Analisis Penerapan Mirdek Cipher dalam Enkripsi Pesan

Yosef Rafael Joshua - 13522133[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13522133@std.stei.itb.ac.id

***Abstrak*— Kriptografi adalah ilmu yang mempelajari cara-cara untuk menjaga keamanan pesan. Dengan kata lain kriptografi adalah bagaimana kita merahasiakan pesan yang ingin kita sampaikan agar hanya diketahui oleh kita dan orang yang ditujukan. Kriptografi dapat dilakukan dengan berbagai macam cara. Di era modern ini, kriptografi menggunakan bantuan program komputer tidaklah jarang. Kita dapat menemukan kriptografi dengan bantuan komputer di kegiatan sehari-hari kita. Mirdek Cipher adalah salah satu metode kriptografi klasik yang memanfaatkan sebuah set kartu bridge untuk mengubah pesan menjadi pesan rahasia. [2]Metode ini diciptakan oleh Paul Crowled, seorang kriptanalis, pada tahun 2000.**

***Kata Kunci*—Dekripsi, Enkripsi, Kriptografi, Mirdek Cipher. Vigenere Cipher**

I. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari cara-cara untuk menjaga keamanan pesan. Dengan kata lain kriptografi adalah bagaimana kita merahasiakan pesan yang ingin kita sampaikan agar hanya diketahui oleh kita dan orang yang ditujukan. Kriptografi dapat dilakukan dengan berbagai macam cara. Bisa sesederhana menuliskan kode rahasia, yang hanya diketahui oleh diri kita dan orang yang ditujukan, di kertas ataupun serumit menggunakan algoritma serta bantuan program komputer.

Di era modern ini, kriptografi menggunakan bantuan program komputer tidaklah jarang. Kita dapat menemukan kriptografi dengan bantuan komputer di kegiatan sehari-hari kita. Contohnya adalah ketika mengirim pesan. Sekarang aplikasi-aplikasi pengirim pesan sudah menggunakan end-to-end encryption dalam pengiriman pesan. Namun kriptografi tidaklah harus serumit itu. Kriptografi dapat dilakukan dengan benda-benda umum di sekitar kita. Contohnya adalah sebuah set kartu *bridge*. Kartu bridge cocok digunakan untuk merahasiakan pesan kita karena di dalamnya terdapat 52 sedangkan alfabet yang kita gunakan berjumlah 26 karakter.

Kriptografi dapat dibagi menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik lebih berfokus pada cara-cara tanpa menggunakan bantuan teknologi modern seperti program komputer. Dengan kriptografi klasik, pesan yang akan dirahasiakan akan diolah dengan metode tertentu menjadi pesan rahasia yang akan dikirim. Kriptografi klasik tidak sebaik kriptografi modern dalam segi keamanan, namun kriptografi klasik tetap merupakan landasan yang penting.

Mirdek Cipher adalah salah satu metode kriptografi klasik yang memanfaatkan sebuah set kartu bridge untuk mengubah pesan menjadi pesan rahasia. [2]Metode ini diciptakan oleh Paul Crowled, seorang kriptanalis, pada tahun 2000. Paul Crowley menciptakan metode ini karena ia menemukan suatu bias pada metode kriptografi yang lain, yaitu Solitaire Cipher yang dibuat oleh Bruce Schneier. Cara kerja mirdek adalah dengan membagi 52 kartu menjadi 2 tumpukan. Tumpukan yang satu akan digunakan untuk menentukan apa yang harus dilakukan terhadap tumpukan kedua. Secara langsung tumpukan yang pertama akan dipengaruhi oleh urutan tumpukan kedua.

Tujuan dari makalah ini adalah untuk menganalisis Mirdek Cipher dari segi keamanan, kemudahan untuk dipakai, dan waktu yang diperlukan untuk melakukan enkripsi serta dekripsi. Pada makalah ini, mirdek akan dibandingkan dengan salah satu metode kriptografi klasik terkenal, yaitu Vigenere Cipher.

