Kriptografi dengan Mengkomposisikan Vigenere *Cipher* dan Algoritma *Knapsack* Merkle-Hellman

Raden Danika Rahma Aghniya, Rini Marwati, Husty Serviana Hussain
Departemen Pendidikan Matematika FPMIPA,
Universitas Pendidikan Indonesia
*surel: danikarahmaa@gmail.com

ABSTRAK. Teknologi informasi dari masa ke masa terus mengalami perkembangan. Namun dengan berkembangnya teknologi, informasi seringkali disadap atau diubah oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena itu diperlukan suatu seni atau ilmu untuk menjaga keamanan pesan yaitu Kriptografi. Masalah yang dikaji yaitu mengembangkan kriptografi Vigenere *cipher* dan Algoritma *Knapsack* Merkle-Hellman dengan cara mengkomposisikan dua algoritma kriptografi tersebut.–kunci Vigenere *Cipher* merupakan alfabet 26 karakter yang akan ditingkatkan menjadi 95 karakter sedangkan algoritma *Knapsack* Merkle-Hellman merupakan barisan *integer superincreasing* yang menyamarkan kunci rahasia menjadi kunci publik. Metode mengkomposisikan kedua algoritma ini yaitu pesan dienkripsi menggunakan Vigenere *cipher*, kemudian *ciphertext* dienkripsi menggunakan algoritma *Knapsack* Merkle-Hellman. Selanjutnya dibuat program aplikasi kriptografi yang bertujuan untuk memudahkan pengguna memakai algoritma komposisi ini.
Kata kunci: Vigenere *cipher*, *knapsack* Merkle-Hellman, enkripsi, dekripsi, komposisi, algoritma.

Cryptography by Composing Vigenere *Cipher* and Merkle-Hellman's *Knapsack* Algorithm

ABSTRACT. Information technology has been increased. However, with the development of technology, the information could be tapped or modified by someone who is not entitled to know the information. Therefore, it is important to have a knack or knowledge to keep the message safety, it is known as Cryptography. The problem in this study is to develop cryptographic Vigenere *Cipher* and Knapsack Merkle-Hellman algorithms, by composing both cryptographic algorithms. Vigenere *Cipher* key has 26 characters of alphabet which will be increased to 95 characters. On the other hand, Merkle-Hellman Knapsack has superincreasing integer series that can hide the secret key by change it to become public key. The methodology, these two algorithms wa composited. Firstly, the message was encrypted by the Vigenere *Cipher*. Then, the *cipher*text was encrypted by Knapsack Merkle-Hellman algorithm. Furthermore, cryptographic application program was made to facilitate users using the compositition algorithm.

Keywords: Vigenere *cipher, Knapsack* Merkle-Hellman, encryption, decryption, composition, algorithm.

1. PENDAHULUAN

Teknologi dan informasi dari masa ke masa terus mengalami perkembangan yang sangat berpengaruh pada hampir semua aspek kehidupan manusia, salah satunya dalam komunikasi. Berkomunikasi menjadi salah satu cara untuk memperoleh informasi. Salah satu cara berkomunikasi yaitu dengan mengirim pesan berupa tulisan. Namun dengan berkembangnya teknologi seringkali pesan disadap oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Salah satu cara agar pesan tidak dapat disadap oleh pihak lain maka diperlukannya suatu seni atau ilmu untuk menjaga keamanan pesan di mana hanya pengirim dan penerima pesan yang mengetahui isi pesan tersebut, ilmu ini dikenal dengan Kriptografi.

Dalam kriptografi terdapat tiga fungsi dasar, yaitu enkripsi, dekripsi dan kunci. Enkripsi yaitu mengubah pesan asli atau *plaintext* ke dalam bentuk pesan yang tidak dimengerti yaitu *ciphertext.* Dekripsi merupakan kebalikan dari enkripsi, yaitu mengembalikan *ciphertext* ke bentuk *plaintext.* Kunci yang dimaksud di sini adalah kunci yang dipakai untuk mengenkripsi dan mendekripsi. Kunci terbagi menjadi dua bagian, yaitu kunci rahasia (*private key*) dan kunci publik (*public key*).

Berdasarkan kuncinya, algoritma kriptografi dibagi menjadi Algoritma Simetri dan Algoritma Asimetri. Ariyus (2008) mendefinisikan bahwa algoritma simetri sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Akibatnya, pada algoritma simetri hanya memiliki satu kunci. Algoritma asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda Ariyus (2008). Pada algoritma asimetri terdapat dua kunci, yaitu kunci publik (*public key*) untuk enkripsi dan kunci rahasia (*private key*) untuk dekripsi.

