Terbit *online* pada laman: http://jurnal.utu.ac.id/JTI

Jurnal Teknologi Informasi

ISSN (Online): 2829-8934

Implementasi Enkripsi Dengan Vigenere Cipher Dan Reverse Cipher Menggunakan Bahasa Pemrograman Python

Abdurrahman Ridho[1], Cukri Rahmi Niani[2]
[1,] Teknologi Informasi, Universitas Teuku Umar, Aceh Barat, Indonesia
Email: [1]abdurrahman.ridho@utu.ac.id, [2]cukrirahminiani@utu.ac.id

INFORMASI ARTIKEL

Sejarah Artikel*:*
Diterima: 8 Maret 2022
Revisi: 15 April 2022
Diterbitkan: 12 Mei 2022

Kata Kunci*:*
Kritografi
Vigenere Cipher
Reverse Cipher
Python
Enkripsi

ABSTRAK

Arus komunikasi pada zaman ini begitu kencang, kelancaran arus komunikasi tersebut dipengaruhi oleh sejumlah faktor diantaranya kemajuan teknologi di bidang informasi serta mudahnya untuk mendapatkan perangkat untuk berkomunikasi tersebut. Dibalik semua kemudahan tersebut terdapat sejumlah ancaman yang ada. Diantaranya peretasan yang dilakukan oleh entitas yang tidak bertanggung jawab. Beberapa aspek yang harus dipenuhi berupa keamanan, keaslian dan otentifikasi dan beberapa aspek lainnya yang harus dipenuhi untuk memenuhi keamanan dan kenyamanan dalam berkomunikasi. Kriptografi hadir sebagai salah satu solusi untuk menjamin keamanan pada data seperti teks, gambar, audio, dan video yang dikirimkan sebagai objek komunikasi. Kriptografi bekerja dengan mengubah objek atau data yang awalnya dapat dipahami menjadi sebuah objek atau data yang tidak dapat dipahami. Salah satu bagian dari kriptografi adalah Vigenere Cipher yang telah digunakan sejak lama. Dalam perjalanannya Vigenere Cipher sudah dapat dipecahkan, hal ini tentu menjadi sebuah tantangan tentang bagaimana cara memperkuat cipher tersebut, untuk itu pada penelitian ini dilakukan eknkripsi ganda dengan menggunakan Vigenere Cipher dan Reverse Cipher yang diharapkan dapat memperkuat Vigenere Cipher tersebut.

1. Pendahuluan

Kriptografi merupakan sebuah bidang ilmu yang masih digunakan khususnya untuk melindungi data yang bersifat rahasia. Berbagai penelitian dan pengembangan terus dilakukan demi mendapatkan metode yang sulit untuk dipecahkan oleh entitas yang tidak berkepentingan. Pertukaran data yang dilakukan secara dua arah memerlukan kepastian akan adanya perlindungan terhadap data yang dikirimkan dari entitas yang tidak berkepentingan. Masalah keamanan merupakan aspek penting yang harus ada terlebih apabila aktivitas pertukaran informasi tersebut dilakukan secara nirkabel [1]

Asal mula kriptografi terdapat dari bahasa Yunani yang memiliki dua buah suku kata yaitu kripto dan graphia yang bila diartikan adalah menyembunyikan tulisan. Adapun kriptografi merupakan ilmu yang mempelajari teknik yang berkaitan dengan aspek keamanan seperti untuk menyembunyikan pesan dan menjamin pesan tersebut tidak sampai pada entitas yang tidak berkepentingan [2]. Enkripsi atau enkripsi yang digunakan oleh bangsa Mesir pada waktu itu sejak 3000 SM dimulai sekitar 1000 SM. Teknik yang digunakan disebut hieroglif dan membantu menyembunyikan pesan yang dilindungi dari badan yang tidak berwenang. Teknik kriptografi ini adalah mengganti satu huruf abjad dengan huruf lain dari abjad yang sama. Cipher ini melibatkan pergeseran alfabet tiga huruf dan kemudian mengganti huruf.