Makalah ini terdiri dari 6 bagian. Bagian pertama adalah pendahuluan. Isi dari pendahuluan adalah pengantar singkat tentang kriptografi dan mirdek cipher. Kemudian ada landasan teori yang berkaitan dengan mirdek cipher dan kriptografi. Setelah landasan teori, ada contoh implementasi dari mirdek cipher dengan sedikit modifikasi. Lalu ada kesimpulan, saran, dan ungkapan terima kasih dari penulis.

II. LANDASAN TEORI

A. Kriptografi

[1] Kriptografi berasal dari Bahasa Yunani “Cryptos” dan “Graphein”. Cryptos berarti rahasia, sedangkan graphein berarti menulis. Jadi Kriptografi adalah “menulis rahasia” atau “secret writing”. [] Kriptografi adalah ilmu yang memanfaatkan teknik-teknik matematika untuk merahasiakan suatu pesan. Kriptografi menyamarkan pesan sehingga pesan asli tersamarkan menjadi kumpulan angka dan huruf tidak dapat dibaca begitu saja.

Tujuan dari Kriptografi adalah untuk menjaga keamanan dari pesan yang ingin disampaikan. Dengan menyandikan pesan asli menjadi pesan yang tidak terbaca, maka tidak semua orang bisa melihat pesan tersebut dan mengerti maksudnya. Hanya pengirim dan penerima pesan yang dapat menerjemahkan pesan tersebut dan membacanya.

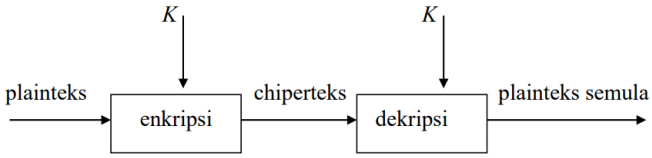
```
Ketika saya berjalan-jalan di pantai,
saya menemukan banyak sekali kepiting
yang merangkak menuju laut. Mereka
adalah anak-anak kepiting yang baru
menetas dari dalam pasir. Naluri
mereka mengatakan bahwa laut adalah
tempat kehidupan mereka.
```

Gambar 1. Contoh *Plaintext* sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian2-2023.pdf, diakses pada 10/12/2023

```
Ztâxzp/épêp/qtüyp{p}<yp{p}/sx/•p}âpx;
  épêp/|t}t|äzp}/qp}êpz/étzp{x/zt•xâx
}v  êp}v/|tüp}vzpz/|t}äyä/{päâ=/\tütz
p  psp{pw/p}pz<p}pz/zt•xâx}v/êp}
v/qpüä  |t}tâpé/spüx/sp{p|/•péxü=/]
p{äüx  |ttüzp/|t}vpâpzp}/qpwåp/{päâ
/psp{pw  ât|•pâ/ztwxsä•p}/|tützp=
```

Gambar 2. Contoh *Ciphertext* sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian3-2023.pdf, diakses pada 10/12/2023

Di dalam ilmu kriptografi terdapat beberapa istilah penting. Yang pertama adalah *plaintext*, yaitu pesan yang dapat kita mengerti atau dapat kita baca secara biasa. Yang kedua adalah *ciphertext*, yaitu pesan yang sudah disandikan menjadi kumpulan angka dan huruf serta sudah kehilangan makna aslinya. Yang ketiga adalah enkripsi, yaitu proses saat *plaintext* diterjemahkan menjadi *ciphertext*. Yang keempat adalah dekripsi, yaitu proses saat *ciphertext*, yang tidak bisa dibaca secara langsung, diterjemahkan kembali menjadi *plaintext*, yang dapat dibaca secara langsung. Yang kelima adalah *key*, yaitu kode atau tulisan atau pesan yang dapat digunakan untuk menerjemahkan pesan.



