Konsep Three-Pass Protocol Pengamanan Teks Menggunakan Metode Playfair Cipher Dengan Gronsfeld Cipher

Abdurrahman Ridho[1)], Cut Mutia[2)], Andriani Putri[3)]
[1234]Universitas Teuku Umar
E-mail :abdurrahman.ridho@utu.ac.id

Abstrak

Keamanan komputer khususnya data merupakan hal yang tidak dapat terpisahkan dari penggunaan komputer sehari-hari baik itu menggunakan gawai seperti telepon seluler maupun komputer/laptop. Aktifitas enkripsi dapat kita jumpai saat ini pada aplikasi pesan instan seperti whatsapp untuk melindungi privasi penggunanya yang menjamin bahwa pesan teks tersebut aman dari gangguan entitas yang tidak berkepentingan, pengembangan metode-metode enkripsi baik itu memunculkan metode baru maupun mengkombinasikan metode yang sudah ada akan terus dilakukan demi tercapainya perlindungan data yang baik. Konsep Three-pass protocol hadir untuk menghindari adanya pertukaran kunci antara pengirim dan penerima yang dapat menjadi masalah ketika di transmisikan, namun Three-pass protocol tidak dapat diimplementasikan kepada semua cipher.

***Keywords**: Kriptografi, Three-Pass Protocol, Enkripsi, Teks*

1. PENDAHULUAN

Pada penelitian sebelumnya, algoritma playfair tradisional ditingkatkan untuk meningkatkan ketahanannya terhadap serangan melalui perluasan matriks kunci cipher playfair asli menjadi (n × n, n > 10), sedangkan pada penelitian ini dilakukan percobaan menggunakan konsep three-pass protocol bersama dengan Gronsfeld Cipher. [1]

Kriptografi berasal dari bahasa Yunani dengan menggabungkan dua kata yaitu kryptos dan graphein. Kryptos artinya tersembunyi atau rahasia, sedangkan graphein artinya menulis. Arti harfiah dari kriptografi adalah menulis rahasia untuk mengirimkan pesan yang harus dirahasiakan.Kriptografi juga memiliki arti lain, yaitu ilmu tentang teknik penyandian teks biasa (plaintext) secara acak dengan menggunakan kunci penyandian sehingga teks biasa diubah menjadi naskah (plaintext) cipher yang tidak dapat dibaca oleh pihak yang tidak berkepentingan.

Kriptografi klasik adalah kriptografi dalam proses pembangkitan dan analisis yang sama sekali tidak berhubungan dengan komputer atau mesin. Alat yang digunakan melibatkan penggunaan kertas, pulpen, batu, dan alat lain yang sama sekali bukan milik alat mesin modern. Keunikan dari kriptografi klasik adalah didasarkan pada karakter yang lebih banyak, baik karakter tertulis maupun karakter pesan. Ciri lainnya adalah penggunaan alat ini masih tergolong tradisional karena pada saat kemunculannya belum dikenal oleh komputer. Sistem kriptografi klasik hanya terbatas pada keamanan berkaitan dengan distribusi kunci.[2]

Menurut catatan sejarah, kriptografi sudah ada sejak zaman Yunani atau sekitar tahun 400 SM. Alat yang digunakan untuk membuat pesan tersembunyi di Yunani pada saat itu disebut Scytale. Scytale adalah batang silinder dengan 18 kombinasi huruf.

Pada zaman Romawi, pada masa pemerintahan Julius Caesar, penggunaan kriptografi semakin marak karena pertimbangan stabilitas negara. Meskipun teknik yang digunakan tidak secanggih bahasa Yunani, namun cukup sulit untuk memahami pesan kriptografi dari zaman Romawi.

Ada beberapa teknik yang dipakai untuk mempertahankan keamanan & kerahasiaan liputan yang dikirim. Satu berdasarkan mereka merupakan menggunakan kriptografi. Kriptografi merupakan bagian enkripsi buat menciptakan sistem rahasia dalam pengiriman pesan.[3]

Enkripsi adalah suatu cara mengubah bentuk data menjadi suatu kode yang sulit diterjemahkan sehingga tidak dapat dibaca oleh pihak manapun. Data terenkripsi hanya dapat dibaca oleh penerima menggunakan kunci tertentu. Kunci ini bisa didapatkan langsung oleh pembuat dokumen atau data.

Implementasi protokol kriptografi tanpa melakukan pertukaran kunci masih merupakan area yang masih membutuhkan perhatian.[4] Three-pass protocol dalam kriptografi, saat mengirim pesan, adalah skema operasi yang memungkinkan satu pihak menjaga kerahasiaan saat mengirim pesan ke pihak kedua tanpa saling bertukar kunci enkripsi. Hal ini disebabkan pengirim dan penerima pesan melakukan tiga tahap pertukaran untuk mengenkripsi pesan. Konsep dasar dari three-pass protocol adalah masing-masing pihak memiliki kunci enkripsi dan kunci dekripsinya sendiri. Kedua belah pihak menggunakan kunci masing-masing untuk mengenkripsi pesan dan kemudian mendekripsi pesan.