Sejarah panjang kriptografi komputer, yang telah digunakan sejak Perang Dunia II, mendorong para sarjana untuk mengembangkan seni kriptografi. Perkembangan kriptografi tidak lagi terbatas pada militer, tetapi pada masyarakat umum. Teknologi kriptografi diharapkan terus berkembang, sekecil apapun perkembangannya, dan memicu perkembangan kriptografi baru yang lebih efisien dan efektif. Pengubahan teks asli menjadi kode atau sekumpulan teks yang tidak dapat dimengerti merupakan bagian dari seni untuk menjaga keamanan pesan yang dikirimkan tersebut. Hal ini dilakukan untuk mencegah adanya entitas yang tidak berkepentingan untuk dapat membaca atau mendapatkan pesan yang dikirimkan tersebut. [3]

Kriptografi memiliki sejumlah tujuan atau aspek yang harus dipenuhi[4], yaitu:

1. Penyembunyian yang memastikan kerahasiaan dari entitas yang tidak berkepentingan.
2. Kelengkapan Data yang merupakan aspek bahwa data yang dikirimkan sesuai dengan kelengkapan semula.
3. Keaslian yang berkaitan dengan autentikasi dari pada sumber data.
4. Tidak ada penolakan yaitu berupa saling terhubung dan tidak dapat menolak data yang dikirimkan maupun diterima.

Beberapa hal yang berkaitan dengan kriptografi. Pengirim yang merupakan entitas yang mengirimkan pesan kepada penerima dengan memastikan bahwa pesan tersebut dapat dikirimkan dengan aman. Plaintext merupakan pesan asli yang dimasukkan ke dalam algoritma kriptografi yang menghasilkan Ciphertext atau merupakan pesan tersandi yang telah melewati serangkaian proses sehingga menjadikannya pesan yang tidak dapat dipecahkan. Enkripsi merupakan proses untuk mengubah plaintext menjadi ciphertext, sedangkan dekripsi merupakan proses untuk mengubah ciphertext menjadi plaintext. Kriptografer merupakan orang yang mempelajari metode kriptografi dan menggunakannya. Kriptanalis merupakan orang yang berusaha untuk memecahkan pesan tersandi tersebut, sedangkan Kriptologis merupakan orang yang mempelajari kriptografi. Cipher merupakan algoritma untuk melakukan enkripsi dan dekrispi Penyadap merupakan entitas yang ingin mendapatkan data atau pesan asli yang dikirimkan oleh pengirim pada penerima.[4]

Kriptanalisis ditemukan oleh orang Arab karena pengetahuan mereka tentang linguistik, statistik, dan matematika. Pada tahun 1790, Thomas Jefferson mengembangkan perangkat pengacakan yang menggunakan tumpukan 26 disk yang dapat dimainkan secara individual. Pesan dihasilkan dengan memutar setiap disk secara bergantian dengan setiap karakter di bawah bilah dengan melintasi panjang tumpukan disk. Oleh karena itu, bilah yang sedang berlangsung berputar pada sudut tertentu.

Vigenere cipher merupakan cipher yang bergantung dengan metodologi confusion untuk membentuk teks yang tersandi. Plaintext atau teks asli memiliki pola berulang yang merupakan kamuflase menggunakan pergeseran Caesar cipher. Vigenere cipher merupakan pola yang efektif untuk menyembunyikan pesan selama 300 tahun dan kemudian dipecahkan oleh Kasiski dan Kerckhoff. [5]

Vigenere cipher juga merupakan salah satu algoritma kriptografi klasik yang sudah ada sejak abad ke 16. Pencetusnya bernama Blaise de Vigenere.

Komponen pada Vigenere cipher:

Enkripsi : $Ciphertext = (Plaintext + Kunci)\ (mod\ 26)$

Dekripsi : $Plaintext = (Ciphertext - Kunci)(mod\ 26)$

Ciphertext : Teks yang tersandi

Kunci : Kunci yang digunakan untuk melakukan operasi menggunakan algoritma tersebut

Plaintext : Text asli yang belum tersandi

Tabel 1. Tabel Alfabet 26 Karakter

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**				
20	21	22	23	24	25				

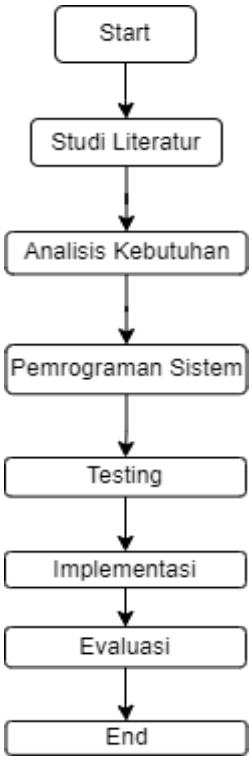
Penggunaan mod 26 pada formula Vigenere cipher adalah untuk membatasi hasil penjumlahan maupun pengurangan diantara range angka 0-25. Hal ini disebabkan apabila karakter yang digunakan hanya berjumlah 26. Sedangkan bila ingin menggunakan lebih dari 26 karakter dapat menggunakan mod 256 yang merupakan jumlah dari karakter ASCII

