamanan data. Metode yang digunakan yaitu metode kriptografi yang dibuat penulis dengan menggunakan tabel konversi berdasarkan tabel *ASCII* yang bertujuan untuk mengubah plainteks menjadi nilai agar mempermudah dalam menerapkan kriptografi *modern*, dengan penggunaan kata kode untuk modifikasi, serta melakukan pemisahan kata kode menjadi 2 sub kata kode yaitu sub kata kode kanan dan kiri, dengan tujuan untuk pembuatan graf yang selanjutnya metode ini diberi nama metode 1. Metode ini dibandingkan dengan metode kriptografi lainnya, yang dikembangkan berdasarkan metode 1 dengan melakukan penambahan *equation* pada sub kata kode kanan yang selanjutnya metode ini diberi nama metode 2. Pemilihan *equation*, dikarenakan mudah untuk diimplementasikan dan dapat meningkatkan kompleksitas, sehingga membuatnya lebih sulit bagi pihak yang tidak berwenang untuk mendekripsi pesan yang telah dienkripsi dan dapat digabungkan kedalam berbagai jenis metode kriptografi sehingga metode ini lebih fleksibel dan pemilihan pergesaran tabel konversi bertujuan untuk mengubah semua data sehingga data menjadi acak dan semakin sulit bagi pihak yang tidak berwenang untuk mendekripsi hasil enkripsinya.

Penelitian ini sangat penting untuk dilakukan, dikarenakan meningkatnya ancaman terhadap keamanan data yang disebabkan oleh tersebarnya data di berbagai database dan kurangnya keamanan dari *database* yang menyimpan data, sehingga *hacker* mudah untuk meretas dan mencuri data. Sebagai contoh, kasus peretasan yang dilakukan oleh kelompok Surabaya *Black Hat* (SBH), yang telah meretas lebih dari 600 situs *web* yang tersebar di 44 negara pada tahun 2018. Dengan pembuatan metode ini dan melakukan perbandingan antara 2 buah metode, penelitian ini bertujuan untuk mengevaluasi efisiensi dan kecepatan masing-masing pendekatan,

serta untuk memahami keunggulan dan kelemahan yang terkait dengan penggunaan struktur graf dan operasi matematika atau logika dalam kriptografi (Ni, P., 2020).

Hasil dari penelitian ini, diharapkan dapat memberikan pemahaman yang lebih baik tentang kelebihan dan kekurangan masing-masing metode kriptografi, serta memberikan panduan dalam pemilihan metode kriptografi yang sesuai dengan kebutuhan keamanan data di era digital saat ini. Dengan demikian, penelitian ini dapat memberikan kontribusi yang signifikan, dalam pengembangan teknologi kriptografi, yang lebih canggih dan andal untuk mengamankan data yang kita miliki.

KAJIAN TEORI

Pada penelitian ini, digunakan tabel konversi yang disusun secara manual oleh peneliti dengan menggunakan tabel *ASCII* sebagai referensi. Tabel konversi mengurutkan entitas berdasarkan kriteria tertentu, seperti urutan huruf besar, huruf kecil, angka, dan simbol.

Tabel 1. Tabel Konversi

SP 0	A 1	B 2	C 3	D 4	E 5	F 6	G 7
H 8	I 9	J 10	K 11	L 12	M 13	N 14	O 15
P 16	Q 17	R 18	S 19	T 20	U 21	V 22	W 23
X 24	Y 25	Z 26	a 27	b 28	c 29	d 30	e 31
f 32	g 33	h 34	i 35	j 36	k 37	l 38	m 49
n 40	o 41	p 42	q 43	r 44	s 45	t 46	u 47
v 48	w 49	x 50	y 51	z 52	1 53	2 54	3 55
4 56	5 57	6 58	7 69	8 60	9 61	0 62	! 63
“ 64	# 65	$ 66	% 67	& 68	‘ 69	(70	) 71
* 72	+ 73	, 74	- 75	. 76	/ 77	[78	\ 79
] 80	^ 81	_ 82	` 83	: 84	; 85	< 86	= 87
> 88	? 89	@ 90	{ 91	| 92	} 93	~ 94	∂ 95
∆ 96	∏ 97	∑ 98	√ 99	∞ 100	∫ 101	≠ 102	≡ 103
≤ 104	≥ 105	α 106	€ 107	£ 108	¥ 109	ϕ 110	Ω 111
β 112	Γ 113	δ 114	ε 115	ζ 116	η 117	Θ 118	λ 119
μ 120	ξ 121	π 122	ω 123	₭ 124	₮ 125	℘ 126	ϖ 127