Sandi Gronsfeld adalah enkripsi yang memiliki ciri seperti sandi Vigenère. Cipher ini merupakan algoritma yang hanya menggunakan numeric sebagai key. Key tersebut ditetapkan oleh programmer[5].

Cipher Gronsfeld menggunakan kunci desimal. Kunci tersebut akan diulang secara berkala agar setiap plainteks memiliki kunci. Oleh karena itu, panjang kunci sama dengan plaintext. Ketika pengguna memasukkan kunci dengan panjang kurang dari teks biasa, kunci itu secara otomatis diulang dari awal untuk teks biasa berikutnya. Tabel Gronsfeld berisi alfabet yang ditulis dalam 10 baris, setiap baris bergeser satu urutan ke kiri dari baris sebelumnya, menciptakan kemungkinan 10. Setiap huruf dikodekan dengan baris yang berbeda, bergantung pada jumlah kunci yang dimiliki tabel Gronsfeld. tetapi terkadang Gronsfeld Cipher dapat menggunakan ASCII. Kunci tersebut diulangi secara periodik, sehingga setiap plainteks akan memiliki kunci. Panjangnya akan menyesuaikan pada panjang teks pada pesan aslinya . Jika pengguna memasukkan kunci yang panjangnya lebih kecil daripada plaintext, maka kunci tersebut akan otomatis diulang dari awal ke plaintext berikutnya.[6]

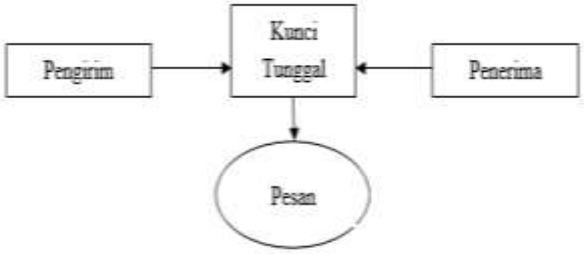
---A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z
0) A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-
1) B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-A-
2) C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-A-B-
3) D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-A-B-C-
4) E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-A-B-C-D-
5) 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-
6) 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-
7) 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-
8) 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-
9) 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-

Gambar 1 Tabel Gronsfeld Cipher

Cipher Playfair atau biasa dikenal dengan Playfair Square adalah teknik kriptografi simetris yang termasuk dalam sistem substitusi ligatur. Sandi Playfair Termasuk dalam sandi poligram. Diciptakan oleh Sir Charles Wheatstone tetapi dipromosikan/dipopulerkan oleh Baron Lyon Playfair pada tahun 1854. Sandi Playfair menyandikan pasangan huruf (ligatur atau ligatur), bukan huruf tunggal seperti sandi klasik/tradisional lainnya. Tujuannya adalah untuk mempersulit analisis frekuensi karena frekuensi huruf dalam ciphertext akan tetap konstan.

2. METODE PENELITIAN

Pertukaran data dalam hal ini pesan rahasia berupa teks menggunakan cara tradisional yaitu dengan bertukar kata kunci yang unik. Diagram di bawah mengilustrasikan bagaimana pertukaran pesan rahasia terjadi menggunakan kunci yang unik.

