Jurnal UJMC, Volume 6, Nomor 1, Hal. 39 - 46
pISSN : 2460-3333 eISSN : 2579-907X

Penggunaan Algoritma *Vigenere Cipher* dan *RSA (Rivest-Shamir-Adleman)* Untuk Keamanan Data Pembelian di PT Lamongan Marine Industry

Fifin Nur Aini[1], Siti Amiroch[2], Novita Eka Chandra[3]

[1]Universitas Islam Darul 'ulum Lamongan, fifinna237@gmail.com
[2] Universitas Islam Darul 'ulum Lamongan, siti.amiroch@unisda.ac.id
[3] Universitas Islam Darul 'ulum Lamongan, novitaeka@unisda.ac.id

Abstract. Purchasing data is very important for business actors because the data is very influential on companies, especially in the field of production and marketing. Therefore, the purchase data is one of the things that is kept secret by the business actors, such as PT Lamongan Marine Industry. With current technology hackers can easily hack such data, so the use of cryptography is a very appropriate solution to this problem. In this study the authors used the Vigenere Cipher algorithm and the RSA algorithm with a high security key. The hacker was not easy to find out the contents of the data. The data obtained is a purchase order, then presented in tabular form. The data is then encrypted and decrypted so that the comparison of the two algorithms is known. The results of the analysis state that the Vigenere Cipher algorithm is more effective in both encryption and decryption processing time. Ciphertext generated from the encryption process of the Vigenere Cipher algorithm is mostly in the form of punctuation, while the ciphertext generated by the RSA algorithm from the encryption process is mostly in alphabetical letters. The ciphertext generated by the RSA algorithm depends on the value of the modulo. but in terms of security the RSA algorithm is superior to the Vigenere Cipher algorithm.

***Keywords*:** *Vigenere Cipher, RSA, Purchase Data*

Abstrak. Data pembelian merupakan hal yang sangat penting bagi pelaku usaha karena data tersebut sangat berpengaruh pada perusahaan khususnya dalam bidang produksi dan pemasaran produk. Oleh karena itu data pembelian menjadi salah satu hal yang sangat dirahasiakan oleh sebuah intansi pelaku usaha, seperti PT Lamongan *Marine Industry*. Dengan teknologi saat ini peretas pun dapat meretas data tersebut dengan mudah, sehingga penggunaan kriptografi merupakan solusi yang sangat tepat untuk permasalahan tersebut. Dalam penelitian ini penulis menggunakan algoritma *Vigenere Cipher* dan algoritma *RSA* dengan kunci keamanan yang cukup tinggi peretas tidak mudah untuk mengetahui isi dari data tersebut. Data yang diperoleh adalah *purchase order*, kemudian disajikan dalam bentuk tabel. Data tersebut kemudian dienkripsi dan didekripsi agar diketahui perbandingan dari kedua algoritma tersebut. Hasil analisis menyatakan bahwa algoritma *Vigenere Cipher* lebih efektif dalam waktu proses enkripsi maupun dekripsi. *Ciphertext* yang dihasilkan dari proses enkripsi algoritma *Vigenere Cipher* lebih banyak berupa tanda baca, sedangkan ciphertext yang dihasilkan algoritma *RSA* dari proses enkripsi lebih banyak berupa huruf abjad. *Ciphertext* yang dihasilkan algoritma *RSA* bergantung pada besarnya nilai modulo. Namun dalam hal keamanan algoritma *RSA* lebih unggul dari algoritma *Vigenere Cipher*.

***Kata Kunci*:** *Vigenere Cipher, RSA, Data Pembelian*

1 Pendahuluan

Keamanan data dan informasi merupakan hal sangat penting di era globalisasi saat ini. Pada umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh dilihat oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan seringkali dapat disadap oleh pihak lain.

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Para pelaku atau praktisi kriptografi disebut *cyrptographers*. Sebuah algoritma kriptografi (*cryptographic algorithm*) disebut cipher merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya persamaan kedua matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat [1].

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Nama *Vigenere* sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama *Vigenere* diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma tersebut dengan metode *autokey cipher* meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista [2].

Algoritma *RSA* ditemukan pertama kali oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1978. Nama *RSA* merupakan singkatan dari inisial nama mereka. Algoritma *RSA* merupakan algoritma kriptografi asimetris yang mempunyai dua kunci yaitu kunci publik dan kunci rahasia. Hingga saat ini algoritma *RSA* merupakan salah satu algoritma yang paling maju dalam bidang kriptografi.

