Halaman jurnal: http://jurnal.yudharta.ac.id/v2/index.php/EXPLORE-IT/

Explore IT!
JURNAL KEILMUAN DAN APLIKASI TEKNIK INFORMATIKA

Akreditasi Sinta 5 (S5) – SK No. 36/E/KPT/2019
p-ISSN 2086-3489 (Print)- e-ISSN 2549-354X (Online)
DOI https://doi.org/10.35891/explorit

Analisis Perbandingan Algoritma *Monoalphabetic cipher* dan *Polyalphabetic substitution cipher* Pada Sistem Keamanan Data

Nuke Sephiana[1], Muhlis Tahir[2], Shinta Dwi Wulandari[3], Faizal Reza Rahmansyah[4], Rofikoh Nabila Nuvitasari[5], Ray Albian Prakasa[6]

[1,2,3,4,5,6] *Pendidikan Informatika, Universitas Trunojoyo Madura, Bangkalan, Indonesia*

email: 190631100035@student.trunojoyo.ac.id[1)], muhlis.tahir@trunojoyo.ac.id[2)] , 190631100039@student.trunojoyo.ac.id[3)], 190631100047@student.trunojoyo.ac.id[4)], 190631100066@student.trunojoyo.ac.id[5)], 190631100044@student.trunojoyo.ac.id[6)]

INFO ARTIKEL

Sejarah Artikel:
Diterima 13 Mei 2023
Direvisi 16 Juni 2023
Disetujui 18 Juni 2023
Dipublikasi 20 Juni 2023

Katakunci:
Kriptografi
Chipper substitusi
Monoalphabetic cipher
Polyalphabetic substitution cipher

ABSTRAK

Pada era menuju perkembangan revolusi industri 5.0, Teknologi informasi dan komunikasi telah menjadi elemen terpenting dalam kehidupan manusia. Sehingga pemanfaatan suatu teknologi informasi dan komunikasi dalam bidang keamanan mampu diterapkan di mana saja, salah satunya pada keamanan data. Ilmu keamanan data disebut dengan kriptografi. Pada penelitian ini, penulis akan menganalisis dua jenis cipher substitusi pada suatu kriptografi klasik, yakni polyalphabetic substitution cipher dan Monoalphabetic cipher. Tujuan dari dilakukannya penelitian ini bermaksud untuk memberikan informasi tentang algoritma polyalphabetic substitution cipher (cipher abjad tunggal) dan Monoalphabetic substitution cipher (cipher abjad majemuk), serta untuk membandingkan kedua metode algoritma kriptografi untuk dapat diketahui penggunaan yang lebih efektif dan efisien untuk menjaga keamanan data. Metode penelitian ini berupa studi literatur menggunakan pendekatan kualitatif dengan teknik pengumpulan data berbentuk catatan, buku, makalah atau artikel, dan jurnal. Hasil analisis yang diperoleh pada uji coba algoritma monoalphabetic cipher dan polyalphabetic cipher yaitu algoritma polyalphabetic cipher lebih sulit dipecahkan karena algoritma lebih panjang. Pada algoritma polyalphabetic cipher, plaintext yang sama didekripsi dengan kunci yang berbeda dan menghasilkan ciphertext yang berbeda, sehingga sulit untuk menggunakan metode tebakan untuk menerjemahkan pesan. Sedangkan pada algoritma monoalphabetic cipher menggunakan analisis frekuensi huruf, sehingga mudah didekripsi mengunakan metode tebakan. Sehingga algoritma kriptografi polyalphabetic cipher efektif dan efisien dalam keamanan data.

Keyword:
Cryptography
Substitution cipher
Monoalphabetic cipher
Polyalphabetic substitution cipher

DOI Artikel:
10.35891/explorit.v15i1.3823

ABSTRACT

In the era leading to the development of the industrial revolution 5.0, information and communication technology has become the most important element in human life. So that the use of information and communication technology in the field of security can be applied anywhere, one of which is data security. The science of data security is called cryptography. In this study, the authors will analyze two types of substitution ciphers in classical cryptography, namely polyalphabetic substitution ciphers and monoalphabetic ciphers. The purpose of this research is to provide information about the polyalphabetic substitution cipher algorithm (single alphabetic cipher) and the Monoalphabetic substitution cipher (multiple alphabetic cipher), as well as to compare the two cryptographic algorithm methods to find out which is more effective and efficient to use to maintain data security. This research method is a literature study using a qualitative approach with data collection techniques in the form of notes, books, papers or articles, and journals. The results of the analysis obtained in the trial of the monoalphabetic cipher algorithm and the polyalphabetic cipher are that the polyalphabetic cipher algorithm is more difficult to solve because the algorithm is longer. In the polyalphabetic cipher algorithm, the same plaintext is decrypted with different keys and produces different ciphertexts, making it difficult to use the guessing method to translate messages. Whereas the monoalphabetic cipher algorithm uses letter frequency analysis, so it is easily decrypted using the guessing method. So that the polyalphabetic cipher cryptographic algorithm is effective and efficient in data security.