Gambar 3. Ilustrasi proses enkripsi dan dekripsi pesan sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian3-2023.pdf, diakses pada 10/12/2023

Kriptografi dapat dibedakan menjadi dua jenis. Yang pertama adalah kriptografi klasik. Kriptografi klasik memanfaatkan kode rahasia untuk menerjemahkan dari *plaintext* menjadi *ciphertext*. Kriptografi klasik sangat bergantung pada teknik-teknik matematika untuk merahasiakan pesan. Kriptografi klasik dapat dibedakan menjadi kriptografi simetris dan kriptografi asimetris. Kriptografi simetris memanfaatkan kode (*key*) yang sama untuk enkripsi dan dekripsi. Pada kriptografi simetris pengirim dan penerima pesan memiliki *key* yang sama. Kriptografi asimetris memanfaatkan kode (*key*) yang berbeda dalam tahap enkripsi dan dekripsi. Pada kriptografi asimetris, pengirim dan penerima pesan memiliki *key* yang berbeda untuk menerjemahkan pesan.

B. Mirdek Cipher

Mirdek cipher adalah metode kriptografi yang dibuat oleh Paul Crowley pada tahun awal tahun 2000. Metode ini tidak memandang kartu sesuai dengan simbolnya (berlian, sekop, hati, keriting) tapi pada warna kartinya. Pada mirdek, setiap kartu melambangkan hurut pada alfabet. Kartu As-King warna hitam melambangkan huruf A-M. Kartu As-King warna merah melambangkan huruf N-Z. Bukan hanya itu setiap kartu juga melambangkan angka yang berbeda-beda mulai dari 1 sampai 26. Kartu warna hitam melambangkan angka 1-13 sedangkan kartu warna merah melambangkan angka 14-26.

Black	A	B	C	D	E	F	G	H	I	J	K	L	M
	Ace	2	3	4	5	6	7	8	9	10	Jack	Queen	King
	1	2	3	4	5	6	7	8	9	10	11	12	13
Red	14	15	16	17	18	19	20	21	22	23	24	25	26
	Ace	2	3	4	5	6	7	8	9	10	Jack	Queen	King
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Gambar 4. Tabel representasi setiap kartu untuk mirdek sumber: http://www.ciphergoth.org/crypto/mirdek/description.html, diakses pada 10/12/23

B.1. Operasi Khusus

Terdapat beberapa operasi khusus yang perlu diketahui untuk mirdek cipher. Pertama-tama kartu harus dibagi menjadi dua tumpukan. Tumpukan pertama terdiri dari kartu dengan simbol sekop dan berlian. Tumpukan kedua terdiri dari kartu dengan simbol keriting dan hati. Mulai dari sini tumpukan pertama akan disebut left dan tumpukan kedua akan disebut right. Kartu-kartu pada left terbuka (tumpukan menghadap ke atas). Kartu-kartu pada right tertutup (tumpukan menghadap ke bawa).

Operasi khusus yang pertama adalah Counted Cut. Pertama ambil kartu paling atas dari right, buka dan letakkan pada discard. Konversi kartu tersebut ke nilai angkanya. Lalu hitung satu per satu kartu di left hingga angka tersebut. Ketika sudah sampai pada angka tersebut, maka ambil sisa kartu di left dan letakkan di atas kartu-kartu yang sudah dihitung. Berikut contohnya

(awal)
Left: **JHFDBZLMNOPQRSTUVWYCGIAKXE**
Right: **IPDZOWKGSTVARMEQYBCFJNH**
Discard: **ULX**

(ambil kartu right teratas, letakkan di discard)
Left: **JHFDBZLMNOPQRSTUVWYCGIAKXE**
Right: **IPDZOWKGSTVARMEQYBCFJN**
Discard: **HULX**

H jika dikonversi akan menghasilkan “8” sehingga langkah selanjutnya adalah menhitung delapan kartu dari left kemudian melakukan *cut*.