Penelitian ini juga menggunakan matriks ($8x16$) yang digunakan sebagai alat untuk mengkonversi teks biasa menjadi hasil enkripsi tanpa perlu melakukan perhitungan ulang, sehingga proses enkripsi menjadi lebih cepat dan efisien. Matriks sendiri terinspirasi dari algoritma dalam melakukan dekripsi yang disebut dengan *rainbow tables* yaitu sebuat proses pencatatan hasil dekripsi agar dapat digunakan kembali sehingga dapat menghemat waktu yang digunakan (Deby dkk., 2021 & Yukai 2019).

METODE

Jenis Penelitian

Penelitian ini adalah penelitian di bidang kriptografi dan keamanan informasi, berfokus pada perbandingan antara 2 metode yaitu, metode 1, dan metode 2 yang dikembangkan oleh peneliti. Secara lebih spesifik, penelitian ini mencakup pengembangan dan analisis algoritma enkripsi dan dekripsi, serta penilaian performa dari kedua metode tersebut. Indikator-indikator untuk memastikan efektivitas metode dalam penelitian ini antara lain keamanan data, efisiensi metode, dan kualitas enkripsi serta dekripsi. Metode yang digunakan dalam pengembangan sistem pada penelitian ini adalah metode pengembangan sistem atau (*System Development Life Cycle - SDLC*) dengan alur kerja sebagai berikut: Analisis kebutuhan, desain sistem, implementasi, pengujian, penerapan, dan pemeliharaan. Metode ini disebut *waterfall* karena alur kerja pengembangannya mengalir secara linier dari satu tahap ke tahap berikutnya, mirip dengan air terjun yang jatuh dari satu tingkatan ke tingkatan berikutnya. Berikut adalah urutan dari pelaksanaan metode *waterfall* (Amos, 2020).

Prosedur Penelitian

Tahapan dalam penelitian kriptografi yang digunakan dijelaskan sebagai berikut

1. Seleksi metode kriptografi
   a. Metode 1
   1. Enkripsi
   - *Input*: Plainteks
   - Konversi plainteks menjadi nilai: Menggunakan tabel konversi
   - Konversi nilai menjadi bit: Setiap nilai di konversi ke dalam bentuk biner dengan panjang 7 bit

- Pembagian bit: Membagi 7 bit menjadi dua sub kata kode, pada sub kata kode kanan berisi 4 bit dan 3 bit untuk sub kata kode kiri
- Penambahan bit: Tambahkan 1 bit pada sub kata kode kanan, lalu hitung nilai keduanya
- Penggabungan nilai: Menggabungkan kedua nilai dari sub kata kode kanan dan kiri
- Membuat matriks: Untuk penyimpanan hasil akhir dari proses enkripsi
- Penentuan kata kunci: Sesuai dengan ketentuan, boleh acak, akan tapi berurutan dari kecil ke besar
- Memasukan kata kunci pada nilai sub kata kode kiri lalu melakukan proses pengacakan
- Membuat graf: Untuk representasi data terenkripsi

2. Dekripsi

- *Input*: Graf terenkripsi
- Konversi graf menjadi nilai: Terjemahan graf menjadi bentuk graf aljabar untuk didekripsi
- Menentukan urutan sesuai dengan kata kunci dari yang terkecil ke terbesar dan menghilangkan kata kunci pada sub kata kode bagian kiri
- Konversi nilai dan melakukan pembagian bit: Menjadi 1 *byte* atau 8 bit dan membagi menjadi 2 sub kata kode kanan yang terdiri dari 5 bit dan kiri 3 bit
- Pengurangan bit: Kurangi 1 bit bernilai 1 pada setiap sub kata kode kanan
- Penggabungan kedua sub kata kode
- Konversi 7 bit menjadi nilai: Kembali menjadi nilai
- Konversi nilai hasil enkripsi ke plainteks: Menggunakan tabel konversi
- Plainteks (hasil)