Reverse cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan metode transposisi atau pertukaran/penggantian satu karakter dengan karakter lainnya. Reverse Cipher juga merupakan salah satu kriptografi sederhana yang menggunakan metode transposisi atau perpindahan/penggantian karakter yang satu dengan lainnya.[6]

2. Metodologi Penelitian

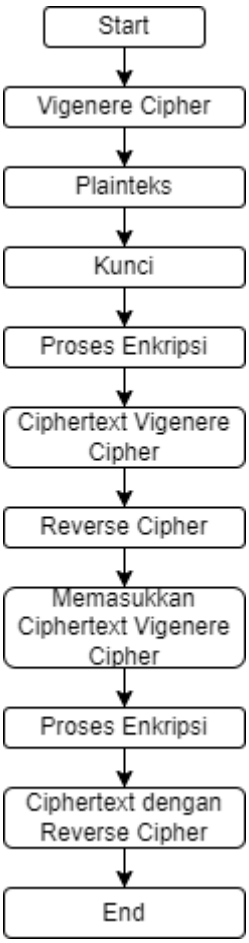
Metode penelitian yang dilakukan dalam penelitian ini mencakup beberapa hal yaitu:

1. Studi literatur
2. Anlisis kebutuhan
3. Pemrograman sistem
4. Testing
5. Implementasi
6. Evaluasi



Gambar 1. Diagram Alur Penelitian

Penelitian ini diawali dengan studi literatur merupakan Berbagai kegiatan yang berkaitan dengan cara mengumpulkan data perpustakaan, membaca dan mencatat catatan, serta mengelola bahan penelitian. Setelah merampungkan studi literatur selanjutnya masuk kepada tahap analisis kebutuhan yang merupakan proses mendapatkan informasi, mode, dan spesifikasi tentang perangkat lunak yang dibutuhkan pengguna, namun dikarenakan pada penelitian ini tidak menjadikan pengguna sebagai target atau bukan menjadikan hasil penelitian ini sebagai hal yang komersil, maka perancangan hanya sebatas dapat digunakan oleh peneliti untuk diambil kesimpulan. Pemrograman sistem merupakan tahap membuat program menggunakan bahasa pemrograman yang telah direncanakan sebelumnya, pada tahap ini pemrograman dibuat berdasarkan analisis kebutuhan. Setelah menyelesaikan pemrograman sistem maka selanjutnya masuk kepada tahap testing. Tahap testing merupakan tahapan untuk melakukan pemeriksaan apakah masih terdapat galat maupun kesalahan-kesalahan yang besar maupun kecil sebelum dilakukan implementasi, apabila masih terdapat galat serta kesalahan maka pada tahap ini dilakukan juga perbaikan untuk hal-hal tersebut. Pada tahap implementasi dilakukan dengan cara memasukkan sampel yang akan diolah menggunakan program yang telah dirancang. Evaluasi dilakukan untuk keperluan analisa yang selanjutnya ditarik kesimpulan. Penelitian ini menggunakan bahasa pemrograman python dengan perangkat lunak anaconda. Python adalah bahasa pemrograman interpretatif tujuan umum. Tidak seperti bahasa pemrograman lain, Python menekankan keterbacaan kode untuk membuat sintaks lebih mudah untuk dipahami. Hal ini yang mebuatnya mudah untuk dipelajari baik pemula maupun yang telah menguasai bahasa pemrograman lain. Bahasa ini muncul pada tahun 1991, dirancang oleh Guidovan Rossum. Hingga saat ini, Python dikembangkan oleh Python Software Foundation. Bahasa ini mendukung hampir semua sistem operasi.



Gambar 2 Proses Enkripsi

3. Hasil dan Pembahasan

Pada bagian ini dipaparkan mengenai hasil dan pembahasan yang didapat dari tahap testing dan evaluasi.

Enkripsi menggunakan Vigenere Cipher akan mengubah karakter ke dalam bentuk angka yang kemudian akan di proses berdasarkan formula cipher tersebut.

Tabel 2. Tabel Alfabet 26 Karakter

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
0	1	2	3	4	5	6	7	8	9
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
10	11	12	13	14	15	16	17	18	19
U	**V**	**W**	**X**	**Y**	**Z**				
20	21	22	23	24	25				

Pada penelitian ini kata yang akan di enkripsi menggunakan bahasa pemrograman python adalah kata UNIVERSITAS, sehingga apabila di konversi ke bentuk angka yang terdapat pada Tabel 3.