Para peneliti sebelumnya, telah banyak mengembangkan cara untuk meningkatkan keamanan pesan rahasia. Firdaus (2017) mengembangkan kriptografi kunci simetri dengan menggunakan barisan Fibonacci untuk menghasilkan kunci *One Time Pad cipher*. Untuk mempersulit pemecahan, *One Time Pad cipher* dikomposisikan dengan *Affine cipher* yang merupakan dasar dari algoritma kriptografi klasik. Selanjutnya Bonita (2017) memodifikasi *Hill cipher* dengan menggunakan *Convert Between Base* dan *Linear Feedback Shift Register*.

Bentuk algoritma yang digunakan di penelitian ini adalah algoritma klasik, yaitu Vigenere *cipher* dan algoritma asimetri, yaitu algoritma *Knapsack* Merkle-

Hellman. Dalam memecahkan masalah keamanan kedua algoritma tersebut tidak lepas dari konsep-konsep matematika seperti aritmatika modulo, relatif prima dan balikan modulo. Kedua algoritma ini dinilai sudah tidak aman lagi karena pada abad ke-19 Vigenere *cipher* telah dipecahkan dengan menggunakan algoritma Kasiski, begitu juga dengan algoritma *Knapsack* Merkle-Hellman yang berhasil dipecahkan pada permulaan 1980. Untuk itu penulis akan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman agar proses enkripsi dan dekripsi lebih sulit dipecahkan. Kemudian hasil komposisi kedua algoritma tersebut dibuat program aplikasi komputer.

2. VIGENERE *CIPHER*

Vigenere *cipher* merupakan salah satu kriptografi algoritma klasik dengan teknik subtitusi. Vigenere *cipher* dipublikasikan oleh diplomat Perancis, Blaise de Vigenere pada abad ke 16, tahun 1586 (Ariyus, 2008). Arjana, Rahayu, Yakub dan Hariyanto (2012) mendefinisikan bahwa "Vigenere *cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci".

Rumus dari enkripsi dan dekripsi Vigenere *cipher* adalah sebagai berikut:

Enkripsi: $C_i = (P_i + K_i)\ mod\ 26$ (2.1)

Dekripsi: $P_i = (C_i - K_i)\ mod\ 26$, untuk $C_i \geq K_i$ (2.2)

$P_i = (C_i + 26 - K_i)\ mod\ 26$, untuk $C_i \leq K_i$ (2.3)

dengan

C_i = *Ciphertext*

P_i= *Plaintext*

K_i = Kunci

Dalam melakukan enkripsi dan dekripsi Vigenere *cipher* menggunakan Tabel 2.1:

Tabel 2.1 Vigenere *Cipher*

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

3. ALGORITMA *KNAPSACK* MERKLE-HELLMAN

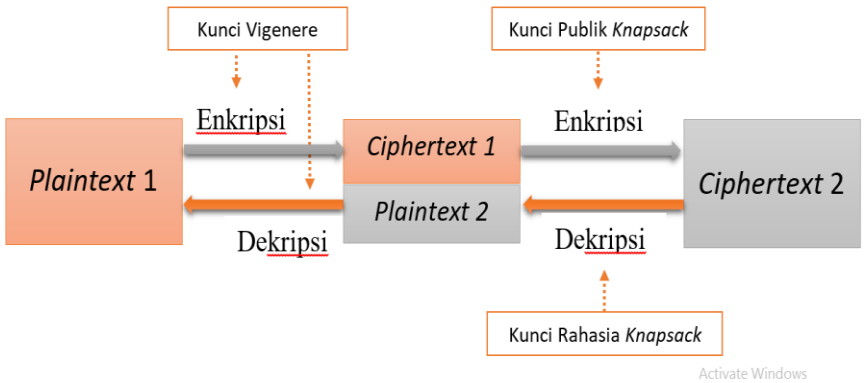
Ariyus (2008) mengatakan algoritma *Knapsack* Merkle-Hellman dapat dituliskan sebagai berikut:

Jika diberikan $s = (s_i, \ldots, s_n)$ barisan *integer* yang *superincreasing*, misalnya bilangan prima $P > \sum_{i=1}^{n} s_i$ dan $1 \leq a \leq p-1$, untuk $1 \leq i \leq n$ didefinisikan $t_i = a.s_i \bmod P$, dan dinyatakan $t = (t_1, \ldots, t_n)$. Misalkan $= \{0,1\}^n$, $C = \{0, \ldots, n(p-1)\}$, dan misalkan kunci $K = \{(s, P, a, t)\}$. Kunci publiknya adalah t dan kunci rahasianya adalah s, a dan P. Untuk $K = \{s, P, a, t\}$ didefinisikan $e_k = (x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i t_i$. Untuk $0 \leq y \leq n(p-1)$, didefinisikan $z = a^{-1} y \bmod P$ dan diperoleh $d_k = (x_1, \ldots, x_n)$.