1. Pendahuluan

Pada era menuju perkembangan revolusi industri 5.0, Teknologi Informasi dan Komunikasi (TIK) berkembang secara signifikan dan telah menjadi elemen penting dalam kehidupan manusia. Perkembangan TIK menjadikan sumbangsih besar tehadap peradaban dari masa ke masa. TIK dapat diartikan sebagai penerapan pengetahuan dan keterampilan yang dilakukan seseorang untuk menyampaikan informasi dengan memanfaatkan perangkat komputer sebagai alat untuk, menyajikan dan mengolah data informasi [1]. Pemanfaatan TIK dapat diimplementasikan dalam banyak bidang, salah satunya pada bidang keamanan.

Pemanfaatan TIK pada bidang keamanan dapat diterapkan di mana saja, salah satunya pada keamanan data. Pada era sekarang penyimpanan dan pengiriman data telah dilakukan dengan efektif dan efisien. Data yang sebelumnya tersimpan di media elektronik seperti *flash disk* akan lebih mudah disimpan pada media yang terhubung internet. Namun keamanan data harus tetap memerlukan penanganan agar dapat terhindar dari resiko yang membahayakan. Oleh karea itu dilakukan penyandian untuk dapat mengamankan data.

Proses penyandian data disebut enkripsi. Sementara itu, mengembalikan data ke keadaan semula disebut dekripsi. Proses enkripsi merupakan suatu proses dalam mengubah teks asli yang berupa *plaintext* menjadi teks sandi yang berupa *ciphertext*. Sedangkan proses dekripsi merupakan proses mengubah teks sandi (*ciphertext*) menjadi teks asli (*plaintext*). Pada tahap proses enkripsi dan deskripsi, diperlukan suatu algoritma yang disebut dengan kriptografi.

Ilmu keamanan data lebih dikenal dengan nama lain yaitu kriptografi. Kriptografi adalah ilmu yang mempelajari proses pengamanan data dengan membuatnya tidak dapat dipahami oleh pengguna [2]. Kriptografi terus berkembang dalam berbagai hal dari waktu ke waktu. Namun, ketika kriptografi pertama kali ditemukan, ada dua jenis, yakni kriptografi klasik dan juga kriptografi modern. Kriptografi klasik merupakan suatu bentuk kriptografi dengan basis identifikasinya menggunakan karakter. Sedangkan kriptografi modern adalah kriptografi berbasis bit. Kriptografi klasik dan modern akan menggunakan pengkodean *plaintext* menjadi *ciphertext* yang dikenal sebagai *cipher*.

Kriptografi klasik dan kriptografi modern memiliki *cipher* yang berbeda. Pada kriptografi klasik, *cipher* diklasifikasikan menjadi 2, yakni *cipher* substitusi atau lebih dikenal dengan nama *substitution cipher* dan *cipher* transposisi atau dikenal dengan nama *transposition cipher*. Sedangk an pada kriptografi modern, *cipher* juga diklasifikasikan menjadi 2, yakni kriptografi kunci simtetris (cipher substitusi dan cipher transposisi) dan kriptografi kunci asimetris (*encryption standard* dan *advanced encryption system*). Algoritma kriptografi klasik memberikan konsep dasar untuk memahami kriptografi dan berfungsi sebagai dasar algoritma kriptografi modern [3].

Kriptografi pada saat ini dimulai dengan kriptografi klasik kemudian dikembangkan lebih lanjut sehingga lebih rumit untuk diimplementasikan dengan kebutuhan berbeda. Awal mula kriptografi klasi *cipher* subtitusi, masih bersifat sederhana dan mudah untuk diprediksi. Dengan berkembangnya peradaban modern, *cipher* subtitusi menjadi semakin rumit sehingga lebih sulit untuk diretas.

Cipher substitusi (*substitution cipher*) adalah bagian mendasar dari *cipher* klasik. *Cipher* Substitusi adalah suatu bentuk dari algoritma kriptografi dimana bentuk ini akan mengubah setiap unit pada *plaintext* menjadi bentuk unit *ciphertext*. Satu unit dapat diartikan sebagai satu karakter, sepasang karakter atau sekelompok lebih dari dua karakter [4]. Dua jenis *substitution cipher* dalam kriptografi klasik adalah *Monoalphabetic cipher* (*cipher* abjad tunggal) dan *polyalphabetic substitution cipher* (*cipher* abjad majemuk). *Monoalphabetic cipher* (*cipher* abjad tunggal) adalah teknik *substitution cipher* yang merubah bentuk setiap karakter pada *plaintext* dengan karakter yang berbeda pada *ciphertext*, dan mengganti karakter yang sama pada *plaintext* dengan karakter yang sama pada *ciphertext* [5]. Untuk membuat pola enkripsi dengan mudah diketahui karena disebabkan oleh teks pada *ciphertext* harus sesuai dengan teks pada *plaintext*.

Polyalphabetic substitusi cipher (*cipher* abjad majemuk) adalah teknik *substitution cipher* dengan mengganti setiap karakter pada *plaintext* menjadi karakter yang berbeda pada *ciphertext*, tergantung kunci yang digunakan. Contoh *polyalphabetic substitution* adalah *vigenere cipher*. Enkripsi teks yang sama dapat menghasilkan teks yang berbeda sehingga akan lebih sulit untuk menemukan polanya. Kunci pengkodean *polyalphabetic substitution cipher (cipher* abjad majemuk) bisa berbeda, sehingga memiliki lebih banyak kemungkinan kombinasi lebih bervariasi dan lebih sulit diselesaikan [6]. Algoritma klasik subtitusi *cipher* pada abjad tunggal memang mudah dipecahkan, tetapi tidak semudah *cipher* abjad majemuk yang mana tiap karakter harus diganti dengan karakter yang sama, sedangkan dengan *cipher* abjad tunggal setelah enkripsi selesai, karakter diganti dengan karakter yang berbeda [7].