b. Metode 2

1. Enkripsi

- *Input*: Plainteks
- Konversi plainteks menjadi nilai : Menggunakan tabel konversi
- Konversi nilai menjadi bit: Setiap nilai di konversi ke dalam bentuk biner dengan panjang 7 bit
- Pembagian bit: Membagi 7 bit menjadi dua sub kata kode, pada sub kata kode kanan berisi 4 bit dan 3 bit untuk sub kata kode kiri
- Penambahan bit : Tambahkan 1 bit pada sub kata kode kanan, lalu hitung nilai keduanya
- Penggabungan nilai : Menggabungkan kedua nilai dari sub kata kode kanan dan kiri
- Membuat matriks: Untuk penyimpanan hasil akhir dari proses enkripsi
- Penentuan kata kunci: Sesuai dengan ketentuan, boleh acak tapi berurutan dari kecil ke besar
- Melakukan perkalian pada kata kunci dengan 2
- Melakukan penjumlahan antara hasil perkalian kata kunci dengan sub kata kode kanan
- Memasukan kata kunci pada nilai sub kata kode kiri lalu melakukan proses pengacakan
- Membuat Graf: Untuk representasi data terenkripsi

2. Dekripsi

- *Input*: Graf terenkripsi
- Konversi graf menjadi nilai: Terjemahan graf menjadi bentuk graf aljabar untuk didekripsi
- Menentukan urutan sesuai dengan kata kunci dari yang terkecil ke terbesar dan menghilangkan kata kunci pada sub kode bagian kiri
- Melakukan perkalian pada kata kunci dengan 2
- Melakukan pengurangan antara hasil perkalian kata kunci dengan sub kata kode kanan
- Konversi nilai dan melakukan pembagian bit: Menjadi 1 *byte* atau 8 bit dan membagi menjadi 2 sub kata kode kanan yang terdiri dari 5 bit dan kiri 3 bit
- Pengurangan bit : Kurangi 1 bit bernilai 1 pada sub kata kode kanan
- Penggabungan kedua sub kata kode
- Konversi 7 bit menjadi nilai: Kembali menjadi nilai

- Konversi nilai hasil enkripsi ke plainteks: Menggunakan tabel konversi
- Plainteks (hasil)

2. Pengembangan implementasi
   Implementasikan masing-masing metode kriptografi menggunakan Bahasa Pemrograman *Python* agar lebih mudah dalam melakukan proses perbandingan. Pada program menggunakan 4 jenis *liblary* yaitu pengunaan *matplotlib* yang bertujuan untuk membuat graf, *random* yang bertujuan untuk membuat nilai acak pada kata kunci, *time* yang digunakan untuk mencatat waktu mulai dan waktu selesai program agar dapat mengetahui waktu yang digunakan, dan *os* yang bertujuan untuk membaca, dan mencatat *file* plainteks dan hasil dari program yang dijalankan.
3. Menentukan plainteks
   Menyiapkan plainteks yang digunakan. Plainteks harus berisi minimal 1 huruf besar, 1 huruf kecil, 1 angka, dan 1 simbol "Tahanan No 148 akan dipindahkan pada tanggal 17 Januari 2026 bertepatan pada bulan purnama."
4. Proses enkripsi
   Lakukan enkripsi terhadap data menggunakan metode kriptografi yang telah diimplementasikan. Catat waktu yang diperlukan untuk melakukan enkripsi dan dekripsi dengan setiap metode.
5. Evaluasi enkripsi
   Bandingkan hasil enkripsi dan dekripsi dari kedua metode kriptografi. Tinjau kecepatan, keamanan, dan efektivitas enkripsi dan dekripsi dari masing-masing metode.
6. Analisis hasil
   Analisis perbandingan antara kedua metode kriptografi berdasarkan hasil evaluasi. Identifikasi kelebihan dan kekurangan dari masing-masing metode.

HASIL DAN PEMBAHASAN

Dari penelitian ini, dihasilkan dua buah metode, yaitu metode 1 dan metode 2, yang menggunakan persamaan matematis (*equation*). Kedua metode ini dibandingkan berdasarkan 3 aspek yakni, dari segi keamanan, efisiensi metode, dan kualitas enkripsi dan dekripsi.