4. KOMPOSISI VIGENERE *CIPHER* DAN ALGORITMA *KNAPSACK* MERKLE-HELLMAN

Pengembangan dari kriptografi Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman yaitu dengan mengomposisikan kedua algoritma tersebut. Karena Vigenere *cipher* merupakan kriptografi simetri, maka kunci yang digunakan hanya satu untuk proses enkripsi dan dekripsi, yaitu kunci Vigenere. Sedangkan, algoritma *Knapsack* Merkle-Hellman merupakan kriptografi asimetri, sehingga proses enkripsi dan dekripsi menggunakan kunci yang berbeda, yaitu kunci publik *knapsack* untuk proses enkripsi dan kunci rahasia *knapsack* untuk proses dekripsi. Skema kriptografi dengan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman digambarkan dalam Gambar 4.1.

Gambar 4.1 Skema Proses Enkripsi dan Dekripsi Kriptografi dengan



Mengkomposisikan Vigenere *Cipher* dan Algoritma *Knapsack* Merkle-Hellman

Langkah-langkah enkripsi dan dekripsi kriptografi dengan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle Hellman dijelaskan sebagai berikut:

4.1 PROSES ENKRIPSI

Proses enkripsi kriptografi dengan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman menggunakan dua kunci, yaitu kunci Vigenere dan kunci publik *knapsack*, di mana kunci publik *knapsack* dibangkitkan oleh kunci rahasia *knapsack.* Proses pembangkitan kunci publik *knapsack* yaitu sebagai berikut:

a. Diketahui barisan *superincreasing* $s = (s_i, \ldots, s_n)$.
b. Diketahui bilangan prima $P > \sum_{i=1}^{n} s_i$.
   Diketahui bilangan bulat a, di mana $1 \leq a \leq P-1$.
c. Untuk memperoleh kunci publik *knapsack* t digunakan persamaan:

$$t_j = a \cdot s_j \; mod \; P \tag{4.1}$$

Proses enkripsi kriptografi dengan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman dapat dilakukan setelah memperoleh kunci publik *knapsack.* Penyelesaiannya adalah sebagai berikut:

a. Diketahui *plaintext* L, kunci Vigenere K dan kunci publik *knapsack* t.
b. Konversi L dan K ke dalam kode ASCII, dengan mengurangi setiap elemen di L dan K dengan 32.
c. Enkripsi *plaintext* L dengan kunci K, jika $K < L$ maka bangkitkan kunci K dengan melakukan pengulangan sehingga banyak elemen di K sama dengan banyak elemen di L. Rumusnya adalah sebagai berikut:

$$C_i = (L_i + K_i) \; mod \; 95 \tag{4.2}$$

   maka akan diperoleh *ciphertext* C.
d. C akan menjadi *plaintext* untuk proses enkripsi menggunakan algoritma *Knapsack* Merkle-Hellman.
e. Konversi C menjadi bilangan biner berdasarkan kode ASCII, disini yang digunakan adalah tabel ASCII 8 bit.
f. Misalkan x adalah elemen-elemen C_i yang sudah dikonversi ke bilangan biner, dan diketahui t adalah kunci publik *knapsack*. Langkah selanjutnya yaitu mendapatkan Y, dengan rumus sebagai berikut:

$$Y_i = \sum_{j=1}^{n} x_j \cdot t_j \tag{4.3}$$

   sehingga diperoleh $Y = (Y_1, Y_2, \ldots, Y_n)$.
g. Y merupakan *ciphertext* yang akan dikirim.