Penelitian sebelumnya telah dibahas terkait analisis perbandingan algoritma kriptografi klasik "*vigenere cipher"* dan *"one time pad"* [8]. Penelitian tersebut menjelaskan bahwa proses enkripsi dan dekripsi dua metode ini tampak sama, akan tetap masih ada perbedaan. Penelitian lain dengan judul "Perbandingan Kriptografi Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher". Perbandingan tersebut memberikan pemahaman konsep algoritma kriptografi klasik untuk memahami kriptografi modern [9]. Oleh karena itu peneliti akan menganalis jenis "*polyalphabetic substitution cipher"* dan *"Monoalphabetic substitution cipher*" untuk mengetahui persamaan dan perbedaan kedua jenis cipher tersebut. Pada penelitian ini akan menganalis tentang dua jenis *substitution cipher* pada kriptografi klasik yakni *polyalphabetic substitution cipher* dan *Monoalphabetic cipher*. Penelitian ini diambil agar dapat memberikan informasi terkait algoritma *polyalphabetic substitution cipher* (cipher abjad tunggal) dan *Monoalphabetic substitution cipher* (cipher abjad majemuk), serta untuk mengetahui perbandingan kedua metode dari algoritma kriptografi untuk menjaga keamanan data. Diharapkan penelitian ini dapat memberikan pengetahuan tentang kriptografi, khususnya *polyalphabetic substitution cipher* dan *Monoalphabetic substitution cipher* untuk menjaga kerahasiaan data.

2. Kajian Teori

2.1 Konsep Algoritma

Algoritma merupakan inti dari ilmu komputer[13]. Istilah algoritma banyak disebut sebagai cabang ilmu komputer. Namun, jangan berasumsi bahwa algoritma akan selalu identik dengan ilmu komputer. Instruksi algoritma mencakup banyak proses, seperti cara menyiapkan kue atau hidangan lainnya. Selalu ada urutan dalam sebuah resep, seperti langkah-langkah memasak. Jika langkahnya tidak logis, Anda tidak bisa membuat hidangan yang diinginkan. Secara umum. Pihak-pihak (objek) yang melakukan proses disebut (prosesor). Pemroses kemudian dapat berupa manusia, komputer, robot, atau perangkat elektronik lainnya. Prosesor menjalankan proses dan kemudian berjalan normal sesuai dengan algoritma yang ada. Itu mengeksekusi langkah-langkah dalam algoritma. Prosesor mengikuti algoritma, seperti koki yang membuat suatu masakan menurut buku resep yang telah disusun dan diberikan kepadanya, seperti pianis yang memainkan lagu di papan catur. Oleh sebab itu, suatu bentuk algoritma harus mengekspresikannya kedalam bentuk yang mudah dipahami oleh prosesor (baik itu manusia, komputer, atau perangkat lain).

2.2 Konsep Kriptografi

Pada bahasa Yunani cryptos dan graphia, yang berarti "tulisan rahasia" sehingga ini merupakan bentuk mendasar Kriptografi. Kriptografi suatu ilmu yang mempelajari tentang cara mengirimkan teks yang ditransfer oleh pengirim kepada penerima melewati jalur yang aman. Kriptografi bertujuan untuk melindungi kerahasiaan informasi yang dimasukkan ke dalam data sehingga pihak lain tidak dapat mengakses informasi tersebut. Pengembang algoritma kriptografi disebut *cryptographers*.

2.3 Tujuan Kriptografi

Kriptografi adalah ilmu dalam teknik matematika diaman ilmu ini berkaitan dengan aspek keamanan . Berikut 4 aspek tujuan dasar dari kriptografi [13].

1. Kerahasiaan (*confidentiality*)
   Privasi adalah sebuah layanan untuk menjaga data penting dari pihak manapun yang tidak memiliki akses ke sana. Berkenaan dengan hal tersebut, data ini tentu saja hanya para pihak berwenang yang bisa mengakses. Demikian, data yang tersimpan akan terjaga kerahasiaannya dari pihak mana saja baik itu situs, *hacker*, dan lain sebagainya.
2. Integritas Data (*data integrity*)
   Integritas data adalah sebagai layanan untuk menyimpan informasi dari sesorang yang tidak berwenang. Wajib dipastikan bahwa sistem informasi dapat menemukan manipulasi/kecurangan data. Dalam hal ini, kecurangan data yang disebutkan disini termasuk menyisipkan, menghapus atau mengganti data.
3. Autentikasi (*authentication*),
   Autentifikasi adalah layanan untuk mengidentifikasi terhadap pihak-pihak yang berkepentingan untuk mengakses keaslian data dalam suatu sistem informasi.

4. Ketiadaan penyangkalan (*nonrepudiation*)
   Ketiadaan penyangkalan adalah berfungsi sebagai layanan yang digunakan untuk mencegah penolakan yang diambil oleh seseorang yang tidak berwenang di sistem informasi tersebut.