Enkripsi metode 1

1. Konversi nilai plainteks menjadi bit, bagi menjadi 2 sub kata kode, lalu tambahkan 1 bit pada sub kata kode kanan dan hitung nilai keduanya diman

Plainteks	Nilai	Kata Kode	Sub Kata Kode Kiri	Sub Kata Kode Kanan	Hasil Enkripsi
T	20	0010100	001	10100	1,20
a	27	0011011	001	11011	1,27
h	34	0100010	010	10010	2,18
a	27	0011011	001	11011	1,27
n	40	0101000	010	11000	2,24
a	27	0011011	001	11011	1,27
n	40	0101000	010	11000	2,24
			...		
.	76	1001100	100	11100	4,28

2. Membuat matriks

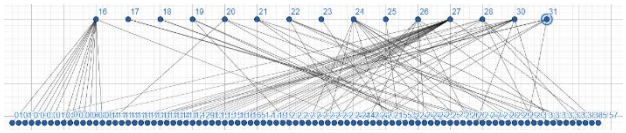
Tabel 2. Tabel Matriks Metode 1

	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111
000	SP(0,16)														8(0,30)	
001					T(1,20)							a(1,27)	b(1,28)		D(1,30)	E(1,31)
010		g(2,17)	h(2,18)	i(2,19)		k(2,21)	l(2,22)	m(2,23)	n(2,24)	o(2,25)	p(2,26)		r(2,28)		t(2,30)	u(2,31)
011						1(3,21)	2(3,22)		4(3,24)		6(3,26)	7(3,27)	8(3,28)		0(3,30)	
100													(4,28)			
101																
110																
111																

3. Menentukan dan memasukan kata kunci pada nilai sub kata kode kiri lalu melakukan proses pengacakan

(019,16), (0101,16), (0128,16), (0145,16), (0136,16), (0111,16), (014,16), (015,30), (082,16), (087,16), (027,16), (037,16), (060,16), (067,16), (11,20), (110,27), (1112,28), (1114,31), (2116,28), (2117,30), (1119,31), (1122,27), (1125,27), (1133,30), (1131,27), (1134,27), (1137,28), (1141,27), (1153,27), (1156,27), (12,27), (129,27), (133,27), (139,30), (150,30), (151,27), (156,27), (162,27), (164,30), (165,27), (177,27), (191,27), (196,27), (17,27), (212,24), (241,19), (244,26), (2120,26), (2124,30), (2100,19), (2127,24), (2129,26), (2139,31), (2140,22), (2143,24), (2146,26), (2148,31), (2150,28), (2151,24), (2155,23), (217,25), (230,21), (235,24), (246,19), (248,24), (25,18), (254,18), (255,21), (258,24), (261,26), (269,30), (170,27), (272,24), (274,17), (276,17), (279,22), (289,20), (29,24), (293,24), (294,31), (297,28), (3103,22), (3105,30), (3108,22), (3110,26), (322,21), (324,24), (325,28), (384,21), (385,27), (4157,28)

4. Membuat graf



Gambar 1. Graf Bipartit Pada Metode 1

Dekripsi metode 1

1. Mengubah graf menjadi nilai dengan menentukan urutan sesuai dengan kata kunci dari yang terkecil ke terbesar dan menghilangkan kata kunci pada nilai sub kata kode kiri

(1,20)	(1,27)	(2,18)	(1,27)	(2,24)
(1,27)	(2,24)	(0,16)	(0,30)	(2,25)
(0,16)	(3,21)	(3,24)	(3,28)	(0,16)
(1,27)	(2,21)	(1,27)	(2,24)	(0,16)
(1,30)	(2,19)	(2,26)	(2,19)	(2,24)
(1,30)	(1,27)	(2,18)	(2,21)	(1,27)
(2,24)	(0,16)	(2,26)	(1,27)	(1,30)
(1,27)	(0,16)	(2,30)	(1,27)	(2,24)
(2,17)	(2,17)	(1,27)	(2,22)	(0,16)
(3,21)	(3,27)	(0,16)	(2,20)	(1,27)
(2,24)	(2,31)	(1,27)	(2,28)	(2,19)
(0,16)	(3,22)	(3,30)	(3,22)	(3,26)
(0,16)	(1,28)	(1,31)	(2,28)	(2,30)
(1,31)	(2,26)	(1,27)	(2,30)	(1,27)
(2,24)	(0,16)	(2,26)	(1,27)	(1,30)
(1,27)	(0,16)	(1,28)	(2,31)	(2,22)
(1,27)	(2,24)	(0,16)	(2,26)	(2,31)
(2,28)	(2,24)	(1,27)	(2,23)	(1,27)
(4,28)				

2. Konversi hasil enkripsi menjadi bit, kurangi 1 bit pada sub kata kode kanan, gabungkan kedua sub kata kode, dan ubah menjadi nilai

Hasil Enkripsi	Kata Kode	Nilai	Hasil Dekripsi
1,20	0010100	20	T
1,27	0011011	27	a
2,18	0100010	34	h
1,27	0011011	27	a
2,24	0101000	40	n
1,27	0011011	27	a
2,24	0101000	40	n
...			
4,28	1001100	75	.