Algoritma *Vigenere Cipher* dan algoritma *RSA* merupakan dua algoritma yang sangat berbeda. Perbedaan dari kedua algoritma tersebut adalah kunci yang digunakan untuk proses enkripsi dan dekripsi. Untuk proses enkripsi dan dekripsi algoritma *Vigenere Cipher* menggunakan kunci yang sama, sedangkan untuk algoritma *RSA* menggunakan kunci yang berbeda. Proses dan hasil penyandian yang dihasilkan dari kedua algoritma tersebut juga akan sangat berbeda, untuk itu dalam penelitian ini penulis akan membandingkan proses penyandian maupun pembentukan kunci dari kedua algoritma tersebut.

Penelitian sebelumnya terkait algoritma *RSA* dilakukan oleh [3], melakukan beberapa uji coba dengan kode hufman dan ASCII, disimpulkan bahwa kode huffman lebih cepat dalam proses penyandian dari pada kode ASCII.

Data pembelian merupakan hal yang sangat penting bagi pelaku usaha karena data tersebut sangat berpengaruh pada perusahaan khususnya dalam bidang produksi dan pemasaran produk. Oleh karena itu data pembelian menjadi salah satu hal yang sangat dirahasiakan oleh sebuah intansi pelaku usaha, seperti PT Lamongan *Marine Industry*. Dengan teknologi saat ini penyadap pun dapat menyadap data tersebut dengan mudah, sehingga penggunaan kriptografi merupakan solusi yang sangat tepat untuk permasalahan tersebut. Dengan menggunakan algoritma *Vigenere Cipher* dan algoritma *RSA* dengan kunci keamanan yang cukup tinggi penyadap tidak mudah untuk mengetahui apa isi dari data tersebut. Untuk itu dalam penelitian ini bertujuan untuk membandingkan

algoritma *Vigenere Cipher* dan algoritma *RSA* dalam proses-proses penyandian maupun hasil yang diperoleh.

2 Tinjauan Pustaka

Pembelian adalah serangkaian tindakan untuk mendapatkan barang dan jasa melalui pertukaran dengan maksud untuk digunakan sendiri atau dijual Kembali [4]. Dokumen yang digunakan dalam proses pembelian diantaranya: surat permintaan pembelian, surat permintaan penawaran harga., surat order pembelian, laporan penerimaan barang, surat perubahan *order* pembelian, dan bukti kas keluar.

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan [5].

Proses yang dilakukan untuk mengubah *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *encipherment*, sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut dekripsi (*decryption*) atau *decipherment.*

Vigenere cipher ditemukan oleh Giovan Battista Bellaso pada tahun 1553 dan dikembangkan oleh Blaisede Vigenere. *Vigenere Cipher* menggunakan bujur sangkar *vigenere* dan perhitungan [6] sebagai berikut:

$$C_i = (P_i + K_i) \ mod\ 26\,,$$

Sedangkan rumus untuk dekripsi adalah:

$$P_i = (C_i - K_i) \ mod\ 26$$

dengan

Ci = nilai desimal karakter *ciphertext* ke-i.

Pi = nilai desimal karakter *plaintext* ke-i.

Ki = nilai desimal karakter kunci ke-i.

3 Metode

Data yang digunakan dalam penelitian ini adalah data sekunder, yakni berupa data pembelian. Dari sekian banyak data pembelian penulis mengambil sampel data pembelian berupa *Purchase Order*. Data yang diperoleh penulis diperoleh dari Divisi Keuangan PT Lamongan *Marine Industry* pada tanggal 29 Juni 2018 Adapun langkah-langkah dalam melakukan penelitian ini sebagai berikut:

1. Peneliti mengambil data di Divisi Keuangan PT Lamongan *Marine Industry.*
2. Menyajikan data dalam bentuk tabel.
3. Membuat *tabula recta* dan tabel subtitusi.
4. Menentukan kata kunci yang dipakai dalam proses enkripsi pada algoritma *Vigenere Cipher* dan menentukan nilai dua bilangan prima yang akan digunakan untuk proses penyandian algoritma *RSA.*
5. Menyandikan data yang didapat dengan menggunakan Algoritma *Vigenere Cipher* dan Algoritma *RSA* dengan bantuan *software* Matlab.
6. Menganalisis hasil output yang didapat dari proses Penyandian

4 Hasil dan Pembahasan

Hasil data pembelian yang disandikan dengan algoritma *Vigenere Cipher* dan algoritma *RSA* dengan menggunakan *software* Matlab dijelaskan pada tabel 1 dan tabel 2 berikut.