2.4 *Monoalphabetic Cipher*

Monoalphabetic merupakan suatu teknik dalam menemukan cipher substitusi dengan mengganti karakter pada *plaintext* dengan karakter lain dalam *ciphertext* [3]. Huruf yang sama dalam *plaintext* dapat memiliki huruf pengganti yang sama juga dalam *ciphertext*. Pada contoh Caesar cipher berikut, huruf A pada *plaintext* akan digantikan menggunakan huruf D pada *ciphertext*. Hal tersebut didasarkan oleh adanya perubahan pergeseran sebanyak 3 baris pada *ciphertext* sehingga merubah A menjadi D. Sebuah alternatif lain dari sandi tabel tunggal adalah ROT13, yang menggantikan setiap huruf dalam teks biasa dengan huruf yang berjarak 13 tempat darinya. Hal tersebut didasarkan oleh hubungan antara *plaintext* dan *ciphertext* yang dengan mudah diprediksi karena kedua huruf *plaintext* dan *ciphertext* sering muncul.

2.5 *Polyalphabetic Cipher*

Polyalpabetic Cipher mengenkripsikan sekumpulan karakter pada pesan dalam sebuah proses [4]. Kriptografi *polyalphabetic* adalah improvisasi teknik substitusi *Monoalphabetic cipher*. Cipher substitusi polyalphabetic menerapkan teknik sandi satu huruf satu kali untuk pesan teks biasa. Selain itu, Cipher polyalphabetic membuat teks sandi lebih mudah diretas karena karakter *plaintext* yang memiliki karakter sama tidak dapat dicocokkan dengan karakter yang sama pada *ciphertext*. Kunci enkripsi polyalphabetic kata sandi bisa berbeda, sehingga memiliki lebih banyak variasi dan kemungkinan kombinasi yang lebih sulit terselesaikan. Polyalphabetic *cipher* dijelaskan oleh Leon Battista di 1568. Cara yang digunakan sebagai perluasan dari cara substitusi huruf tunggal. Berdasarkan seperti namanya, algoritma cipher polyalphabetic mengenkripsi satu set karakter atau string karakter melibatkan penggunaan kunci yang berbeda. Algoritma *Polyalphabetic Cipher* meminimalisir penggunaan kunci yang sama, itulah sebabnya enkripsi polialfabetik lebih sulit dipecahkan karena algoritma tersebut tidak hanya lebih panjang daripada algoritme *Monoalphabetic*, namun juga mendekripsi teks biasa yang sama dengan kunci yang berbeda menghasilkan teks sandi yang berbeda.

3. Metodologi Penelitian

Penelitian ini menggunakan jenis *library research* atau penelitian kepustakaan yang mana peneliti bergantung pada berbagai macam literatur yang digunakan sebagai acuan untuk data penelitian dan menggunakan metode kualitatif karena data yang diperoleh bebentuk kata-kata atau deskripsi [10]. Dalam penelitian ini diperlukan buku atau hasil penelitian terdahulu yang dapat peneliti gunakan sebagai referensi. Tujuan penelitian ini untuk membandingkan algoritma *Monoalphabetic cipher* dengan *polyalphabetic subtitution cipher* yang sudah ada sebelumnya maupun yang sedang dibahas. Informasi yang didapatkan bisa melalui sumber yaitu buku, internet, jurnal, atau artikel yang berkaitan dengan penelitian.

Teknik pengumpulan data yang digunakan dalam penelitian ini berupa dokumen yakni menemukan informasi tentang suatu permasalahan atau variabel berbentuk tulisan, buku, makalah atau artikel, dan jurnal [11]. Alat penelitian yang digunakan berupa skema penulisan, dan format catatan, dan daftar kategori bahan penelitian. Teknik pengumpulan data merupakan suatu metode ataupun alat yang berguna dalam mengumpulkan data [12]. Pada penelitian ini jenis teknik pengumpulan data yang digunakan adalah data sekunder. Sumbernya adalah data yang sudah tersedia, jadi kita tinggal mencari dan mengumpulkannya. Untuk mendapatkan data yang benar dan memenuhi tujuan penelitian, kita perlu mempertimbangkan beberapa aspek.

Pada penelitian ini teknik analisis data yang digunakan berupa penyusunan data dan proses pencarian secara sistematis dari berbagai sumber dengan mengkategorikan data dengan tujuan untuk mendapatkan simpulan yang dapat dipahami oleh penulis serta pembaca [12]. Teknik analisis data yang digunakan adalah analisis isi. Analisis isi merupakan teknik yang digunakan untuk memahami teks dan menganalisis teks. Analisis teks diartikan sebagai teknik investigasi dengan mencari gambaran objektif, sistematis, dan kuantitatif. Oleh karena itu, analisis ini berfokus pada perbedaan antara *Monoalphabetic cipher* dengan polyalphabetic subtitution cipher. Analisis tersebut daoat digunakan dalam memperoleh kesimpulan yang benar dan dapat diperiksa kembali maksud dari konteksnya. Analisis ini akan dilakukan dengan proses membandingkan, memilih, menggabungkan, dan memilah makna yang berbeda sehingga ditemukan makna yang relevan [11].