3. Plainteks (Hasil)
   Tahanan No 148 akan dipindahkan pada tanggal 17 Januari 2026 bertepatan pada bulan purnama.

Enkripsi metode 2

1. Konversi nilai plainteks menjadi bit, bagi menjadi 2 sub kata kode, lalu tambahkan 1 bit pada sub kata kode kanan dan hitung nilai keduanya

Plainteks	Nilai	Kata Kode	Sub Kata Kode Kiri	Sub Kata Kode Kanan	Hasil Enkripsi
T	20	0010100	001	10100	1,20
a	27	0011011	001	11011	1,27
h	34	0100010	010	10010	2,18
a	27	0011011	001	11011	1,27
n	40	0101000	010	11000	2,24
a	27	0011011	001	11011	1,27
n	40	0101000	010	11000	2,24
			...		
.	76	1001100	100	11100	4,28

2. Membuat matriks

Tabel 3. Tabel Matriks Metode 2

	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001	11010	11011	11100	11101	11110	11111
000																
001					T(1,20)							a(1,27)	h(1,28)		T(1,30)	T(1,31)
010		a(2,17)	h(2,18)	a(2,19)		h(2,21)	h(2,22)	a(2,23)	a(2,24)	a(2,25)	a(2,26)		a(2,28)		a(2,30)	a(2,31)
011						3(3,21)	2(3,22)		4(3,24)		6(3,26)	7(3,27)	8(3,28)		0(3,30)	
100													(4,28)			
101																
110																
111																

3. Menentukan dan mengalikan kata kunci dengan 2 serta Melakukan penjumlahan pada kata kunci dengan sub kata kode kanan

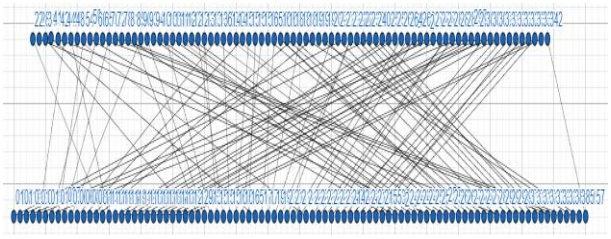
Hasil Enkripsi	Sub Kata Kode Kanan		Hasil Perkalian	Hasil Perkalian Enkripsi
1,20	20	+	2	1,22
1,27	27	+	4	1,31
2,18	18	+	10	2,28
1,27	27	+	14	1,41
2,24	24	+	18	2,42
1,27	27	+	14	1,47
2,24	24	+	18	2,48
...				
4,28	28	+	314	4,342

4. Memasukan hasil perkalian kata kunci pada nilai sub kata kode kiri lalu melakukan proses pengacakan

(0111,238)	(0101,218)	(0128,272)
(0136,288)	(014,44)	(0145,306
(015,60)	(019,54)	(027,70)
(037,90)	(060,136)	(067,150)
(082,180)	(087,190)	(11,22)
(110,47)	(1112,252)	(1114,259)
(1119,269)	(1122,271)	(1125,277)
(1131,289)	(1133,296)	(1134,295)
(1137,302)	(1141,309)	(1153,333)
(1156,339)	(12,31)	(129,85)
(133,93)	(139,108)	(150,130)

(151,129) (156,139) (162,151)
(164,158) (165,157) (17,41)
(170,167) (177,181) (191,209)
(196,219) (25,28) (29,42)
(212,48) (217,59) (230,81)
(235,94) (241,101) (244,114)
(246,111) (248,120) (254,126)
(255,131) (258,140) (261,148)
(269,168) (272,168) (274,165)
(276,169) (279,180) (289,198)
(293,210) (294,219) (297,222)
(2100,219) (2116,260) (2117,264)
(2120,266) (2124,278) (2127,278)
(2129,284) (2139,309) (2140,302)
(2143,310) (2146,318) (2148,327)
(2150,328) (2151,326) (2155,333)
(322,65) (324,72) (325,78)
(384,189) (385,197) (3103,228)
(3105,240) (3108,238) (3110,246)
(4157,342)