(counted cut)

Left: **JHFDBZLM + NOPQRSTUVWYCGIAKXE**
Right: **IPDZOWKGSTVARMEQYBCFJN**
Discard: **HULX**

(setelah cut)
Left: **NOPQRSTUVWYCGIAKXE + JHFDBZLM**
Right: **IPDZOWKGSTVARMEQYBCFJN**
Discard: **HULX**

(hasil)
Left: **NOPQRSTUVWYCGIAKXEJHFDBZLM**
Right: **IPDZOWKGSTVARMEQYBCFJN**
Discard: **HULX**

Operasi khusus yang kedua adalah Letter Search. Pada operasi ini akan diseleksi satu huruf untuk diterjemahkan. Kemudian huruf tersebut dikonversi ke representasi kartunya. Kemudian dari left akan diambil kartu satu per satu dan diletakkan di dua tumpukukan berbeda secara bergantian. Akan terus dilakukan hingga kartu representasi dari huruf yang sudah ditentukan berada pada salah satu tumpukan. Hitung total kartu di kedua tumpukan, kemudian konversi hasilnya ke representasi huruf. Huruf tersebut adalah *ciphertext* untuk huruf awal yang ditentukan. Berikut contohnya

(awal)
Left: **EJFDBZLMPNOQRSTUVWYAGICKXH**

Huruf "S" akan diterjemahkan. Maka konversinya adalah kartu 6 berwarna merah. Letakkan kartu satu per satu di tumpukan yang berbeda hingga kartu 6 merah diletakkan

(hasil)
P1: **ROPLBFE**
P2: **SQNMZDJ**
Left: **TUVWYAGICKXH**

Jumlah P1 + P2 adalah 14. Konversi 14 adalah "N", sehingga dalam kasus ini huruf "S" diterjemahkan menjadi "N".

(penyatuan kembali)
Left: **TUVWYAGICKXH + SQNMZDJ + ROPLBFE**

B.2. Enkripsi

Untuk melakukan enkripsi, pastikan 52 kartu sudah terbagi menjadi 2 tumpukan sesuai aturan di atas. Setelah itu lakukan counted cut. Kemudian lakukan letter search untuk huruf pertama yang ingin dienkripsi. Lakukan terus menerus hingga semua huruf sudah dienkripsi.

B.3. Dekripsi

Untuk dekripsi lakukan pastikan 52 kartu sudah terbagi menjadi 2 tumpukan sesuai aturan di atas. Kemudian lakukan kebalikan dari langkah-langkah enkripsi. Pertama-tama lakukan counted cut terlebih dahulu. Kemudian ubah huruf yang ingin diterjemahkan ke angka. Letakkan kartu satu per satu dari left di dua tumpukan yang berbeda sampai angka tersebut. Ketika angka tersebut tercapai, kartu yang diletakkan akan dikonversi menjadi huruf. Huruf tersebutlah yang merupakan terjemahan *plaintext* dari *ciphertext*.

C. Vigenere Cipher

Vigenere Cipher adalah salah satu metode kriptografi klasik yang sangat populer. Metode ini pertama kali ditemukan oleh Giovan Battista Bellaso, seorang kriptografer asal Italia, pada tahun 1553. Namun metode ini dibuat terkenal oleh kriptografer Blaise de Vignere yang menemukan metode serupa pada tahun 1586.

[6] Vignere Cipher adalah metode yang mengubah *plaintext* menjadi *ciphertext* dengan *Caesar's Cipher* yang berulang kali. Vignere cipher memerlukan *keyphrase* berupa kata yang panjangnya harus sama dengan pesan yang ingin dirahasiakan. Cara termudah untuk melakukan ini adalah menentukan suatu kata, kemudian mengulangnya sampai panjangnya sama dengan pesan yang ingin dienkripsi.