4. Hasil Uji Coba Dan Pembahasan

4.1 Deskripsi Data Uji Coba

1. *Monoalphabetic cipher*

Monoalphabetic cipher atau sering kita sebut dengan cipher abjad-tunggal adalah suatu bentuk kriptografi susbtitusi dimana pada setiap kalimat atau karakter pada huruf *ciphertext* diubah menjadi bentuk yang berbeda pada suatu *ciphertext*. Huruf abjad yang memiliki kesamaan pada suatu karakter plainteks akan diubah menggunakan huruf yang sama pada *ciphertext* tersebut. Pada contoh *caesar cipher*, huruf A pada susunan abjad *plaintext* diubah menjadi huruf D pada *ciphertext*. Selain metode tersebut terdapat juga metode ROT13 yang dimana pada metode ini dilakukan pergeseran huruf abjad awal sebanyak 13 huruf [13]. Dapat disimpulkan dari hal tersebut antara *plaintext* dan *ciphertext* yang ada mudah untuk ditebak ketika dilakukan penyadapan pada kode *ciphertext* tersebut. Hal tersebut berkaitan juga dengan sering munculnya huruf yang sama pada susunan *ciphertext* yang ada. Berdasarkan pertimbangan diatas maka diciptakanlah kriptografi *Monoalphabetic cipher* sebagai bentuk baru dari *caesar cipher*.

Pada kriptografi ini huruf terdapat *ciphertext* yang dapat disusun dalam sebuah bentukyang berbeda-beda sebanyak 26! = 403.291.461.126.605.635.584.000.000 [13]. Dalam menyusun suatu *ciphertext* pada *Monoalphabetic cipher* dapat disusun seperti Tabel 1 berikut.

Tabel 1: *Contoh Monoalphabetic cipher)*

Plaintext	K	U	A	T	K	U	A	T	B	A	H	U	A	N	A	K	P	E	R	T	A	M	A

Penyusunan lain dari huruf *ciphertext* yang ada bisa dikembangkan dengan suatu bentuk kalimat sehingga mudah diingat. Berikut merupakan contoh kalimat kunci yang digunakan yaitu “semoga mendapatkan gelar”. Kemudian kalimat ini dipersingkat dengan cara menghilangkan huruf yang sama pada kalimat tersebut sesuai dengan keinginan pembuat. Maka didapatkan susunan seperti Tabel 2 berikut.

Tabel 2: *Kata Kunci (Key Text)*

Ciphertext	S	G	M	N	D	A	P	T	E	L	R

Kemudian *ciphertext* tersebut ditambakan dengan huruf-huruf yang belum ditambahkan pada kata kunci tersebut. Hal itu diaksudkan untuk menambah atau menyesuaikan dengan panjangnya huruf plainteks yang akan diubah ke ciherteks Berikut Tabel 3 bentuk kata kunci yang telah ditambahkan huruf pelengkap. Maka didapatkan susunan seperti Tabel 3 berikut.

Tabel 3: *Hasil Penambahan Huruf Pelengkap*

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

Pada kata kunci tersebut huruf yang baru ditambahkan juga diacak sesuai dengan keinginan pembuat agar susunan yang ada susah untuk ditebak. Hal tersebut dimaskudkan agar yang hanya mengetahui pola dari kunci tersebut adalah pengirim dan penerima pesan. Dengan susunan kata kunci tersebut dapat diperoleh table 4 subtitusi sebagai berikut.

Tabel 4: *Tabel Substitusi*

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

Tahap terakhir, akan *plaintext* akan dicocokkan, sehingga diperoleeh *Ciphertext*nya yaitu "LISC LISC GSTI SBSL ODWDXOISB ODWCSXS".

Proses pengenkripsian suatu plainteks perlu melewati beberapa tahap enkripsi pada kriptografi *Monoalphabetic cipher*, kemudian hasil yang diperoleh pada enkripsi dari plainteks tersebut dienkripsi menggunakan kriptografi Vigenere Cipher sehingga diperoleh *ciphertext* yang terenkripsi dan menghasilkan *ciphertext* yang tidak mudah untuk dimengerti oleh orang lain selain pengirim dan orang yang diberi kata kunci.

1) Tahap Enkripsi *Monoalphabetic cipher*

Monoalphabetic cipher (*cipher* abjad-tunggal) merupakan suatu kriptografi dengan algoritma dimana dirubahlah setiap bentuk huruf abjad dengan huruf yang berbeda dalam susunan huruf abjad yang sama [13]. Jumlah keseluruhan kunci pada *Monoalphabetic cipher* sesuai dengan cara penyusun 26 huruf abjad pada susunan alfabet. Hal ini membuktikan bahwa terdapat 26 jenis kunci ketika penyusun huruf – huruf alphabet tersebut ke dalam sebuah tabel substitusi. Contoh penyusunan huruf–huruf ketika memperoleh *ciphertext* cara melakukan penyusunan huruf–huruf alphabet menggunakan metode *ROT13*, *Caesar Cipher*, dan *Simple Subsitution Cipher,* dibawah ini merupakan table 5 substitusi dengan metode *caesar cipher* yang disusun sesuai dengan ke tiga metode yang telah dijabarkan.