5. Membuat Graf



Gambar 2. Graf Bipartit Pada Metode 2

Dekripsi metode 2

1. Mengubah graf menjadi nilai dengan menentukan urutan sesuai dengan kata kunci dari yang terkecil ke terbesar dan menghilangkan kata kunci pada nilai sub kata kode kiri

(1,22), (1,31), (2,28), (1,41), (2,42), (1,47), (2,48), (0,44), (0,60), (2,59), (0,54), (3,65), (3,72), (3,78), (0,70), (1,85), (2,81), (1,93), (2,94), (0,90), (1,108), (2,101), (2,114), (2,111), (2,120), (1,130), (1,129), (2,126), (2,131), (1,139), (2,140), (0,136), (2,148), (1,151), (1,158), (1,157) , (0,150), (2,168), (1,167), (2,168), (2,165), (2,169), (1,181), (2,180), (0,180), (3,189), (3,197), (0,190), (2,198), (1,209), (2,210), (2,219), (1,219), (2,222), (2,219), (0,218), (3,228), (3,240), (3,238), (3,246), (0,238), (1,252), (1,259), (2,260), (2,264), (1,269), (2,266), (1,271), (2,278), (1,277), (2,278), (0,272), (2,284), (1,289), (1,296), (1,295), (0,288), (1,302), (2,309), (2,302), (1,309), (2,310), (0,306), (2,318), (2,327), (2,328), (2,326), (1,333), (2,333), (1,339), (4,342)

2. Kalikan kata kunci dengan 2, kurangi sub kata kode kanan dengan hasil perkalian kata kunci, konversi hasilnya menjadi bit, kurangi 1 bit pada sub kata kode kanan, gabungkan kedua sub kata kode, dan ubah menjadi nilai

Hasil Perkalian Dekripsi	Hasil Pengurangan Dekripsi	Kata Kode	Nilai	Hasil Dekripsi
1,22	1,20	0010100	20	T
1,31	1,27	0011011	27	a
2,28	2,18	0100010	34	h
1,41	1,27	0011011	27	a
2,42	2,24	0101000	40	n
1,47	1,27	0011011	27	a
2,48	2,24	0101000	40	n
...				
4,342	4,28	1001100	75	.

3. Hasil

Tahanan No 148 akan dipindahkan pada tanggal 17 Januari 2026 bertepatan pada bulan purnama.

Penelitian ini menggunakan program dengan menggunakan Bahasa Pemrograman *Python* dan dijalankan menggunakan *Visual Studio Code.* Program ini dirancang untuk melakukan proses enkripsi sederhana dengan langkah-langkah yang jelas dan terstruktur. Berikut adalah rincian isi dan langkah-langkah dari program yang digunakan.

```
def enkripsi(plainteks):
    waktu_mulai = time.time()  # Waktu mulai proses enkripsi
    nilai_acak = buat_nilai_acak(len(plainteks))
    nilai = plainteks_ke_nilai(plainteks)
    bit_7 = nilai_ke_7bit(nilai)
    bit_kiri, bit_kanan = bagi_bit(bit_7)

    hasil_enkripsi = []
    for i in range(len(bit_kiri)):
        bit_kanan_decimal = int(bit_kanan[i], 2)
        bit_kiri_decimal = int(bit_kiri[i], 2)
        nilai_gabungan = str(bit_kiri_decimal) + str(nilai_acak[i])
        hasil_enkripsi.append((nilai_gabungan, bit_kanan_decimal + 16))

    waktu_selesai = time.time()  # Waktu selesai proses enkripsi
    waktu_proses = waktu_selesai - waktu_mulai  # Menghitung durasi proses enkripsi
```

Gambar 3. Program pada Metode 1

1. Enkripsi metode 1

Ketika kita menjalankan program tersebut menghasilkan sebagai berikut:

[(13,20);(15,27);(26,18);(17,27);(211,24);(114,27);(217,24);(022,16);(027,30);(228,25);(031,16);(335,21);(337,24);(341,28);(042,16);(144,27);(248,21);(153,27);(255,24);(060,16);(163,30);(264,19);(267,26);(270,19);(274,24);(175,30);(180,27);(284,18);(286,21);(190,27);(294,24);(097,16);(298,26);(1102,27);(1106,30);(1108,27);(0111,16);(2116,30);(1121,27);(2123,24);(2126,17);(2127,17);(1131,27);(2133,22);(0134,16);(3135,21);(3136,27);(0137,16);(0142,26);(1143,27);(2146,24);(2148,

