Edu Komputika 5 (1) (2018)

Edu Komputika Journal

http://journal.unnes.ac.id/sju/index.php/edukom

Pengamanan Teks Pada Dokumen *Email* Menggunakan Enkripsi Rotor

Arief Arfriandi✉

Jurusan Teknik Elektro, Universitas Negeri Semarang

Info Artikel

Sejarah Artikel:

Diterima: 02 Mei 2018

Disetujui: 28 Juni 2018

Dipublikasikan: 20 Juli 2018

Keywords:
email, rotor encryption, cryptography, document, text

Abstrak

Pengiriman surat secara elektronik sangat populer beberapa tahun terakhir ini, sehingga banyak pihak memanfaatkan untuk mengirimkan dokumen penting ke tujuan. Surat elektronik yang biasa disebut dengan email, menggunakan akses internet dalam operasionalnya. Email tersebut ketika dikirim, secara realistis tidak sampai ke tujuan akan tetapi disimpan di server pemilik layanan email. Setelah email tersebut disimpan ke server maka email tersebut dapat dibaca oleh akun email tujuan yang dituliskan saat pengiriman email. Ketika data atau dokumen yang tersimpan di server dapat berpotensi dimanfaatkan oleh penyedia layanan email tanpa seijin pemilik data, hal tersebut tentunya merupakan masalah keamanan data terkait kerahasiaan data. Untuk menjaga kerahasiaan data tersebut, salah satu metode yang dipercaya dapat mengatasi hal tersebut adalah kriptografi. Dalam penelitian ini, peneliti mengembangkan teknik pengamanan teks pada dokumen email menggunakan metode kriptografi dengan algoritma rotor. Metode penelitian yang digunakan berawal dari review literatur untuk mengetahui model pengamanan teks pada dokumen. Kemudian menganalisis kelemahan berdasar penelitian terdahulu terkait pengemanan teks pada dokumen. Langkah berikutnya dilanjutkan dengan desain implementasi enkripsi rotor pada pesan teks yang akan dikirim melalui email serta berlanjut untuk melakukan perhitungan menggunakan enkripsi rotor pada teks dokumen. Hasil pengamanan teks pada dokumen yang akan dikirimkan melalui email, diharapkan dapat meningkatkan kerahasiaan data ketika tersimpan di server email.

Abstract

The delivery of a letter electronically are very popular the last few years, so many people utilize to send important documents to the destination. Electronic mail that is commonly referred to by email, use the internet access in its operation. The email when sent, realistically not up to the destination but kept on the server the owner of email services. After the email is saved to the server then the email can be read by the destination written email account when sending email. When data or documents stored on the server can be potentially exploited by the email service providers without the permission of the owner of the data, it is certainly a security issue related to the data confidentiality of the data. To maintain the confidentiality of such data, one of the methods that is believed to be able to cope with it is Cryptography. In this study, researchers developed a technique of securing text on document email using cryptography method with rotor encryption. Research methods used were derived from a review of the literature to find out the model of the safeguards text in the document. Then analyze the weaknesses of earlier related research based pengemanan the text of the document. The next step is followed by the design of the rotor encryption implementation on the text message and continues to perform calculations using rotor encryption on the text of the document to be sent via email. The results of securing the text in documents that will be sent via email, is expected to enhance the confidentiality of data when stored on the server.
.

✉ Alamat korespondensi:
Gedung E11 Lantai 2 FT Unnes
Kampus Sekaran, Gunungpati, Semarang, 50229
E-mail: arfriandi@mail.unnes.ac.id

ISSN 2252-6811

PENDAHULUAN

Awal tahun 1980, pengiriman surat atau dokumen masih dalam bentuk manual yang dikirimkan dengan sarana media pos. Seiring perkembangan zaman surat dalam bentuk manual mulai tergantikan dengan surat secara elektronik atau yang sering disebut *email*. Hingga saat ini pengiriman *email* sangat populer, sehingga banyak pihak yang memanfaatkannya untuk mengirimkan surat atau dokumen penting ke tujuan. *Email* tersebut menggunakan akses internet dalam operasionalnya. Secara realistis *email* yang dikirim tidak sampai ke tujuan akan tetapi disimpan di *server* atau *cloud storage* pemilik layanan *email* dalam bentuk data digital. Setelah *email* tersebut disimpan di *cloud storage* maka *email* tersebut dapat dibaca oleh akun *email* tujuan yang dituliskan saat pengiriman *email* serta penyedia layanan *email* tersebut. Dengan melihat konsep *email* saat ini maka menimbulkan permasalahan yaitu ketika data digital atau dokumen yang tersimpan di *cloud storage* dapat berpotensi dimanfaatkan oleh penyedia layanan *email* tanpa seijin pemilik data. Berbagai ancaman keamanan terhadap informasi antara lain:

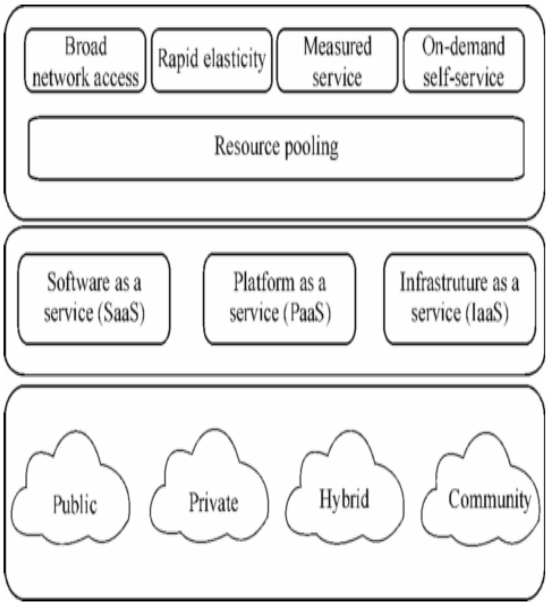
1. Modifikasi
   Modifikasi merupakan salah satu ancaman terkait integritas data dan informasi yang terlibat. Pada proses modifikasi, data atau informasi diubah oleh pihak yang tidak mempunyai kewenangan/akses terhadap informasi tersebut.
2. Pembuatan ulang atau *fabrication*
   Fabrication juga merupakan ancaman terhadap integritas informasi. Pada proses ini, informasi diubah dan dikirimkan ke penerima, akan tetapi penerima tetap beranggapan bahwa data yang dikirim tetap berasal dari pengirim sebenarnya.
3. Penangkapan atau *interception*
   Interception merupakan salah satu ancara terhadap kerahasiaan data. Pada interception, data atau informasi berhasil disadap dan diketahui isinya oleh pihak yang tidak berwenang.
4. Gangguan atau *Interuption*
   Interuption ini merupakan ancaman terhadap ketersediaan data atau informasi, karena pada proses interuption, informasi dihapus dari penyimpanannya. Hal ini menyebabkan pemilik informasi atau data tidak dapat menggunakannya.

Cloud Storage

Mulai awal tahun 1980-an, teknologi *cloud computing* atau komputasi awan semakin sering digunakan di berbagai sektor. *Cloud computing* ini merupakan salah satu kemajuan teknologi informasi, dan informasi tersebut disimpan pada *server* dengan jumlah yang banyak, informasi tersebut dapat diakses melalui berbagai macam perangkat keras serta berbeda *platform* yang terhubung melalui jaringan telekomunikasi. Teknologi *cloud computing* merupakan teknologi yang komplek karena melibatkan berbagai macam sumber daya *hardware* dan *software* yang saling terintegrasi. Dengan adanya *cloud computing*, maka biaya dapat dihemat sehingga lebih efisien serta efektif. Pada *cloud computing* terdapat beberapa layanan antara lain:

1. *Infrastructure as a Service (IaaS)*
   Layanan ini menyediakan sumber daya perangkat keras atau teknologi dasar yang dapat dimanfaatkan oleh pengguna layanan untuk menjalankan *software* yang diperlukan.
2. *Platform as a Service (PaaS)*
   PaaS merupakan salah satu layanan *operating system* atau *platform* tertentu yang memudahkan pengguna layanan tidak perlu memikirkan wadah dari aplikasi atau *software* yang sedang dikembangkan.
3. *Software as a Service (SaaS)*
   Pada layanan ini, pelanggan dapat menggunakan *software* yang secara *online* disediakan oleh penyedia perangkat lunak. Dengan disediakan *software* oleh penyedia layanan tersebut, maka pelanggan tidak memerlukan pembelian *software licenses*.

Framework *cloud computing* ditunjukkan pada Gambar 1 (Peng dkk, 2012).



Gambar 1. Framework *Cloud Computing*

Beberapa karakteristik pada *cloud computing* antara lain : (Zikrul A, 2016)

1. *Resource Pooling*
   Resource yang disediakan oleh penyedia layanan, dapat dipakai pengguna bersama-sama. Sumber daya yang disediakan ini dapat berupa perangkat keras ataupun perangkat lunak.
2. *Broad Network Access*
   Dapat diakses dengan berbagai macam perangkat dan dari berbagai platform melalui jaringan telekomunikasi.
3. *Measured Service*
   Layanan yang disediakan dapat di pantau oleh pengguna secara transparan serta terukur.
4. *Rapid Elasticity*
   Kebutuhan pengguna dapat secara dinamis terpenuhi sesuai dengan keinginan.
5. *Self Service*
   Layanan yang disediakan dapat memenuhi kebutuhan dengan segera secara otomatis.