Tabel 1. Hasil Penyandian dengan Algoritma *Vigenere Cipher*

No	Nomor PO	*Supplier*	Proyek	Nama Barang	Jumlah Barang	*Term Payment*
1	b33FF EK4I4 SeXF	QhPZ4P aGR`Pf	bgR\4VhG RbV	• bcZGc[3SR]]g#^Ua^H c4_hWZ •]b]]Y/UORbSXU1`_Z #_c=351hhcH1U	• GC#S\ • AC#S\	F3KRfX

Tabel 2. Hasil Penyandian dengan Algoritma *RSA*

No	Nomor PO	*Supplier*	Proyek	Nama Barang	Jumlah Barang	*Term Payment*
1	X0:P681 8bMU5	BURIAN bAQAX	XYOFG UbANG	• Xp ioqPainyRamfjmPuyi h • Nno qjBqanjmQPGNOPY TPJA	• 3+BH • 7+BH	2Hami

Hasil analisis perbandingan dari algoritma *vigenere cipher* dan algoritma *RSA* dijelaskan pada tabel 3 berikut.

Tabel 3. Analisis Perbandingan Algoritma *Vigenere Cipher* dan Algoritma *RSA.*

No	Perbandingan	Algoritma *Vigenere Cipher*	Algoritma *RSA*
1	Pembentukan kunci	Dalam algoritma *Vigenere Cipher* cara pembentukan kunci yaitu dengan menentukan sendiri kunci yang akan digunakan. Kunci yang digunakan dalam algoritma *Vigenere Cipher* berupa teks. Kunci yang digunakan dalam menenkripsi atau mendekripsikan pesan menggunakan kunci yang sama.	Dalam algoritma *RSA* proses pembentukan kunci menggunakan operasi perhitungan. Bilangan yang digunakan dalam proses perhitungan yaitu bilangan prima. Dan hasil dari proses pembentukan kunci algoritma *RSA* berupa *public key* untuk menenkripsi pesan dan *private key* untuk mendekripsi pesan.
2	Proses enkripsi	Ada dua cara dalam proses penyandian algoritma *Vigenere Cipher*, yaitu: a) Jika dalam proses penyandian menggunakan *tabula recta*, maka dalam proses penyandian tidak ada operasi perhitungan. b) Jika dalam proses penyandian menggunakan tabel subtitusi maupun kode ASCII maka proses penyandian	Dalam proses penyandian algoritma *RSA* menggunakan tabel subtitusi maupun kode ASCII dengan rumus yang sudah ditentukan sebelumnya. Hasil enkripsi penyandian algoritma *RSA* bergantung pada besarnya nilai modulo pada kunci yang dipakai. Waktu yang dibutuhkan dalam proses dekripsi 0,007 detik.

		menggunakan rumus dan operasi perhitungan. Waktu yang dibutuhkan dalam proses enkripsi 0.002 detik	
2	Proses enkripsi	Ada dua cara dalam proses penyandian algoritma *Vigenere Cipher*, yaitu: a) Jika dalam proses penyandian menggunakan *tabula recta*, maka dalam proses penyandian tidak ada operasi perhitungan. b) Jika dalam proses penyandian menggunakan tabel subtitusi maupun kode ASCII maka proses penyandian menggunakan rumus dan operasi perhitungan. c) Waktu yang dibutuhkan dalam proses enkripsi 0.002 detik	Dalam proses penyandian algoritma *RSA* menggunakan tabel subtitusi maupun kode ASCII dengan rumus yang sudah ditentukan sebelumnya. Hasil enkripsi penyandian algoritma *RSA* bergantung pada besarnya nilai modulo pada kunci yang dipakai. Waktu yang dibutuhkan dalam proses dekripsi 0,007 detik.
3	Proses Dekripsi	Proses dekripsi dalam algoritma *Vigenere Cipher* menggunakan kode ASCII dan rumus yang telah ditentukan, namun masih menggunakan kunci yang sama dengan proses enkripsi. Waktu yang digunakan proses dekripsi sama dengan proses enkripsi yaitu 0,002 detik.	Proses dekripsi dalam algoritma *RSA* menggunakan kode ASCII dan rumus yang telah ditentukan, namun menggunakan kunci yang berbeda (*private key*). Waktu yang digunakan proses dekripsi sama dengan proses enkripsi yaitu 0,005 detik.
4	*ciphertext*	*Chipertext* yang dihasilkan dari proses enkripsi dari algoritma *Vigenere Cipher* lebih banyak menghasilkan *ciphertext* berupa tanda baca daripada huruf abjad.	Hasil enkripsi algoritma *RSA* berupa *ciphertext* diketahui tidak berbeda jauh dari karakter asli (*plaintext*), atau dapat dikatakan keluaran karakter pada cipherteks masih menghasilkan huruf abjad karena nilai modulo pada algoritma *RSA* mempengaruhi hasil keluaran karakter pada *ciphertext* Ada juga beberapa *ciphertext* yang sama dengan *plaintext*nya.