31);(1150,27);(2153,28);(2158,19);(0160,16);(3164,22);(3168,30);(3171,22);(3174,26);(0177,16);(1182,28);(1185,31);(2190,28);(2194,30);(1195,31);(2199,26);(1202,27);(2205,30);(1209,27);(2214,24);(0219,16);(2222,26);(1223,27);(1227,30);(1229,27);(0232,16);(1233,28);(2234,31);(2239,22);(1243,27);(2246,24);(0249,16);(2250,26);(2252,31);(2256,28);(2259,24);(1262,27);(2264,23);(1265,27);(4269,28);]

Waktu proses enkripsi: 0.0468802452087402 detik

2. Enkripsi metode 2

   Ketika kita menjalankan program tersebut menghasilkan sebagai berikut:

   [(15,30);(18,43);(29,36);(114,55);(217,58);(118,63);(219,62);(024,64);(028,86);(233,91);(038,92);(340,101);(341,106);(344,116);(048,112);(151,129);(254,129);(159,145);(262,148);(064,144);(168,166);(271,161);(276,178);(278,175);(281,186);(186,202);(190,207);(291,200);(292,205);(196,219);(2101,226);(0106,228);(2110,246);(1114,255);(1117,264);(1119,265);(0121,258);(2126,282);(1131,289);(2134,292);(2138,293);(2139,295);(1143,313);(2147,316);(0149,314);(3153,327);(3158,343);(0163,342);(0166,358);(1169,365);(2174,372);(2176,383);(1179,385);(2181,390);(2182,383);(0186,388);(3191,404);(3194,418);(3199,420);(3200,426);(0202,420);(1206,440);(1207,445);(2211,450);(2216,462);(1221,473);(2223,472);(1228,483);(2232,494);(1236,499);(2239,502);(0242,500);(2244,514);(1248,523);(1253,536);(1256,539);(0260,536);(1261,550);(2264,559);(2268,558);(1272,571);(2274,572);(0279,574);(2284,594);(2285,601);(2288,604);(2290,604);(1292,611);(2295,613);(1298,623);(4303,634);]

   Waktu proses enkripsi: 0.0468821525573730 detik

```python
def decrypt(hasil_enkripsi):
    waktu_mulai = time.time()  # Waktu mulai proses dekripsi

    plainteks = ""
    for bit_kiri_decimal, kata_kunci, bit_kanan_decimal in hasil_enkripsi:
        bit_kiri = bin(bit_kiri_decimal)[2:].zfill(3)
        bit_kanan = bin(bit_kanan_decimal - 16)[2:].zfill(4)
        nilai_bit = bit_kiri + bit_kanan
        nilai_decimal = int(nilai_bit, 2)
        if nilai_decimal in tabel_konversi.values():
            plainteks += list(tabel_konversi.keys())[list(tabel_konversi.values()).index(nilai_decimal)]
        else:
            plainteks += '?'

    waktu_selesai = time.time()  # Waktu selesai proses dekripsi
    waktu_proses = waktu_selesai - waktu_mulai  # Menghitung durasi proses dekripsi

    return plainteks, waktu_proses
```

Gambar 4. Program Pada Metode 2

3. Dekripsi metode 1

   Ketika kita menjalankan program tersebut menghasilkan sebagai berikut:

   Tahanan No 148 akan dipindahkan pada tanggal 17 Januari 2026 bertepatan pada bulan purnama.

   Waktu proses dekripsi:

   0.015622854232788085937500000000000000000000000000000 detik

4. Dekripsi metode 2

   Ketika kita menjalankan program tersebut menghasilkan sebagai berikut:

   Tahanan No 148 akan dipindahkan pada tanggal 17 Januari 2026 bertepatan pada bulan purnama.

   Waktu proses dekripsi:

   0.593800067901611328125000000000000000000000000000000 detik

Penelitian ini juga menggunakan plainteks lain berupa novel untuk mencari tau seberapa banyak plainteks yang dapat dijalankan pada program metode 1 dan metode 2. Novel yang digunakan memiliki 406.450 karakter termasuk huruf, angka, spasi, dan enter sehingga pada saat dijalankan, peneliti memperoleh waktu yang dibutuhkan untuk melakukan proses enkripsi metode 1 yaitu 2,797 detik dan untuk melakukan proses dekripsi yaitu 6,453 detik. Sedangkan waktu yang dibutuhkan dalam menjalankan program enkripsi metode 2 yaitu 2,8596 detik dan waktu yang dibutuhkan dalam menjalankan proses dekripsi yaitu 6,4848 detik. Dari percobaan di atas, juga tidak terdapat kesalahan karena ketika dilakukan dekripsi pada hasil enkripsi untuk masing-masing metode, semua cipherteks berhasil terdekripsi menjadi plainteks.