Definisi yang pasti tentang *cloud storage* sampai saat ini belum jelas, tetapi berdasarkan jenis layanan pada *cloud computing*, maka *cloud storage* merupakan bagian dari *IaaS* (Peng dkk, 2012) (CSA, 2011) . *IaaS* juga mengelola seluruh infrastruktur yang ada pada *cloud computing*. Pada *cloud storage*, data tersimpan dan diakses secara online menggunakan jaringan internet, akan tetapi seiring semakin besarnya data yang disimpan di *cloud storage* maka dapat memunculkan masalah keamanan data terkait kerahasiaan, integritas dan ketersediaan data. Sedangkan *PaaS* memnyediakan layanan pengembangan aplikasi yang dikembangkan oleh konsumen. *SaaS* bertugas menyediakan aplikasi yang siap digunakan oleh konsumen secara *online*.

Berbagai ancaman terkait keamanan data pada *cloud storage* antara lain:

1. Penyedia layanan *cloud storage* tidak menjamin bahaya terkait penyadapan akun.
2. Penyedia layanan *cloud storage* tidak menjamin terkait tidak adanya pencurian data digital
3. Penyedia layanan *cloud storage* tidak menjamin untuk menggunakan atau memanfaatkan data digital yang tersimpan untuk kepentingan tertentu.

Kriptografi

Untuk menjaga kerahasiaan data tersebut, salah satu metode yang dipercaya dapat mengatasi hal tersebut adalah kriptografi (Peng dkk, 2012).

Salah satu tujuan dari kriptografi adalah menyediakan metode untuk mencegah serangan pada data (Mc Donald, 2009). Pada dasarnya metode kriptografi terdiri dari beberapa bagian, antara lain:

1. *Plaintext* atau teks asli
   Merupakan teks asli atau hasil pesan acak yang telah di deskripsi. *Plaintext* ini merupakan pesan yang dapat dibaca.
2. Enkripsi
   Proses mengacak pesan menggunakan algoritma tertentu, sehingga pesan asli mencadi kabur atau acak sehingga tidak

bisa dibaca oleh pihak yang tidak diijinkan.

3. Kunci
   Kunci pada metode kriptografi terbagi menjadi dua macam yaitu *symetric key* dan *asymetric key*. *Symetric key* merupakan kunci yang sama dan identik ketika digunakan pada proses enkripsi dan deskripsi pesan. *Symetric key* ini biasanya dikirim melalui jalur aman atau jalur rahasia. Sedangkan *asymetric key* merupakan kunci berbeda yang digunakan pada proses enkripsi dan deskripsi. *Asymetric key* terdiri dari kunci umum yang dikirimkan melalui jalur terbuka dan kunci rahasia yang dikirim melalui jalur rahasia. Fungsi dari kunci umum, digunakan untuk proses enkripsi *plaintext* dan kunci rahasia berfungsi untuk proses deskripsi *ciphertext*.
4. *Ciphertext*
   Hasil proses enkripsi yang berupa teks acak atau pesan yang tidak bisa dibaca
5. Deskripsi.
   Proses mengubah pesan acak menjadi pesan asli.
6. Kriptanalis
   Proses menganalisa *ciphertext* agar dapat diketahui pesan aslinya atau *plaintext* menggunakan metode tertentu. Proses ini juga berfungsi untuk mengetahui kekurangan metode kriptografi yang digunakan.

Pada proses enkripsi dan deskripsi tersebut, dapat menggunakan algoritma kriptografi tertentu yang telah ditentukan oleh pengirim dan penerima pesan sebelumnya. Kedua proses tersebut membutuhkan kunci agar algoritma pada kriptografi dapat berjalan. Berbagai macam algoritma ada pada metode kriptografi. Beberapa algoritma pada metode kriptografi tersebut dapat berbasis substitusi maupun transposisi. Algoritma berbasis substitusi mempunyai cara kerja mengganti karakter dengan karakter lainnya dengan kunci yang telah ditentukan. Sebagai pengganti karakter dapat berupa alfabet, maupun karakter lain. Salah satu contoh algoritma pada metode kriptografi yang berbasis subtitusi adalah algoritma rotor. Sedangkan algoritma berbasis transposisi cara kerjanya adalah dengan menukar posisi dari karakter berdasarkan algoritma transposisi tertentu dengan tidak menghilangkan karakter asli atau mengganti karakter aslinya.