Untuk mengenkripsi pesan, keyphrase akan menentukan terjemahan dari *plaintext*. Pertama-tama buat dulu table (matriks) yang melambangkan pemetaan dari satu huruf ke huruf lainnya.

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

Gambar 5. Matriks Vigenere Cipher

Setelah matriks tersebut berhasil dibuat, maka langkah selanjutnya adalah enkripsi. Baca huruf pertama dari pesan yang akan dienkripsi, lalu pindah ke kolom tersebut. Setelah itu baca huruf pertama dari *keyphrase*, lalu pindah ke baris tersebut. Pertemuan antara baris dan kolom adalah terjemahan dari huruf pertama ke *ciphertext*. Berikut contohnya

Plaintext: JOS
Keyphrase: HUA
Ciphertext: QIS

Dari plaintext "JOS" dan keyphrase "HUA" didapatkanlah ciphertext "QIS".

Untuk melakukan dekripsi maka lakukan kebalikan dari enkripsi. Pertama-tama lihat huruf *ciphertext*. Kemudian temukan huruf *ciphertext* pada baris huruf *keyphrase* pertama. Itu adalah pertemuan dari kolom dan baris. Karena baris adalah

keyphrase, maka sudah pasti kolom yang bertemu dengan baris tersebut adalah *plaintext*.

III. Implementasi dan Analisis

Sekarang akan dilakukan enkripsi pesan yang berbeda dengan dua metode yang berbeda. Yang pertama akan dilakukan menggunakan Vigenere Cipher. Kemudian akan dilakukan dengan Mirdek Cipher. Setelah itu akan dilakukan analisis berdasarkan waktu yang diperlukan untuk menghasilkan ciphertext, kemudahan untuk melakukan enkripsi, dan keamanan dari metode yang digunakan. Untuk enkripsi Vignere akan digunakan pesan "IFDUATIGA". Untuk metode Vigenere Cipher akan dipakai *keyphrase* "INSTITUTE". Untuk Mirdek akan dilakukan enkripsi pesan "INFO"

A. Implementasi Vigenere Cipher

Pada kondisi awal kita memiliki
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: -

(Enkripsi huruf ke-1)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: Q

(Enkripsi huruf ke-2)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QS

(Enkripsi huruf ke-3)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSV

(Enkripsi huruf ke-4)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVN

(Enkripsi huruf ke-5)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVNI

(Enkripsi huruf ke-6)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVNIM

(Enkripsi huruf ke-7)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVNIMC

(Enkripsi huruf ke-8)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVNIMCZ

(Enkripsi huruf ke-9)
Plaintext: IFDUATIGA
Keyphrase: INSTITUTE
Ciphertext: QSVNIMCZE

Jadi didapatkan bahwa keyphrase "INSTITUTE" dan plaintext "IFDUATIGA" menghasilkan ciphertext "QSVNIMCZE".

B. Implementasi Mirdek Cipher

(kondisi awal)
Left: **ABCDEFGHIJKLKMOPQRSTUVWXYZ**
Right: **NOPQRSTUVWXYZABCDEFGHIJKLM**
Discard: -

(enkripsi huruf ke-1)
(counted cut)
Left: **OPQRSTUVWXYZABCDEFGHIJKLMN**
Right: **NOPQRSTUVWXYZABCDEFGHIJKL**
Discard: **M**

(letter search)
P1: **OQSUWYACEGI**
P2: **PRTVXZBDFH**
Left: **JKLMN**
Right: **NOPQRSTUVWXYZABCDEFGHIJKL**
Discard: **M**
Ciphertext: "U"

(dilakukan seterusnya)

C. Analisis Vigenere Cipher

Dari segi waktu yang diperlukan, penulis memerlukan waktu 30 menit untuk membuat matriks vigenere kemudian mengenkripsi plaintext menjadi ciphertext. Mungkin waktu yang diperlukan dapat berkurang jika matriks vigenere sudah dipersiapkan sebelumnya.