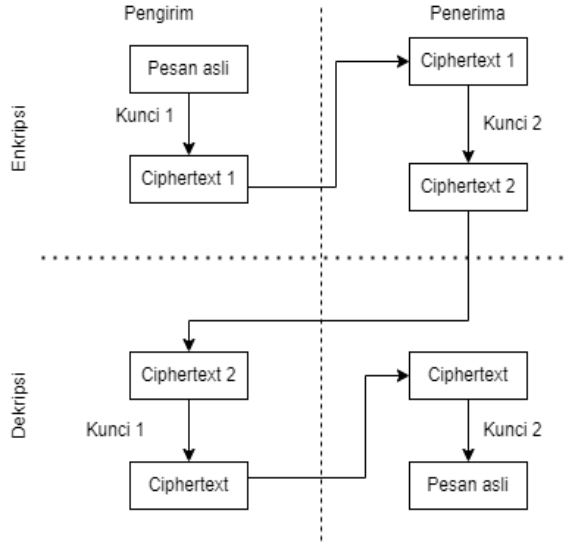


Gambar 2. Skema pengiriman pesan menggunakan kunci tunggal

Menggunakan satu kata kunci dapat menyebabkan kesalahpahaman. Dalam hal ini,

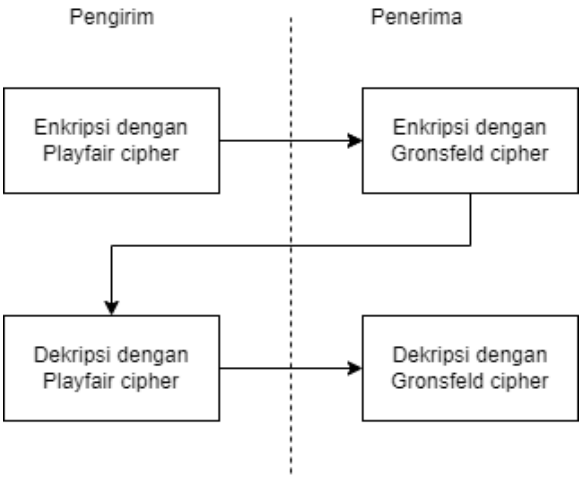
sangat mungkin penerima salah mengartikan kunci yang diberikan oleh pengirim. Selain itu, pertukaran pesan atau kata kunci yang dikirimkan oleh pengirim kepada penerima kemungkinan besar diketahui oleh orang lain sehingga pesan rahasia tersebut dapat diketahui.

Penggunaan three-pass protocol akan meminimalisir terjadinya kebocoran data yang di transmisikan, hal ini dikarenakan pengirim dan penerima tidak perlu bertukar kunci rahasia saat mengirimkan pesan yang merupakan konsep dasar dari Three-Pass Protocol[7]



Gambar 3. Alur Three-pass protocol

Pada penelitian ini pengirim akan menggunakan Playfair cipher, sedangkan penerima akan menggunakan Gronsfeld cipher tanpa berbagi kunci.



Gambar 4. Alur pembagian cipher

3. HASIL DAN PEMBAHASAN

Pada penelitian ini pengiriman pesan diawali menggunakan Playfair Cipher yang digunakan oleh pengirim untuk melakukan enkripsi, kata yang akan di enkripsi pada penelitian ini adalah kata SELAMAT PAGI.

Plainteks : SELAMAT PAGI

Ketentuan menggunakan playfair cipher adalah:

1. Dilakukan pengecekan apakah terdapat huruf J pada plainteks yang akan di enkripsi.
2. Ubah rangkaian teks ke bentuk berpasangan 2 huruf. Maka plainteks yang kita miliki berubah menjadi:

SE LA MA TP AG IX

3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Langkah selanjutnya adalah pemilihan kunci, pilihlah kunci dari kata atau kalimat yang mudah diingat, misal kunci : MEULABOH

Untuk kunci kemudian dilakukan pengecekan apakah terdapat huruf yang sama dalam satu kata atau kalimat tersebut. Bila ada yang sama maka sisakan 1 huruf saja, kemudian susun kata tersebut diikuti dengan huruf dari karakter alfabet yang belum ada kecuali huruf J

MEULABOHCDFGIKNPQRSTVWXYZ

Tabel 1. Kunci playfair

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

Sehingga didapatkan hasil:

Plainteks : SELAMAT PAGI
Bigram : SE LA MA TP AG IX
Kunci :

Tabel 2 Kunci playfair

M	E	U	L	A
B	O	H	C	D

F	G	I	K	N
P	Q	R	S	T
V	W	X	Y	Z

Cipherteks : QL UL AL ST NE RU
Maka didapatkan cipherteks QLULALSTNERU oleh pengirim yang kemudian diteruskan kepada penerima.
Penerima mendapatkan cipherteks yang dikirimkan oleh pengirim kemudian melakukan enkripsi menggunakan Gronsfeld cipher dengan kunci miliknya sendiri, sehingga cipherteks yang didapat kemudian diubah kedalam bentuk angka

Tabel 3. Konversi karakter

Q	L	U	L	A	L	S	T	N	E	R	U
17	12	21	12	1	12	19	20	14	5	18	21

Setelah mengubah cipherteks ke bentuk angka, selanjutnya penerima menetapkan kunci yang akan digunakan, misal penerima menggunakan kunci 1234 sehingga bila dipasangkan dengan angka hasil konversi mendapatkan susunan

Tabel 4. Pemasangan kunci pada setiap karakter

17	12	21	12	1	12	19	20	14	5	18	21
1	2	3	4	1	2	3	4	1	2	3	4

Kemudian dilakukan operasi enkripsi cipherteks menggunakan Gronsfeld Cipher dengan formula

$$Ciphertext = Plainteks + Key\ Mod\ 26$$

Sehingga didapatkan angka cipherteks untuk setiap karakternya.