Tabel 3. Konversi Karakter ke Bentuk Angka

U	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**A**	**S**
20	13	8	21	4	15	18	8	19	0	18

Dengan menggunakan kunci ABC yang turut dikonversi ke bentuk angka, sehingga didapatkan hasil konversi pada Tabel 4

Tabel 4. Konversi Karakter Kunci ke Bentuk Angka

A	**B**	**C**
0	1	2

Penetapan kunci akan memberikan satu karakter dari kunci untuk masing-masing karakter pada plaintext yang ditunjukkan pada Tabel 5

Tabel 5. Pembagian Kunci

U	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**A**	**S**
A	B	C	A	B	C	A	B	C	A	B

Dengan menggunakan formula enkripsi Vigenere Cipher yaitu:

$$Ciphertext = Plaintext + Kunci\ (mod\ 26)$$

Apabila dimasukkan ke dalam formula masing masing karakter dapat menghasilkan ciphertext pada masing -masing karakter, sebagai contoh perubahan karakter pada karakter U dari kata UNIVERSITAS yang akan di enkripsi.

$Plaintext = U = 20$
$Kunci = A = 0$
$Ciphertext = Plaintext + Kunci\ (mod\ 26)$
$Ciphertext = 20 + 0\ (mod 26)$
$Ciphertext = 20 = U$

Implementasi enkripsi menggunakan python dilakukan menggunakan perangkat lunak Anaconda, hasil yang didapatkan terdapat pada Gambar 3

Gambar 3 Implementasi Enkripsi dengan Vigenere Cipher

```
Vigenere Cipher.

Teks yang akan di enkripsi berbentuk huruf alfabet
Tekan 1 untuk enkripsi
Tekan 2 untuk dekripsi
Choice: 1
masukkan plainteks: universitas
masukkan kunci: abc
20
14
10
21
5
19
18
9
21
0
19
hasil ciphertext:  UOKVFTSJVAT
```

Hasil yang didapat adalah UOKVFTSJVAT. Berdasarkan literatur yang didapat, bahwa Vigenere cipher sudah dapat dipecahkan, untuk itu maka sebaiknya dilakukan enkripsi lanjutan.

Pada penelitian ini dilakukan enkripsi lanjuran menggunakan Reverse Cipher yang di-implementasikan menggunakan bahasa pemrograman Python juga. Secara tertulis seharusnya hasil yang didapat berupa

Tabel 6. Reverse Cipher

U	O	K	V	F	T	S	J	V	A	T
T	A	V	J	S	T	F	V	K	O	U

Gambar 4 Implementasi Enkripsi dengan Reverse Cipher

```
    tukar = tukar + pesan[i]
    i = i - 1

print(tukar)
```

```
masukkan teks yang akan di enkripsi dengan Reverse Cipher: UOKVFTSJVAT
TAVJSTFVKOU
```

Setelah dilakukan percobaan dengan menggunakan python, maka hasil yang didapat sesuai dengan yang diharapkan. Yaitu berupa pergeseran karakter-karakter tersebut.

4. Kesimpulan

Hasil dari penelitian berupa enkripsi dua kali yaitu menggunakan Vigenere Cipher dan Reverse Cipher dengan tujuan memperkuat enkripsi Vigenere Cipher yang telah dipecahkan adalah berhasil sesuai dengan perhitungan yang dilakukan secara manual. Karakter-karakter asli berhasil berubah sesuai dengan kunci yang dimasukkan saat menggunakan Vigenere Cipher. Sementara untuk cipherteks hasil enkripsi Vigenere Cipher juga berhasil dilakukan transposisi menggunakan Reverse Cipher.

Daftar Pustaka

[1] Y. Yusfrizal, “Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android,” *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[2] A. Dony, *Keamanan Data dan Kriptografi*. Yogyakarta: Penerbit Andi, 2006.

[3] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," *Pseudocode*, vol. 3, no. 2, pp. 129–136, 2017, doi: 10.33369/pseudocode.3.2.129-136.

[4] A. B. Nasution, "Implementasi Pengamanan Data Dengan Menggunakan Algoritma Caesar Cipher Dan Transposisi Cipher," *J. Teknol. Inf.*, vol. 3, no. 1, p. 1, 2019, doi: 10.36294/jurti.v3i1.680.

[5] A. Manaor, H. Pardede, H. Manurung, and D. Filina, "Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi," *J. Tek. Inform. Kaputama*, vol. 1, no. 1, pp. 26–33, 2017.

[6] A. Rizki, S. Rahman, and A. Sembiring, "Implementasi Kriptografi Kombinasi Algoritma Reverse Cipher dan Algoritma Vigenere Cipher untuk Keamanan Pesan Teks Padasi Catatan Berbasis Desktop".