4.2 PROSES DEKRIPSI

Proses dekripsi kriptografi dengan mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman menggunakan kunci Vigenere dan kunci rahasia *knapsack*. Penyelesaiannya adalah sebagai berikut:

a. Diketahui Y merupakan *ciphertext* yang akan didekripsi dengan kunci rahasianya adalah S, P, a dan kunci Vigenerenya adalah K.
b. Cari nilai invers a atau a^{-1} dari $a \ mod \ P$.
c. Hitung z dengan rumus berikut:

$$z = (a^{-1} \cdot Y) \ mod \ P \tag{4.4}$$

d. Konversi bilangan z kedalam bilangan biner dengan menggunakan algoritma *superincreasing knapsack*.
e. Konversi dari bilangan biner ke karakter C berdasarkan kode ASCII.
f. Konversi karakter C dan kunci Vigenere K menjadi desimal berdasarkan kode ASCII. Kemudian kurangi setiap elemen di C dan K dengan 32.
g. Selanjutnya menghitung L, jika $K < C$ maka bangkitkan kunci K dengan melakukan pengulangan sehingga banyak elemen di K sama dengan banyak elemen di L. Rumusnya sebagai berikut:

$$L_i = (C_i - K_i) \ mod \ 95, \text{ untuk } C_i \geq K_i \tag{4.5}$$

$$L_i = (C_i + 95 - K_i) \ mod \ 95, \text{ untuk } C_i < K_i \tag{4.6}$$

h. Ubah L ke dalam karakter berdasarkan kode ASCII, L merupakan *plaintext* atau pesan asli.

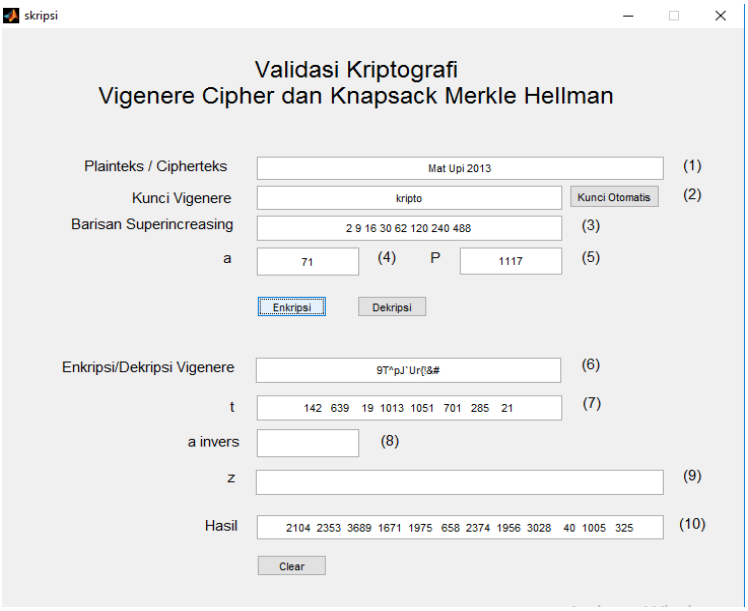
4.3 PENERAPAN

Diberikan *plaintext* $L = Mat\ Upi\ 2013$ dengan kunci-kunci yang diberikan Kunci Vigenere $K = kripto$, Barisan *superincreasing* $s = (2, 9, 16, 30, 62, 120, 240, 488)$, Bilangan bulat $a = 71$ dan bilangan prima $P = 1117$. Sebelum melakukan enkripsi yang harus dilakukan adalah membangkitkan kunci publik *knapsack* t. Berikut adalah proses pembangkitan kunci publik *knapsack* t dengan menggunakan kunci rahasia S, P dan a. Berdasarkan persamaan (4.1) maka diperoleh $t = (142, 639, 19, 1013, 1051, 701, 285, 21)$. Proses enkripsi diilustrasikan pada Tabel 4.1. Berdasarkan Tabel 4.1, *ciphertext* yang diperoleh adalah
(2104 2353 3689 1671 1975 658 2374 1956 3028 40 1005 325).

Tabel 4.1 Tabel Enkripsi *Plaintext*

Plaintext	*M*	*a*	*t*		*U*	*p*	*i*		2	0	1	3
Kunci *Vigenere*	K	R	i	p	T	o	k	r	i	p	t	o
Kunci Publik	142	639	19	1013	1051	701	285	21				
Enkripsi *Vigenere*	9	*T*	^	*p*	*J*	'	*U*	*r*	{	!	&	#
Ciphertext	2104	2353	3689	1671	1975	658	2374	1956	3028	40	1005	325

Gambar 4.2 menampilkan program aplikasi kriptografi untuk proses enkripsi yang telah dikontruksi menggunakan bahasa pemograman MATLAB. Sebelum melakukan enkripsi yang harus dilakukan adalah membangkitkan kunci public *knapsack t.*