Dari sisi kenyamanan dan kemudahan untuk dipakai, vigenere cipher cukup mudah untuk dipahamai. Selain itu proses melakukan enkripsi juga tidak terlalu rumit serta tidak perlu melakukan persiapan tambahan selain dari menyiapkan matriks vigenere. Dalam enkripsi pesan, penulis tidak mengalami terlalu banyak kesulitan. Tapi vigenere cipher memerlukan ketelitian untuk melakukan enkripsi, terlebih jika pesan yang diterjemahkan sangat panjang.

Dari segi keamanan, vigenere cipher dinilai cukup aman asalkan keyphrase terjaga dengan baik. Di sisi lain vigenere cipher adalah salah satu cipher paling populer jadi tentu banyak orang yang sudah mengetahui cipher ini. Jadi kemungkinan orang mengenali metode ini lebih besar. Walaupun demikian, asalkan hanya pengirim dan penerima pesan yang mengetahui keyphrase, maka vigenere cipher ternilai cukup aman.

D. Analisis Mirdek Cipher

Dari segi waktu yang diperlukan, penulis memerlukan waktu 60 menit untuk melakukan persiapan dan enkripsi pesan. Hal tersebut mungkin karena penulis belum terbiasa dengan metode mirdek ini. Selain itu jika semua persiapan sudah dilakukan sebelumnya mungkin waktu yang diperlukan untuk enkripsi bisa lebih cepat.

Dari segi kenyamanan dan kemudahan, mirdek cipher kurang mudah untuk digunakan. Hal ini karena beberapa hal. Yang pertama untuk mirdek cipher pengirim dan penerima pesan harus mengetahui dulu operasi khusus untuk mirdek. Yang kedua proses menghitung dan meletakkan kartu dalam waktu yang bersamaan tidaklah mudah dilakukan untuk orang yang baru mempelajari metode ini. Ketiga karena memerlukan waktu yang lebih lama, jika ada pesan yang sangat panjang utuk dienkripsi, maka dapat memerlukan waktu 1 hari penuh untuk mengenkripsi pesan tersebut. Yang keempat perlu ketelitian yang sangat selama seluruh proses enkripsi karena satu kesalahan dapat menyebabkan seluruh proses enkripsi berujung salah

Dari segi keamanan, mirdek cipher bukanlah cipher terkenal seperti vigenre cipher. Oleh karena itu kemungkinan seseorang mengenali cipher ini lebih rendah. Namun karena mirdek memerlukan ketelitian yang sangat banyak untuk proses enkripsi, maka sebaliknya juga berlaku. Jika sampai seseorang selain pengirim dan penerima pesan berhasil untuk mendapatkan urutan kartu yang diperlukan untuk mendekripsi, maka mereka juga harus sangat teliti dalam prosesnya. Hal ini menambah nilai keamanan dari mirdek cipher, terutama jika pesan yang dienkripsi lumayan panjang.

Mirdek bukanlah metode yang mudah dipelajari ataupun digunakan, namun keunikan dari metode ini adalah untuk proses dekripsi diperlukan kedua tumpukan left dan right yang sama dengan urutan pada enkripsi. Jadi 1 tumpukan saja tidak cukup. Harus ada 2 tumpukan dengan urutan yang sama.

IV. KESIMPULAN

Berdasarkan hasil uji kasus yang telah dilakukan dapat disimpulkan beberapa hal mengenai mirdek cipher.

Yang pertama adalah segi waktu yang diperlukan. Mirdek cipher memerlukan banyak sekali waktu, mulai dari persiapan kartu mula-mula hinggal engkripsi. Oleh karena itu enkripsi dengan metode ini memerlukan waktu yang lebih lama dibandingkan dengan metode kriptografi yang lain seperti vigenere cipher. Jika pesan yang dienkripsi lebih panjang, maka waktu yang diperlukan untuk enkripsi juga lebih panjang, bahkan bisa memerlukan waktu satu hari penuh untuk melakukan enkripsi.