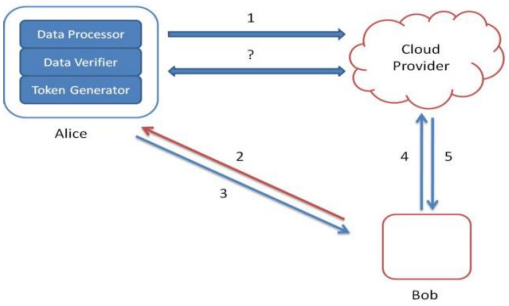
Beberapa penelitian terkait kriptografi antara lain Claude Shannon yang disebutkan pada penelitian yang dilakukan Hill (Hill, 2008), bahwa Shannon mengembangkan tiga metode kriptografi. Ketiga metode kriptografi tersebut adalah *multistage*, substitusi dan transposisi. Selain itu Shannon juga menciptakan *unicity distance* yang merupakan salah satu metode kriptografi menggunakan *metric.* Prinsip dasar pada *unicity distance* tersebut yang digunakan oleh IBM dalam standar enkripsi keamanan data dan sekaligus mengawali era kriptografi modern. Dengan mulai digunakannya prinsip dasar pada *unicity distance* pada standar keamanan data IBM, maka peneliti-peneliti lainnya juga ikut mengembangkan metode kriptografi modern yang dipengaruhi oleh prinsip dasar tersebut. Salah satunya adalah Whitfield Diffie dan Martin Hellman yang mengembangkan metode kriptografi dengan menggunakan *asymetric-key cipher system* (*public key*) dan berlanjut dengan ditemukannya metode *Prety Good Privacy* (PGP) oleh Phil Zimmerman yang berfungsi untuk mengenkripsi *scheme* di jaringan internet. PGP tersebut merupakan dasar dari pengembangan algoritma RSA yang menjadi bagian dari algoritma *Data Encryption Standard* (DES). Algoritma DES, menggunakan sistem *block cipher*. *Block cipher* mempunyai konsep membagi pesan ke dalam beberapa *block* dengan masing-masing *block* mempunyai panjang bervariasi yaitu 64 *bit* dan 56 *bit*. Beberapa penelitian tentang metode kriptografi substitusi telah dilakukan oleh peneliti. Salah satunya adalah penelitian yang dilakukan oleh Putu H (2012), yang mengimplementasikan algoritma *vigenere* dengan cara mengenkripsi data yang ada pada *database*. Berbeda dengan penelitian

sebelumnya, Fidelis (2015) melakukan penelitian kriptanalisis, yaitu berusaha memecahkan *cipher teks* yang telah dienkripsi menggunakan algoritma *columnar*. Penelitian yang dilakukan oleh Fidelis (2015) tersebut bertujuan untuk menguji keamanan enkripsi menggunakan algoritma *columnar*. Metode yang digunakan untuk kriptanalisis adalah dengan menggunakan *brute force attack* serta *kasiski*. Metode *brute force attack* adalah suatu metode untuk memecahkan *cipher teks* dengan cara mencoba secara berulang-ulang. Sedangkan metode *kasiski* bertujuan untuk memecahkan cipher teks dengan cara mencari *cipher teks* yang muncul secara periodik.

Penelitian terkait pengamanan *cloud storage* dengan metode kriptografi telah dilakukan sebelumnya. Salah satunya adalah penelitian yang dilakukan oleh Kamara,dkk (2010) yang menjelaskan tentang arsitektur pengamanan *cloud storage*. Pada arsitektur pengamanan tersebut dijelaskan bahwa terdapat beberapa komponen utama yaitu:

1. Data *processor*
2. Data *verifier*
3. Token generator

Data *processor* berfungsi untuk memproses data digital yang akan disimpan ke dalam *cloud storage*, sedangkan data *verifier* bertugas memverifikasi data digital sebelum diubah. Hal ini berfungsi untuk menjaga integritas data. Fungsi dari token generator adalah membuat atau meng-*generate* kunci atau token yang menghubungkan penyedia layanan *cloud storage* dengan *user* yang menggunakannya. Skema pengamanan data pada *cloud storage* yang dilakukan oleh Kamara,dkk (2010), ditunjukkan pada Gambar 2.



Gambar 2. Skema teknik pengamanan yang dilakukan oleh Kamara,dkk (2010).

Pada skema tersebut menunjukkan bahwa pengirim (Alice) selain mengirimkan data ke *cloud storage*, pengirim juga memberikan token hasil generate kepada penerima (Bob). Token tersebut juga akan diberikan ke penyedia layanan *cloud storage* yang berfungsi untuk mencari data yang tersimpan. Sebelum data tersebut disimpan di *cloud storage*, data digital tersebut di enkripsi menggunakan algoritma enkripsi yang telah disepakati bersama antara pengirim dan penerima. Pada penelitian yang lain yang dilakukan oleh Jamgekar (2013), menjelaskan bahwa sebelum data disimpan di *cloud storage* maka data tersebut dienkripsi dahulu menggunakan algoritma kriptografi RSA. Beberapa teknik kriptografi lainnya yang berfungsi untuk mengamankan data antara lain (Rajasudhan, 2014):

1. enkripsi berbasis identifikasi
2. enkripsi *homomorphic*
3. enkripsi berbasis atribut

Penelitian yang dilakukan oleh Blasco (2015), menjelaskan bahwa sebelum data dikirimkan, data digital tersebut dienkripsi secara bertingkat. Hal tersebut akan membuat data digital sulit dibaca meskipun data tersebut berhasil dicuri.