PENUTUP

SIMPULAN

Berdasarkan pembahasan dan percobaan yang telah dilakukan, kesimpulan dari percobaan menunjukan bahwa pada kedua metode enkripsi menggunakan algoritma simetris dengan kata kunci yang sama, pada metode 1 lebih cepat dan memiliki algoritma yang sederhana, namun memiliki batas 16 simpul dan keamanan rendah. Sebaliknya, pada metode 2 algoritmanya lebih komplek, dalam segi waktu memerlukan waktu yang lebih lama, tetapi pada segi keamanan lebih unggul. Secara keseluruhan metode 1 dapat diterapkan pada data yang tidak bersifat sensitif dan singkat, sedangkan pada metode dapat diterapkan pada data yang bersifat sensitif dan rahasia.

SARAN

Menggunakan satu teknik kriptografi saja sudah baik, namun lebih optimal jika kita mengombinasikannya dengan beberapa metode kriptografi untuk meningkatkan tingkat keamanannya. Akan tetapi, kita juga harus

memperhatikan efisiensi dari teknik tersebut dengan melihat waktu pengerjaannya. Jika teknik tersebut memerlukan waktu yang lama, maka teknik tersebut kurang efisien untuk digunakan, terutama jika diterapkan pada masalah yang membutuhkan respon cepat seperti perbankan dan aplikasi pesan instan.

DAFTAR PUSTAKA

Amos, R. O., 2020. *Cryptography Arithmetic Algorithms and Hardware Architectures*. *Advances in Information Security* (Vol. 77). Retrieved from http://www.springer.com/series/5576

Deby, E., dan Dewi, D., 2021. Aplikasi Matrik Pada Ilmu Kriptografi Dengan Menggunakan Matlab. doi:10.35134/komtekinfo.v7i4

Frode, W., dan Sandy, Z., 2019. *German Mathematicians and Cryptology in WWII*.

Ghazaly, A., 2023. Makalah IF2120 Matematika Diskrit-Sem. I Tahun. doi:10.1007/978-981

Hani'ah, Z., Ika, H. A., Kusbidiono., dan Dafik., 2021. Analisa Antimagic Total Covering Super pada Eksponensial Graf Khusus dan Aplikasinya dalam Mengembangkan Chipertext. *CGANT JOURNAL OF MATHEMATICS AND APPLICATIONS*, *2*(1). doi:10.25037/cgantjma.v2i1.52

Hidayatuloh, K., Yustantina, Y., dan Kusmadi, K., 2021. Perbandingan Metode Stream Cipher Dan Hill Cipher Dalam Keamanan Data. *Infotronik : Jurnal Teknologi Informasi Dan Elektronika*, *6*(1), 27. doi:10.32897/infotronik.2021.6.1.647

Hongbo, L., Yan, W., Yanzhi, R., dan Yingying, C., 2021. *Bipartite graph matching based secret key generation*. In *Proceedings - IEEE INFOCOM* (Vol. 2021-May). Institute of Electrical and Electronics Engineers Inc. doi:10.1109/INFOCOM42981.2021.9488848

Ni, B., Qazi, R., Rehman, S. U., dan Farid, G., 2021. Some Graph-Based Encryption Schemes. *Journal of Mathematics*, *2021*. doi:10.1155/2021/6614172

Ni, P., 2020. Pemanfaatan Teknologi Kriptografi Dalam Mengatasi Kejahatan Cyber. *Satya Dharma: Jurnal Ilmu Hukum*, *3*(2). Retrieved from https://ejournal.iahntp.ac.id/index.php/satya-dhamat

Suriadi, R., Satra, R., dan Fattah, F., 2020. Peningkatan Keamanan Data dengan Menggunakan Equation pada Metode Playfair Cipher, *1*(1), 266–269.

Watrianthos, R. (2021). Perbandingan Teknik Kriptografi Metode Sapphire II Dan RC4. *Jurnal Ilmiah AMIK Labuhan Batu*, *3*(2).

Yukai Zang., 2019. *Rainbow Tables.*