Tabel 5. Konversi karakter

18	14	24	16	2	14	22	24	15	7	21	25
R	N	X	P	B	N	V	X	O	G	U	Y

Maka penerima mendapatkan ciphertext berupa rangkaian karakter RNXPBNVXOGUY
Karakter hasil enkripsi tersebut kemudian diteruskan kembali kepada pengirim yang akan melakukan dekripsi menggunakan playfair cipher dengan kunci yang sama

Cipherteks : RNXPBNVXOGUY
Bigram : RN XP BN VX OG UY
Kunci :

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

Dekripsi: TI VR DF WY EO LX

Hasil dari dekripsi untuk cipherteks yang dikirimkan oleh penerima mendapatkan hasil:
TIVRDFWYEOLX
Selanjutnya hasil dekripsi yang didapat dari cipherteks sebelumnya dikirimkan kepada penerima dengan tujuan penerima akan mendapatkan pesan aslinya.
Proses dekripsi menggunakan Gronsfeld cipher menggunakan formula

$$Plaintext = Ciphertext - Key\ Mod\ 26$$

Adapun ciphertext yang didapat dari pengirim kemudian diubah terlebih dahulu ke bentuk angka sehingga susunannya menjadi

Tabel 6. Konversi karakter

T	I	V	R	D	F	W	Y	E	O	L	X
20	12	22	18	4	6	23	25	5	15	12	24

Kunci yang digunakan oleh penerima adalah rangkaian angka 1234 , maka setelah rangkaian karakter diubah ke bentuk angka dilakukan pengurangan dengan kunci yang menggunakan formula dekripsi pada Gronsfeld Cipher, sehingga didapatkan pasangan masing-masing karakter dengan kunci

Tabel 7. Pemasangan Kunci

20	12	22	18	4	6	23	25	5	15	12	24
1	2	3	4	1	2	3	4	1	2	3	4

Hasil operasi dekripsi menggunakan formula dekripsi Gronsfeld cipher menghasilkan

19	10	19	14	3	4	20	21	4	13	9	20
S	J	S	N	C	D	T	U	D	M	I	T

Plainteks yang didapatkan dari hasil operasi tersebut adalah rangkaian karakter

S	J	S	N	C	D	T	U	D	M	I	T

Sehingga dapat disimpulkan bahwa penerima tidak dapat membaca pesan asli yang dikirimkan oleh pengirim.

Pada penilitian yang dilakukan didapatkan hasil bahwa konsep Three-pass protocol tidak dapat di jalankan dengan kombinasi kriptografi klasik Playfair cipher dengan Gronsfeld Cipher. Pesan yang diterima oleh penerima pesan berbeda dengan pesan asli yang dikirimkan oleh pengirim.

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan, konsep Three-pass protocol tidak dapat dijalankan dengan menggunakan kombinasi Playfair cipher yang dimiliki oleh pengirim dengan Gronsfeld cipher yang digunakan oleh penerima.

Hasil menunjukkan bahwa pesan yang di dekripsi oleh penerima setelah mengikuti alur konsep three-pass protocol berbeda dengan pesan asli yang dikirimkan oleh pengirim pesan.

5. REFERENSI

[1] M. S. Yousif, R. K. Salih, and N. M. G. Alsaidi, "A new modified playfair cipher," *AIP Conf. Proc.*, vol. 2086, no. April, pp. 2–6, 2019, doi: 10.1063/1.5095132.

[2] G. Li, D. Wang, C. Cao, H. Qin, L. Zhang, and G. Zhao, "Research on the fusion architecture and application mode of quantum cryptography and classic cryptography," *ACM Int. Conf. Proceeding Ser.*, pp. 28–32, 2017, doi: 10.1145/3157737.3157741.

[3] D. Rachmawati, M. A. Budiman, and M. M. Batubara, "Enhancing File Security by using Vigenere Cipher and even Rodeh Code Algorithm," *2018 Int. Conf. Comput. Control. Informatics its Appl. Recent Challenges Mach. Learn. Comput. Appl. IC3INA 2018 - Proceeding*, pp. 54–59, 2019, doi: 10.1109/IC3INA.2018.8629510.

[4] A. G. D. Uchôa, M. E. Pellenz, A. O. Santin, and C. A. Maziero, "A three-pass protocol for cryptography based on padding for wireless networks," *2007 4th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2007*, pp. 287–291, 2007, doi: 10.1109/CCNC.2007.63.

[5] B. O. Sinaga, D. Almahera, and ..., "Pengamanan File Docx Menerapkan Algoritma Gronsfeld," *... Komput. Sains ...*, pp. 438–446, 2020, [Online]. Available: https://www.prosiding.seminar-id.com/index.php/sainteks/article/view/472

[6] Z. Ramadhan and A. P. U. Siahaan, "Protection of Important Data and Information using Gronsfeld Cipher," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 6–10, 2018.

[7] D. Rachmawati, M. A. Budiman, and L. Aulya, "Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 308, no. 1, 2018, doi: 10.1088/1757-899X/308/1/012003.