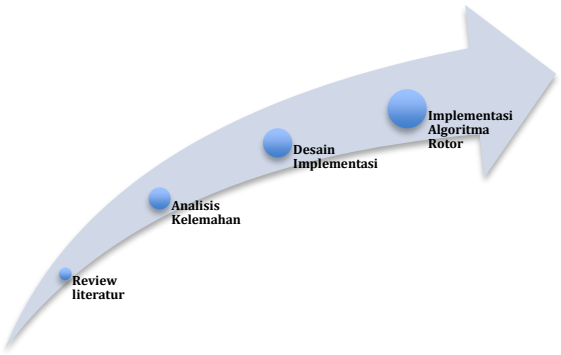
Penelitian-penelitian sebelumnya belum pernah dilakukan pengamanan teks pada *email* menggunakan algoritma rotor. Sehingga dalam penelitian ini, peneliti mengembangkan teknik pengamanan teks pada dokumen *email* menggunakan metode kriptografi dengan algoritma rotor

Enkripsi Rotor

Beberapa proses yang ada pada metode kriptografi adalah enkripsi dan deskripsi. Enkripsi adalah proses mengaburkan data awal yang dapat berupa teks atau angka agar tidak dapat dibaca oleh pihak yang tidak diberikan ijin, sedangkan deskripsi adalah proses mengubah data yang telah dikaburkan ke bentuk aslinya atau menjadi data awal. Terdapat proses enkripsi yang digunakan pada metode kriptografi, salah satunya adalah enkripsi rotor. Kunci pada enkripsi ini selalu berubah seperti rotor atau berputar. Kriptografi jenis ini merupakan kriptografi berbasis subtitusi atau mengganti karakter awal dengan karakter lainnya sesuai dengan kunci yang telah dibentuk. Ketika menggunakan enkripsi rotor, maka pengenkripsi dan pendeskripsi harus menyepakati posisi awal putaran dan beberapa kunci subtitusi yang digunakan. Kunci yang digunakan dikirimkan melalui jaringan aman dan hasil enkripsi atau *chiperteks* dikirim melalui jaringan terbuka ke tujuan. Enkripsi rotor ini sulit dipecahkan menggunakan teknik *brute force*, karena kunci yang digunakan selalu berubah dan ruang kunci yang digunakan adalah 26!. Salah satu metode serangan lain yang sering digunakan untuk memecahkan hasil enkripsi adalah dengan metode statistik. Metode statistik yang digunakan untuk memecahkan hasil enkripsi dari enkripsi rotor juga tidak bisa dilakukan karena statistik kemunculan karakter teks asli tidak ada pada hasil enkripsi (Rifki Sadikin, 2012).

METODE PENELITIAN

Metode penelitian yang digunakan cenderung menggunakan metode pengembangan prototipe pengamanan data digital, dan langkah penelitian ditunjukkan pada Gambar 3.



Gambar 3. Langkah pengembangan teknik pengamanan data

Langkah penelitian berawal dari *review* literatur untuk mengetahui model pengamanan teks pada dokumen. Kemudian menganalisis kelemahan berdasar penelitian terdahulu terkait pengemanan teks pada dokumen. Langkah berikutnya dilanjutkan dengan desain implementasi enkripsi rotor pada pesan teks serta berlanjut untuk melakukan perhitungan menggunakan enkripsi rotor pada teks dokumen yang akan dikirim melalui *email*.

HASIL DAN PEMBAHASAN

Pesan teks pada *email* yang akan diamankan terdiri dari beberapa kalimat. Pada kalimat tentunya terdapat spasi, dalam hal ini spasi akan digantikan dengan karakter " Z ". Pesan teks yang akan dienkripsi adalah " PEMERIKSAAN PELAKU AKAN DILAKSANAKAN HARI RABU ". Kemudian pada algoritma rotor ini dapat menggunakan kunci subtitusi yang dapat secara bebas ditentukan sejak awal tanpa ada ketentuan tertentu sehingga dapat digunakan berapapun kunci subtitusinya, sebagai contoh kunci subtitusi yang digunakan adalah 6 kunci subtitusi yaitu:

K0 = {D,U,K,R,L}
K1 = {E,G,F,X,W}
K2 = {Y,T,W,Q,P}
K3 = {J,V,B,C,M}
K4 = {Q.D.H.K.H}
K5 = {Y,T,M,I,S}

Kemudian posisi awal putaran adalah 0. Untuk menghilangkan spasi maka karakter spasi diganti dengan karakter " Z ", sehingga pesan teks asli menjadi:"PEMERIKSAANZPELAKUZAKA NZDILAKSANAKANZHARIZRABU"
Hasil dari subtitusi pesan teks alfabet dengan enkripsi rotor ditunjukkan pada Tabel 1.