Tabel 5: *Substitusi dengan Metode Caesar Cipher*

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

Menyusun tabel kriptografi subsitusi menggunakan metode *Simple Subsitution Cipher* menggunakan suatu kalimat yang dengan mudah untuk difahami dan diingat sehingga dapat mempermudah pe. Misalkan plainteksnya "Dalam lindungan Ka'bah" digunakan kunci "dia cinta orang lain". Dari kunci yang ada, perlu dibuang perulangan huruf yang ada sehingga menjadi "diacntorgl". Kemudian disusun menggunakan huruf-huruf alfabet lainnya yang tidak ada pada kalimat *ciphertext* tersebut sehingga dihasilkan susunan seperti Tabel 6 berikut.

Tabel 6: *Hasil Penambahan Huruf Pelengkap*

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

Dengan demikian, dapat diperoleh susunan huruf *key teks* yang telah dihilangkan huruf yang terdapat kesamaan dan menambahkan huruf yang belum ada pada susunan sehingga sesuai dengan jumlah huruf alfabet di tabel subsitusi sebagai berikut.

Tabel 7: *Tahap Enkripsi*

Plainteks = "DALAM LINDUNGAN KABAH"

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

Maka hasil *ciphertext* yaitu "*CDHDF HGBCXBODB EDID* "

2) Tahap Dekripsi *Monoalphabetic cipher*

Hasil yang didapatkan dari pendeskripsian *plaintext Monoalphabetic cipher* memakai sebuah tabel subsitusi yang telah ditentukan berdasarkan kunci *dia cinta orang lain* saat dilakukan tahap enkripsi [13]. Proses pendekripsian dilakukan pada tabel 8 berikut.

Tabel 8: *Tahap Dekripsi*

Plainteks = "DALAM LINDUNGAN KABAH"

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

Maka hasil *ciphertext*nya caitu "*CDHDF HGBCXBODB EDID". Ciphertext* tersebut didapatkan dari hasil penyesuain huruf alfabet dengan *key teks* yang ada sehingga *key teks* tersebut kan menghasilkan *ciphertext* yang diubah dari plainteks kemudian diubah dengan menggunakan *key teks* yang ada. Sehingga dalam table tersebut huruf plainteks D dan A diubah menjadi *ciphertext* menghasilkan huruf C dan D diikuti dengan huruf lainnya.

2. *Polyalphabetic Substitution Cipher*

Polyalphabetic Cipher atau *cipher* abjad-majemuk adalah suatu bentuk *cipher* subtitusi dengan melakukan pengelompokan huruf menjadi satu kesatuan. Pada kriptografi ini digunakan kunci yang berbeda sehingga dihasilkan percampuran huruf antara *plaintext* dengan *key text* sehingga akan dihasilkan *ciphertext* hasil penjumlahan nilai huruf *plaintext* dengan nilai huruf *key text*. *Polyalphabetic Substitution Cipher* dibuat berdasarkan sejumlah cipher abjad tunggal [16].

Tabel 9: *Tabel Polyalphabet*

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

Keterangan:
Plaintext = datamining
Key = rimarimari
Ciphertext = vjgberajfp
Dalam menyusun suatu *ciphertext* pada *poloalphabetic cipher* dapat disusun seperti Tabel 10 berikut.

Tabel 10: *Contoh Polyalphabet Cipher*

Plaintext	J	A	N	G	A	N	L	U	P	A	B	E	R	S	Y	U	K	U	R
Ciphertext	I	N	S	E	C	U	R	E	I	N	S	E	C	U	R	E	I	N	S

Dengan menggunakan metode Polyalphabetic Substitution dilakukan perhitungan dengan cara:

(J + I) mod 26 = 9 + 8 = mod 26 = 17 = "R"
(A + N) mod 26 = 0 + 13 = mod 26 = 13 = "N"
(N + S) mod 26 = 13 + 18 = mod 26 = 31 = "F"
(G + E) mod 26 = 6 + 4 = mod 26 = 10 = "K"
(A + C) mod 26 = 0 + 2 = mod 26 = 2 = "C"
(N + U) mod 26 = 13 + 20 = mod 26 = 33 = "H"
(L + R) mod 26 = 11 + 17 = mod 26 = 24 = "C"
(U +E) mod 26 = 20 + 4 = mod 26 = 24 = "Y"
(P + I) mod 26 = 15 + 8 = mod 26 = 23 = "X"
(A + N) mod 26 = 0 + 13 = mod 26 = 13 = "N"
(B + S) mod 26 = 1 + 18 = mod 26 = 19 = "T"
(E + E) mod 26 = 4 + 4 = mod 26 = 8 = "I"
(R + C) mod 26 = 17 + 2 = mod 26 = 19 = "T"
(S + U) mod 26 = 18 + 20 = mod 26 = 38 = "M"
(Y + R) mod 26 = 24 + 17 = mod 26 = 41 = "P"
(U +E) mod 26 = 20 + 4 = mod 26 = 24 = "Y"
(K + I) mod 26 = 10 + 8 = mod 26 = 18 = "S"
(U + N) mod 26 = 20 + 13 = mod 26 = 33 = "H"
(R + S) mod 26 = 17 + 18 = mod 26 = 35 = "J"

Sehingga akan didapatkan *ciphertext* yaitu RNFKCHCYXNTITMPYSHJ

Kriptografi *polyalphabetic subtittion cipher* menghasilkan suatu pola enkripsi acak dikarenakan terdapat huruf yang sama pada kalimat tersebut, sehingga menghasilkan suatu pola enkripsi yang berlainan [15]. Plainteks yang dicontohkan tersebut, memiliki 3 huruf A dan U yang dienkripsi menggunakan huruf kunci yang berbeda. Pada huruf A menjadi N dan C sedangkan huruf U menjadi Y dan S.