Selanjutnya dilakukan uji validasi yang bertujuan untuk mengetahui tingkat keamanan algoritma yang dipakai dalam penelitian ini. Berikut merupakan hasil perbandingan dua algoritma kriptografi yang telah di kriptanalis menggunakan dua metode untuk menguji keamanan algoritma yaitu metode *kraitchik* dan metode analisis frekuensi.

Input yang dibutuhkan dalam metode *kraitchik* untuk mengkriptanalis yaitu *public key*. Algoritma *Vigenere Cipher* merupakan algoritma kunci simetris, maka penggunaan metode *kraitchik* untuk mengkriptanalis algoritma kriptografi simetris tidak disarankan karena peretas dapat dengan mudah mengetahui *plaintext* yang dirahasiakan. Sedaangkan teknik pemecahan kunci dengan metode *kraitchik* berhasil diterapkan untuk mengkriptanalis kunci algoritma *RSA*. Waktu yang

dibutuhkan bergantung pada besarnya bilangan prima yang dipakai dalam pembuatan kunci.

Pada metode analisis frekuensi input yang dibutuhkan dalam mengkriptanalis yaitu *ciphertext* dan menggunakan alat bantu tabel frekuensi. Langkah-langkah kriptanalis dengan metode analisis frekuensi sebagai berikut:

1. Analisis frekuensi pada algoritma *Vigenere Cipher*
   a. Ambil *Ciphertext* = QhPZ4PaGR`Pf
   b. Hitung frekuensi kemunculan relatif huruf-huruf di dalam *ciphertext.*

Tabel 4. Perhitungan Frekuensi Kemunculan Huruf dalam *Ciphertext*

Karakter	Jumlah	Frekuensi Kemunculan
Q	1	8,33%
h	1	8,33%
P	3	25%
Z	1	8,33%
4	1	8,33%
a	1	8,33%
G	1	8,33%
R	1	8,33%
`	1	8,33%
f	1	8,33%
Jumlah	12	100%

Dari Tabel 4 dapat diketahui bahwa karakter P merupakan karakter yang sering muncul dalam *ciphertext*. Kemungkinan P merupakan pemetaan dari a, namun hasil pemetaan tersebut belum dapat dipastikan kebenarannya karena diperlukan *trial and error* dan pengetahuan tentang bahasa yang dipakai.

Iterasi 1

Q	**h**	**P**	**Z**	**4**	**P**	**a**	**G**	**R**	**`**	**P**	**f**
		a			a					a	

Karena karakter yang lain mempunyai frekuensi yang sama, maka pemetaan dilakukan dengan mencari karakter pada Tabel Frekuensi yang mempunyai nilai yang berdekatan satu sama lain. dengan memperhatikan nilai frekuensi dalam Tabel 4.

Iterasi 2

Q	**h**	**P**	**Z**	**4**	**P**	**a**	**G**	**R**	**`**	**P**	**f**
2	5	a	B	I	a	L	M	N	S	a	D

Langkah ini dilakukan sampai semua karakter yang mempunyai nilai frekuensi yang berdekatan telah diacak hingga membentuk sebuah kata atau kalimat.

Iterasi 15

Q	**h**	**P**	**Z**	**4**	**P**	**a**	**G**	**R**	**`**	**P**	**f**
B	U	M	I	e	a	N	D	a	L	a	S

Dari hasil iterasi karakter e dalam iterasi 15 kemungkinan merupakan spasi dan dapat disimpulkan bahwa *plaintext* yang dihasilkan yaitu BUMI ANDALAS.

2. Analisis frekuensi pada algoritma *RSA*
   a. Ambil *Ciphertext* = BURIANbAQAX
   b. Hitung frekuensi kemunculan relatif huruf-huruf di dalam ciphertext.