Tabel 1. Hasil Subtitusi Pesan Teks Alfabet

i	Posisi Putaran	P[i]	C[i]
0	0	P	K0(P) = D
1	1	E	K1(E) = W
2	2	M	K2(M) = W
3	3	E	K3(E) = M
4	4	R	K4(R) = H
5	5	I	K5(I) = I
6	0	K	K0(K) = D
7	1	S	K1(S) = X
8	2	A	K2(A) = Y
9	3	A	K3(A) = J
10	4	N	K4(N) = K
11	5	Z	K5(Z) = Y
12	0	P	K0(P) = D
13	1	E	K1(E) = W
14	2	L	K2(L) = T
15	3	A	K3(A) = Y
16	4	K	K4(K) = Q
17	5	U	K5(U) = Y
18	0	Z	K0(Z) = D
19	1	A	K1(A) = E
20	2	K	K2(K) = Y
21	3	A	K3(A) = J
22	4	N	K4(N) = K
23	5	Z	K5(Z) = Y
24	0	D	K0(D) = R
25	1	I	K1(I) = X
26	2	L	K2(L) = T
27	3	A	K3(A) = J
28	4	K	K4(K) = Q
29	5	S	K5(S) = I
30	0	A	K0(A) = D
31	1	N	K1(N) = X
32	2	A	K2(A) = Y
33	3	K	K3(K) = J
34	4	A	K4(A) = Q
35	5	N	K5(N) = I
36	0	Z	K0(Z) = D
37	1	P	K1(P) = E
38	2	A	K2(A) = Y
39	3	D	K3(D) = C
40	4	A	K4(A) = Q
41	5	Z	K5(Z) = Y
42	0	H	K0(H) = K
43	1	A	K1(A) = E
44	2	R	K2(R) = W
45	3	I	K3(I) = C
46	4	Z	K4(Z) = Q
47	5	R	K5(R) = M
48	0	A	K0(A) = D
49	1	B	K1(B) = G
50	2	U	K2(U) = Y

Dari hasil subtitusi tersebut maka diperoleh teks enkripsi yaitu:
"DWWMHIDXYJKYDWTYQYDEYJKYRX TJQIDXYJQIDEYCQYKEWCQMDGY "
Kemudian untuk pesan angka saja, proses enkripsi juga hampir sama, tetapi yang membedakan hanya kunci yang digunakan. Pesan teks berupa angka yang akan di enkripsi adalah:"98234610928341208312759237587234871923669283135729 7 "
Kunci subtitusi yang digunakan adalah 6 kunci subtitusi yaitu:
K0 = {4,3,5,7,9}
K1 = {9,7,4,3,2}
K2 = {8,1,3,2,6}
K3 = {8,5,6,1,2}
K4 = {2.5.8.9.7}
K5 = {3,7,8,1,9}
Hasil dari subtitusi pesan teks angka dengan enkripsi rotor ditunjukkan pada Tabel 2.

Tabel 2. Hasil Subtitusi Pesan Teks Angka

i	Posisi Putaran	P[i]	C[i]
0	0	9	K0(9) = 9
1	1	8	K1(8) = 3
2	2	2	K2(2) = 3
3	3	3	K3(3) = 1
4	4	4	K4(4) = 7
5	5	6	K5(6) = 7
6	0	1	K0(1) = 3
7	1	0	K1(7) = 9

8	2	9	K2(9) = 6
9	3	2	K3(2) = 6
10	4	8	K4(8) = 8
11	5	3	K5(3) = 1
12	0	4	K0(4) = 9
13	1	1	K1(1) = 7
14	2	2	K2(2) = 3
15	3	0	K3(0) = 8
16	4	8	K4(8) = 8
17	5	3	K5(3) = 1
18	0	1	K0(1) = 3
19	1	2	K1(2) = 4
20	2	7	K2(7) = 1
21	3	5	K3(5) = 2
22	4	9	K4(9) = 7
23	5	2	K5(2) = 8
24	0	3	K0(3) = 7
25	1	7	K1(7) = 7
26	2	5	K2(5) = 8
27	3	8	K3(8) = 6
28	4	7	K4(7) = 5
29	5	2	K5(2) = 8
30	0	3	K0(3) = 7
31	1	4	K1(4) = 2
32	2	8	K2(8) = 3
33	3	7	K3(7) = 5
34	4	1	K4(1) = 5
35	5	9	K5(9) = 9
36	0	2	K0(2) = 5
37	1	3	K1(3) = 3
38	2	6	K2(6) = 8
39	3	6	K3(6) = 8
40	4	9	K4(9) = 7
41	5	2	K5(2) = 8
42	0	8	K0(8) = 5
43	1	3	K1(3) = 3
44	2	1	K2(1) = 1
45	3	3	K3(3) = 1
46	4	5	K4(5) = 2
47	5	7	K5(7) = 7
48	0	2	K0(2) = 5
49	1	9	K1(9) = 2
50	2	7	K2(7) = 1