Pada uji coba kedua kriptografi tersebut, terdapat 3 poin yang dapat dianalisis. Pertama, terdapat rumus yang berbeda untuk kedua algoritma tersebut. Kunci *monoalphabetic cipher* hanya memiliki 1 rumus yang harus sesuai dengan kunci yang diberikan, sedangkan polyalphabetic cipher terdapat 2 rumus penyelesaian. Kedua, algoritma *monoalphabetic cipher* menggunakan kunci untuk mengenkripsi dengan memperpendek kalimat sedangkan algoritma *polyalphabetic cipher* menggunakan kunci dengan mengulang kata sesuai dengan panjang pesan yang akan dienkripsi. Ketiga, dalam segi keamananan selama penggunaan, polyalphabetic cipher lebih sulit dipecahkan karena algoritmanya lebih panjang daripada algoritma *monoalphabetic cipher*. Algoritma *monoalphabetic cipher* menggunakan analisis frekuensi huruf, sehingga mudah didekripsi mengunakan metode tebakan. Pada saat yang sama, algoritma *polyalphabetic cipher* plaintext yang sama didekripsi dengan kunci yang berbeda dan menghasilkan ciphertext yang berbeda, sehingga sulit untuk menggunakan metode tebakan untuk menerjemahkan pesan. Oleh karena itu, algoritma kriptografi *polyalphabetic cipher* efektif dan efisien dalam memperoleh keamanan data. Oleh karena itu, *Monoalphabetic cipher* jauh lebih mudah dipecahkan daripada *polyalphabetic substitusi cipher*. Sehingga penggunaan *polyalphabetic substitusi cipher* dianggap efektif dan efisien pada penerapan keamanan data.

4.2 Pembahasan

Hasil yang didapat dari perbandingan antara kriptografi *Monoalphabetic cipher* dan *polyalphabetic substitution cipher* dapat dilihat pada table 11.

Tabel 11: Perbedaan Monoalphabetic cipher dan Polyalphabetic Subtsitution

Perbedaan	***Monoalphabetic cipher***	***Polyalphabetic Subtitution Cipher***
Fungsi	Merubah setiap karakter huruf pada *plaintext* menjadi karakter lain pada suatu *ciphertext*	Mengelompokan huruf menjadi satu kesatuan
Kunci	Penyingkatan suatu kalimat yang digunakan sebagai kunci	Penggunaan kunci lebih menekankan mengulang kata yang digunakan sebagai kunci
Arrange	Tidak ada nilai dari kata kunci	Nilai dari kata kunci berulang
Jumlah Rumus	1 Rumus	2 Rumus
Cara Penyelesaian	*Ciphertext* yang dicari harus disesuaikan dengan huruf kata kunci yang tersedia	*Plaintext* yang ada dijumlahkan dengan nilai dari kata kunci yang disediakan sehingga menghasilkan *ciphertext* dari hasil penjumlahan nilai *plaintext* dan *ciphertext*

Perbedaan c*hipper Monoalphabetic* dan *polyalphabetic substitution* yaitu pada *Monoalphabetic* merupakan kriptografi substitusi yang merubah setiap karakter huruf pada *plaintext* sehingga didapatkan karakter lain pada suatu *ciphertext*. Sedangkan pada *polyalphabetic substitution* merupakan suatu bentuk cipher subtitusi dengan melakukan pengelompokan huruf menjadi satu kesatuan.Penggunaan kunci dalam pemecahan dan pembuatan *ciphertext Monoalphabetic* selalu menyingkat suatu kalimat yang digunakan sebagai kunci. Sedangkan pada *polyalphabetic* dalam penggunaan kunci lebih menekankan mengulang kata yang digunakan sebagai kunci. Pada *arrange* yang ada pada *Monoalphabetic cipher* tidak ada nilai yang digunakan untuk menghasilkan *ciphertext*, sedangkan pada *polyalphabetic subtitution cipher* dalam setiap alfabet memiliki nilai yang dapat dijumlahkan dengan nilai *key text* sehingga menghasilkan *ciphertext* dari hasil penjumlahan tersebut. Namun, dalam *Monoalphabetic cipher* hanya terdapat 1 rumus penyelesaian yang dimana ia harus menyesuaikan dengan kunci yang disediakan. Sedangkan dalam *polyalphabetic subtitution cipher* terdapat 2 rumus penyelesaian. Sedangkan dalam penyelesain dari *Monoalphabetic cipher* harus disesuaikan dengan *key teks* yang disediakan sehingga akan diperoleh *ciphertext* yang sesuai dengan pola dari *key teks* yang disediakan. Sedangkan pada *polyalphabetic cipher* melakukan penjumlahan antara plainteks dan *key teks* sehingga dihasilkan *ciphertext* hasil dari penjumlahan tersebut.