Yang kedua adalah segi kemudahan dan kenyamanan. Dari hasil uji kasus, mirdek tidaklah mudah dipelajari ataupun digunakan. Ada banyak hal yang harus dipelajari untuk mirdek. Operasi khusus, tabel representasi kartu, serta urutan langkah-langkah dalam proses enkripsi dan dekripsi tidaklah mudah untuk diingat. Selain itu selama proses enkripsi dari awal sampai akhir diperlukan konsentrasi yang besar. Hal tersebut karena satu langkah yang salah dapat menyebabkan seluruh proses enkripsi gagal. Hal yang sama juga berlaku pada proses dekripsi. Oleh karena itu dapat dikatakan bahwa mirdek cipher tidaklah mudah ataupun nyaman untuk digunakan.

Yang ketiga adalah segi keamanan. Mirdek cipher adalah metode kriptografi yang lebih aman. Hal tersebut karena mirdek cipher memerlukan dua tumpukan dengan urutan yang sama seperti pada proses enkripsi untuk melakukan dekripsi. Tanpa tumpukan yang satu maka proses dekripsi tidak dapat dilakukan. Selain itu ketelitian yang diperlukan juga menambah keamanan dari mirdek cipher. Jika seseorang merhasil menemukan urutan dan tumpukan semula, mereka harus tetap memiliki konsentrasi yang tinggi selama proses dekripsi. Jika pesan sangat panjang maka akan rawan terjadi kesalahan.

Secara keseluruhan mirdek cipher adalah mirdek yang lebih aman dibandingkan metode kriptografi lain seperti vigenere cipher. Namun walaupun lebih aman, mirdek cipher lebih sulit untuk dipelajari dan digunakan sebagai metode kriptografi

V. SARAN

Penulis menyarankan bagi para penulis lainnya agar dapat mempersiapkan metode kriptografi dengan baik sebelum melakukan uji kasus. Operasi khusus, tabel, dan langkah-langkah khusus serta persiapan lain sebaiknya sudah dipersiapkan matang-matang agar proses enkripsi pesan dapat dilakukan dengan waktu yang lebih cepat

VI. UCAPAN TERIMA KASIH

Terima kasih kepada Tuhan Yang Maha Esa karena berkat rahmat dan kasih karunia-Nya penulis dapat menyelesaikan makalah kali ini dengan baik dan tanpa kendala yang terlalu berat. Tak lupa juga penulis ingin mengucapkan terima kasih kepada keluarga yang telah memberi dukungan sehingga penulis dapat menyelesaikan makalah ini. Teirma kasih juga kepada pak Rinaldi Munir selaku dosen pengampu mata kuliah IF 2120 Matematika Diskrit karena telah memberikan ilmu dan bimbingan yang sangat berguna dalam penulisan makalah ini. Terima kasih juga kepada teman-teman yang telah membantu dalam pengerjaan makalan ini secara langsung maupun tidak langsung.

REFERENCES

[1] Munir, Rinaldi. 2023. “Teori Bilangan Bagian 2”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian2-2023.pdf, diakses pada 10/12/2023

[2] Munir, Rinaldi. 2023. “Teori Bilangan Bagian 3”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2023-2024/16-Teori-Bilangan-Bagian3-2023.pdf, diakses pada 10/12/2023

[3] https://www.schneier.com/academic/solitaire/ diakses pada 10/12/2023

[4] http://www.ciphergoth.org/crypto/mirdek/description.html diakses pada 10/12/2023

[5] https://www.youtube.com/watch?v=vivovrdaSoQ diakses pada 10/12/2023

[6] https://www.youtube.com/watch?v=SkJcmCaHqS0 diakses pada 10/12/2023

[7] https://www.geeksforgeeks.org/classical-cryptography-and-quantum-cryptography/ diakses pada 10/12/2023

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2023

Yosef Rafael Joshua - 13522133