Gambar 4.2 Tampilan Program Aplikasi Proses Enkripsi

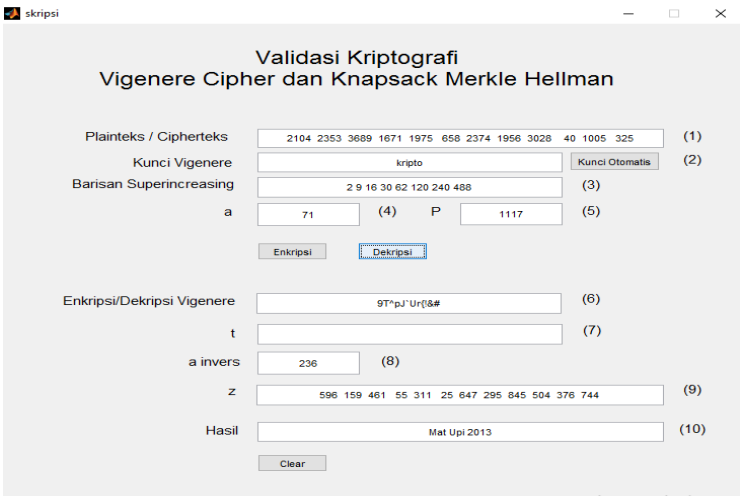
Kemudian *ciphertext* yang telah dikirim didekripsi oleh penerima pesan dengan menggunakan kunci vigenere dan kunci rahasia barisan *superincreasing s*,

bilangan bulat a dan bilangan prima P. Tabel 4.2 memperlihatkan proses dekripsi *ciphertext.* Berdasarkan Tabel 4.2 diperoleh *plaintext* yang dikirim adalah $Mat\ Upi$ 2013.

Tabel 4.2 Tabel Dekripsi *Ciphertext*

Ciphertext	2104	2353	3689	1671	1975	658	2374	1956	3028	40	1005	325
Kunci Vigenere	k	R	i	p	t	O	K	R	i	p	t	o
Barisan *s*	2 9 16 30 62 120 240 488											
a invers	71											
P	1117											
dekripsi *Vigenere*	9	*T*	^	*p*	*J*	'	*U*	*r*	{	!	&	#
Plaintext	*M*	*a*	*t*		*U*	*p*	*i*		2	0	1	3

Gambar 4.3 menampilkan program aplikasi kriptografi untuk proses dekripsi yang telah dikontruksi menggunakan bahasa pemograman MATLAB. Alurnya adalah input chipertext beserta kunci Vigenere K dan kunci rahasia *knapsack* yang terdiri dari barisan super increasing.



Gambar 4.3 Tampilan Program Aplikasi Proses Dekripsi

5. KESIMPULAN

Berdasarkan latar belakang dan isi yang telah diuraikan, maka dapat disimpulkan sebagai berikut:

a. Pengembangan kriptografi dari Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman, yaitu dengan mengkomposisikan kedua algoritma tersebut. Proses enkripsi yaitu *plaintext* dienkripsi menggunakan kunci Vigenere, kemudian dienkripsi kembali menggunakan kunci publik *knapsack* yang dibangkitkan oleh kunci rahasia *knapsack.* Sedangkan, proses dekripsi yaitu *ciphertext* didekripsi menggunakan kunci rahasia *knapsack*, kemudian didekripsi kembali menggunakan kunci Vigenere.

b. Pembuatan program aplikasi kriptografi dibuat dengan menggunakan bahasa pemograman Matlab R2013a dengan memanfaatkan *Graphic User Interface* atau GUI. Kemudian pengujian program aplikasi dilakukan dengan membandingkan hasil yang diperoleh secara manual dan hasil yang diperoleh dari program aplikasi. Hasil yang diperoleh secara manual dan hasil yang diperoleh dari program aplikasi keduanya sama, maka program aplikasi yang dirancang telah sesuai dengan yang diinginkan.

DAFTAR PUSTAKA

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi.* Yogyakarta: Andi

Arjana, P. H., Rahayu, T. P., Yakub, & Hariyanto. (2012*). Implementasi Enkripsi Data dengan Algoritma Vigenere Cipher.* Yogyakarta: Seminar Nasional Teknologi dan Komunikasi 2012.

Bonita, S. T. (2017). *Pembangkit Kunci Linear Feedback Shift Register pada Algoritma Hill Cipher yang Dimodifikasi Menggunakan Convert Between Base.* (Skripsi). Universitas Pendidikan Indonesia, Bandung

Firdaus, I. L. (2017). *Aplikasi Kriptografi Komposisi One Time Pad Cipher dan Affine Cipher.* (Skripsi). Universitas Pendidikan Indonesia, Bandung