Dari hasil subtitusi tersebut maka diperoleh hasil enkripsi yaitu: "9331773966819738813412787786587235595387853112752 1 "

Untuk pesan alfabet dan angka, pesan yang akan dienkripsi adalah " HARI INI KODE YANG AKAN DIKIRIM ADALAH 777777 ". kunci subtitusi yang digunakan yaitu:

K0 = {A,3,H,7,K}
K1 = {9,F,4,N,2}
K2 = {C,1,3,2,R}
K3 = {E,W,6,P,2}
K4 = {2.5.D.9.V}
K5 = {3,X,8,N,M}

Dan untuk menghilangkan karakter spasi, maka karakter spasi diganti dengan karakter " Z ". Sehingga pesan asli menjadi "HARIZINIZKODEZYANGZAKANZDIKIRIMZADALAHZ777777 "

Hasil dari subtitusi pesan teks alfabet dan angka ditunjukkan pada Tabel 3.

Tabel 3. Hasil Subtitusi Pesan Teks Alfabet dan Angka

i	Posisi Putaran	P[i]	C[i]
0	0	H	K0(H) = H
1	1	A	K1(A) = 9
2	2	R	K2(R) = 3
3	3	I	K3(I) = P
4	4	Z	K4(Z) = 2
5	5	I	K5(I) = N
6	0	N	K0(N) = 7
7	1	I	K1(I) = N
8	2	Z	K2(Z) = C
9	3	K	K3(K) = E
10	4	O	K4(O) = V
11	5	D	K5(D) = N
12	0	E	K0(E) = K
13	1	Z	K1(Z) = 9
14	2	Y	K2(Y) = R
15	3	A	K3(A) = E
16	4	N	K4(N) = 9
17	5	G	K5(G) = X
18	0	Z	K0(Z) = A
19	1	D	K1(D) = N
20	2	I	K2(I) = 2
21	3	K	K3(K) = E

22	4	I	K4(I) = 9
23	5	R	K5(R) = 8
24	0	I	K0(I) = 7
25	1	M	K1(M) = 4
26	2	Z	K2(Z) = C
27	3	A	K3(A) = E
28	4	D	K4(D) = 9
29	5	A	K5(A) = 3
30	0	L	K0(L) = 3
31	1	A	K1(A) = 9
32	2	H	K2(H) = 3
33	3	Z	K3(Z) = E
34	4	7	K4(7) = 9
35	5	7	K5(7) = N
36	0	7	K0(7) = 7
37	1	7	K1(7) = N
38	2	7	K2(7) = 2
39	3	7	K3(7) = P

Dari hasil subtitusi tersebut maka diperoleh hasil enkripsi yaitu

“

H93P2N7NCEVNK9RE9XAN2E9874CE9339 3E9N7N2P ”.

Proses subtitusi atau untuk memperoleh hasil teks enkripsi maka setiap kunci subtitusi yang digunakan menyesuaikan dengan awal putaran atau jumlah putaran yang telah ditentukan sejak awal, sehingga memungkinkan kunci yang digunakan dapat berbeda pada setiap karakter. Putaran yang digunakan putaran atau rotor 6 posisi, ketika digunakan maka posisi selalu berputar dari posisi 0,1,2,3,4,5 kemudian kembali lagi ke posisi 0 dan seterusnya. Saat putaran pada posisi 4, maka digunakan kunci subtitusi 4, dan ketika posisi 2, digunakan kunci posisi 2, begitu seterusnya dengan mempertimbangkan urutan huruf pada alfabet dan angka. Proses subtitusi ini berlaku juga jika putaran yang digunakan berbeda dan jumlah subtansi kunci subtitusinya. Pada pesan teks serta kunci angka, maka perhitungan pertama pada banyaknya angka, bermula dari angka “0”. Jika alfabet dan angka digabungkan, maka banyaknya karakter merupakan gabungan antara keduanya, akan tetapi ururan perhitungan dimulai dari alfabet kemudian angka, sehingga total karakter sebanyak 36 karakter. Kunci yang digunakan merupakan gabungan dari alfabet dan angka.