5. Kesimpulan

Berdasarkan penjelasan pembahasan sebelumnya dapat disimpulkan dari pembahasan Algoritma *Monoalphabetic cipher* dengan *polyalphabetic cipher* sebagai berikut:

1. Ada beberapa rumus yang berbeda untuk algoritma *monoalphabetic cipher* dan algoritma *polyalphabetic cipher.* Kunci *monoalphabetic cipher* hanya memiliki 1 rumus yang harus sesuai dengan kunci yang diberikan. Namun, ada 2 rumus penyelesaian dalam *polyalphabetic cipher.* Penyelesaian algoritma *monoalphabetic cipher* harus disesuaikan dengan *keytext* yang disediakan agar diperoleh *ciphertext* yang sesuai dengan pola *keytext* yang disediakan, sedangkan algoritma *polyalphabetic cipher* melakukan penjumlahan antara plaintext dan *keytext*, sehingga menghasilkan *Ciphertext* hasil dari penjumlahan.

2. Algoritma *monoalphabetic cipher* menggunakan kunci untuk mengenkripsi dengan memperpendek kalimat dengan menghapus huruf yang sama dalam kalimat, sedangkan algoritma *polyalphabetic cipher* menggunakan kunci dengan mengulang kata sesuai dengan panjang pesan yang akan dienkripsi.
3. Dalam segi keamananan selama penggunaan, *polyalphabetic cipher* lebih sulit dipecahkan karena algoritmanya lebih panjang daripada algoritma *monoalphabetic cipher*. Algoritma *monoalphabetic cipher* menggunakan analisis frekuensi huruf, sehingga mudah didekripsi mengunakan metode tebakan. Pada saat yang sama, algoritma *polyalphabetic cipher* plaintext yang sama didekripsi dengan kunci yang berbeda dan menghasilkan *ciphertext* yang berbeda, sehingga sulit untuk menggunakan metode tebakan untuk menerjemahkan pesan. Oleh karena itu, algoritma kriptografi *polyalphabetic cipher* efektif dan efisien dalam memperoleh keamanan data.

6. Daftar Pustaka

[1] Daryanto Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya Impact of Information Technology Development and Communication on," *J. Pendidik.*, vol. X, no. 2, pp. 195–211, 2017.

[2] A. Budi, A. Chicali, S. Pengajar, and S. Teknik Informatika, "System (Studi Kasus Pada Pt. One Standard Group Pte Ltd)," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, p. 253, 2019.

[3] Permanasari, Y, "Kriptografi Klasik *Monoalphabetic*," *Matematika*, vol. 16, no. 1, pp. 7–10, 2017, doi: 10.29313/jmtm.v16i1.2543.

[4] Permanasari Y. and E. Harahap, "Kriptografi Polyalphabetic," *Matematika*, vol. 17, no. 1, pp. 31–34, 2018, doi: 10.29313/jmtm.v17i1.4065.

[5] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[6] T. Khairani, K. Agung, and A. Kamsyakawuni, "Pengkodean *Monoalphabetic* Menggunakan Affine Cipher dengan Kunci Diffie-Hellman," *Prism. (Prosiding Semin. Nas. Mat.*, vol. 4, pp. 553–559, 2021, [Online]. Available: https://journal.unnes.ac.id/sju/index.php/prisma/ ISSN

[7] A. Musla, Tommy, and A. M. Elhanafi, "Kombinasi Kriptografi Algoritma Polyalphabetic Dan KompresiHuffman Untuk Pengamanan Data," *SNASTIKOM Semin. Nas. Teknol. Inf. Komun.*, pp. 303–310, 2021.

[8] D. R. I. M. S. S. P. Candra Irawan, T. Informatika, F. I. Komputer, and U. D. Nuswantoro, "Implementasi Algoritma Auto*key* Cipher," *Pros. SENDI_U*, pp. 978–979, 2019.

[9] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 61–64, 2016, doi: 10.30743/infotekjar.v1i1.43.

[10] A. Hanifah, "Perbandingan Kriptografi Cipher Substitusi Homofonik dan Poligram dengan Caesar Cipher," *Univ. Langlang Buana*, pp. 1–10, 2021.

[11] M. Sari and Asmendri, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," *Penelit. Kepustakaan (Library Res. dalam Penelit. Pendidik. IPA*, vol. 2, no. 1, p. 15, 2018, [Online]. Available: https://ejournal.uinib.ac.id/jurnal/index.php/naturalscience/article/view/1555/1159

[12] M. T and Budi Purwoko, "Studi Kepustakaan Mengenai Landasan Teori Dan Praktik Konseling Expressive Writing Library," *J. BK UNESA*, vol. 8, no. 1, pp. 1–8, 2017.

[13] Romindo, "Analisa Perbandingan Algoritma *Monoalphabetic cipher* Dengan Algoritma One Time Pad Sebagai Pengamanan Pesan Teks," *Sink. (Jurnal dan PenelitianTeknik Inf.*, vol. 2, no. 2, pp. 62–66, 2018.

[14] Sugiyono. (2017). Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R&D) (25th ed.). ALFABETA CV.

[16] Fahriani, N., Suryo, Y. A., & Devi, P. A. R. (2016). Pembangkit *Key Polyalphabetic Cipher* Pada Kriptografi Simetri Menggunakan Java Nuniek Fahriani, Yoedo Agung Suryo , Putri Aisyiyah R. Devi. *Dosen Teknik Informatika Universitas Muhammadiyah Gresik*, *26*(1), 136–147.