Tabel 5. Perhitungan Frekuensi Kemunculan Huruf dalam Ciphertext

Karakter	Jumlah	Frekuensi Kemunculan
B	1	9,09%
U	1	9,09%
R	1	9,09%
I	1	9,09%
A	3	27,27%
N	1	9,09%
b	1	9,09%
Q	1	9,09%
X	1	9,09%
Jumlah	11	100%

Dari Tabel 5 dapat diketahui bahwa karakter P merupakan karakter yang sering muncul dalam *ciphertext*. Kemungkinan A merupakan pemetaan dari a, namun hasil pemetaan tersebut belum dapat dipastikan kebenarannya karena diperlukan *trial and error* dan pengetahuan tentang bahasa yang dipakai.
Iterasi 1

B	**U**	**R**	**I**	**A**	**N**	**b**	**A**	**Q**	**A**	**X**
				a			a		a	

Karena karakter yang lain mempunyai frekuensi yang sama, maka pemetaan dilakukan dengan mencari karakter pada Tabel Frekuensi yang mempunyai nilai yang berdekatan satu sama lain. dengan memperhatikan nilai frekuensi dalam Tabel 5.
Iterasi 2

B	**U**	**R**	**I**	**A**	**N**	**b**	**A**	**Q**	**A**	**X**	**B**
"	-	.	3	a	8	D	a	E	a	G	P

Langkah ini dilakukan sampai semua karakter yang mempunyai nilai frekuensi yang berdekatan telah diacak hingga membentuk sebuah kata atau kalimat
Iterasi 34

B	**U**	**R**	**I**	**A**	**N**	**b**	**A**	**Q**	**A**	**X**	**B**
G	E	m	P	a	3	8	m	u	a	r	a

Dari hasil iterasi 34 dapat disimpulkan bahwa *plaintext* yang dihasilkan yaitu gempa38muara

5 Kesimpulan

Dari pembahasan diatas dapat disimpulkan bahwa dalam proses pembentukan kunci algoritma *RSA* lebih rumit jika dibandingkan dengan algoritma *Vigenere Cipher* karena algoritma *RSA* dalam pembentukan kunci

melalui operasi perhitungan, sedangkan untuk algoritma *Vigenere Cipher* pembentukan kuncinya tidak melalui proses perhitungan. Proses enkripsi dan dekripsi algoritma *Vigenere Cipher* menggunakan kunci sama, sedangkan algoritma *RSA* menggunakan kunci yang berbeda (*public key* dan *private key*). Dalam proses penyandian algoritma *Vigenere Cipher* dapat menggunakan dua cara, yaitu dengan rumus yang ditentukan dan dengan tabula recta. Rumus yang digunakan dalam algoritma *Vigenere Cipher* sangat sederhana dan perhitungannya tidak menggunakan nilai yang cukup besar seperti algoritma *RSA*. Waktu yang dibutuhkan algoritma *Vigenere Cipher* dalam proses enkripsi relatif lebih cepat dari algoritma *RSA*. Jumlah karakter *plaintext* yang akan dienkripsi juga mempengaruhi waktu yang dibutuhkan. Hasil yang didapat dari penyandian algoritma *Vigenere Cipher* lebih banyak menghasilkan *ciphertext* berupa tanda baca berbeda dengan algoritma *RSA* yang lebih banyak menghasilkan *ciphertext* berupa huruf abjad, karena bergantung pada besarnya nilai modulo pada kunci yang dipakai.

6 Daftar Pustaka

[1] J. Sasongko, "Pengamanan Data Informasi menggunakan Kriptografi Klasik," *Dinamik*, vol. 10, no. 3, 2005.

[2] A. Pudoli, A. Muchbarak, and S. H. Farham Harvianto, "Keamanan Data Pada File Excel Dengan Menggunakan Vigenere Cipher." Mei, 2014.

[3] S. A. Fauji, M. S. Pradana, and N. A. Azhari, "Penerapan Kode Huffman Pada Algoritma RSA (Rivest-Shamir-Adleman) Untuk Menyandikan Password Email," *Unisda J. Math. Comput. Sci.*, vol. 2, no. 1, pp. 41–49, 2016.

[4] D. N. Permata, L. Lambey, and S. Tangkuman, "Analisis Penerapan Sistem Informasi Akuntansi Pembelian Suku Cadang Pada Pt. Hasjrat Abadi Sudirman Manado," *Going Concern J. Ris. Akunt.*, vol. 12, no. 2, 2017.

[5] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, pp. 20–31, 2016.

[6] T. Cahyadi, "Implementasi steganografi LSB dengan enkripsi vigenere cipher pada citra JPEG," *Transient J. Ilm. Tek. Elektro*, vol. 1, no. 4, pp. 281–288, 2012.