SIMPULAN

Pada penelitian ini telah dilakukan pengamanan teks pada dokumen yang dikirimkan melalui *email*. Pengamanan yang dilakukan menggunakan metode kriptografi dengan enkripsi rotor. Contoh jumlah kunci subtitusi yang digunakan sebanyak 6 kunci dan subtansi masing-masing kunci sebanyak 5 karakter. Hasil pengamanan teks pada dokumen yang akan dikirimkan melalui *email* tersebut, diharapkan dapat meningkatkan kerahasiaan data ketika tersimpan di *server* atau *cloud storage*. Sehingga dapat mencegah pihak yang tidak diijinkan untuk memanfaatkan data digital yang tersimpan di *server* atau *cloud storage* milik penyedia layanan *email*. Pada penelitian ini belum dilakukan enkripsi bertingkat menggunakan beberapa enkripsi secara berurutan, sehingga pada penelitian selanjutnya dapat digunakan beberapa algoritma yang dijalankan secara berurutan untuk mengamankan teks pada dokumen yang akan dikirim melalui *email.*

DAFTAR PUSTAKA

Bhattacharya, T. , T.K. Bhattacharya, dan S.R. Bhadra Chaudhuri. 2009. A General Bit Level Data Enryption Technique using Helical & Session Based Columnar Transpositions. *IEEE International Advance Computing Conference:* 364-368.

Blasco, J., et al. 2015. “Hidering Data Thef With Encrypted data Trees”, The Journal of Systems and Software, p 147-158.

Churchhouse, R. 2004.*Codes and Ciphers.*1st ed United Kingdom : The Press Syndicate Of The University Of Cambridge.

Cloud Security Alliance. 2011. “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,” Cloud Secure. Alliance, vol. 3, p. 155.

Cohen, F. 1995. *Short History of Cryptography.*1st ed United States : Fred Cohen & Associates.

D. Mukhopadhyay, G. Sonawane, P. S. Gupta, S. Bhavsar, and V. Mittal. 2013. "Enhanced Security for Cloud Storage using File Encryption.".

Fidelis V.A. 2015. Kriptanalisis Algoritma Transposisi Columnar, Skripsi, Tidak diterbitkan, Fakultas Sains dan Teknologi, Universitas Sanata Dharma : Yogyakarta.

Forouzan,B.A. dan S.C. Fegan. 2007. *Data Communication and Networking*. 4th ed McGraw-Hill Companies, Inc. New York.

Hill, C.J. dan Life Senior Member IEEE. 2008 . *Vigenere through Shannon to Planck-a Short History of Elcetronic Cryptographic Systems*. Journal of Cranfield University. 1(8) : 41-46.

Jamgekar, R.S., Joshi, G.S. 2013. "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering, Vol-1, Issue-4.

McDonald, N.G. 2009. Past, Present, And Future Methods of Cryptography and Data Encryption. Research Review. Utah : Deparment of Electrical and Computer Engineering University of Utah.

Meena, R. 2015. Automated Teller Machine – Its Benefit and Challenges. International Journal Commerce, Business and Management : 815-821.

Pramanik, M.B. 2014. Implementation of Cryptography Technique using Columnar Transposition. International Journal of Computer Application :19-23.

Pratama, G.M. dan E.N. Tamatjita. 2015. Modifikasi Algoritma Vigenere Cipher Menggunakan Metode Catalan Number dan Double Columnar Transposition. Jurnal Sekolah Tinggi Teknologi Adisutjipto Yogyakarta 4(1) : 31-40.

Putu, H.A., Rahayu, T.P., Yakub, Hariyanto. 2012. "Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher", SENTIKA, p. 164.

Rajasudhan, S., Nallusamy, R. 2014. "A Study on Cryptography Methods in Cloud Storage", International Journal of Communication and Computer Technologies, Vol 02-No.01, Issue:02.

Rifki Sadikin. 2012. Kriptografi Untuk Keamanan Jaringan, Yogyakarta, Penerbit Andi.

S. Kamara and K. Lauter. 2010. "Cryptographic Cloud Storage," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6054 LNCS, pp. 136–149.

Wenbo Mao Hewlett-Packard Company. 2003. Modern Cryptography : Theory and Practice. July.New Jersey : Prentice Hall PTR.

Wilson, P.I dan M. Garcia. 2006. A Modified Version of the Vigenere Algorithm. Internasional Journal of Computer Science and Network Security 6(3B) : 140-143.

Y. Peng, W. Zhao, F. Xie, Z. H. Dai, Y. Gao, and D. Q. Chen. 2012. "Secure Cloud Storage Based On Cryptographic Techniques," J. China Univ. Posts Telecommun., vol. 19, no. October, pp. 182–189.