WORK PAPER

Kriptanalisis Vigenere Bahasa Indonesia

Sutanto[(1)], Wan Khudri[(2)]
Lab. Cyber Math
Universitas Sebelas Maret Solo

Email : sutanto@uns.ac.id, chudry81@yahoo.com

Abstrak

Ada 2 hal yang dihasilkan dalam kriptanalisis Vigenere dengan plain teksnya berbahasa Indonesia : (1) Menguji kebenaran Tabel Probabilitas dan Indeks Coincidence munculnya huruf pada tulisan yang menggunakan bahasa Indonesia (2) Proses kriptanalis sendiri yang menggunakan teori probabilitas dalam proses penguraian chiper tkesnya.

Kata Kunci : Vigenere, Indeks Coincidence

A. Pendahuluan

Kriptanalisis Vigenere yang akan dijelaskan menggunakan konsep *Index Coincidence* (I_c) untuk menentukan kata kuncinya. Konsep ini didefinisikan oleh Wolfe Friedman pada tahun 1920. Untuk nilai *Index coincidence* Bahasa Indonesia mengacu pada penelitian (skripsi) Anita D.R. [ref.....] yaitu

Nilai I_c Bahasa Indonesia = 0.0786

Untuk melakukan kriptanalisis Vigenere Bahasa Indonesia ini, diasumsikan bahwa telah diketahui panjang kuncinya m dan teks sandinya C_i.

Langkah pertama, huruf-huruf dalam teks sandi dikelompokkan menjadi m kolom dan dicari nilai I_c masing-masing kolom. Panjang kunci m dapat ditentukan jika I_c tiap kolom mendekati I_c bahasa Indonesia.

Langkah kedua, menghitung nilai *Index coincidence* bersama (*MIc*) dengan *relative shift* sebanyak kombinasi $\binom{m}{2}$ dan dipilih MI_c yang mendekati I_c bahasa Indonesia.

Langkah ketiga, dari hasil Langkah kedua dibentuk persamaan linier dan diselesaikan dengan eliminasi Gauss Jordan untuk menentukan 26 kemungkinan kata kuncinya.

Langkah keempat, berdasarkan hasil 26 kata kunci yang diperoleh dari Langkah ketiga, dilakukan proses penguraian Vigenere menggunakan salah satu kata kunci yang sesuai sehingga diperoleh hasil teks asli yang dapat dibaca dalam bahasa Indonesia.

B. Studi Kasus Kriptanalisis Vigenere:

Teks sandi :

PUTHGAWCKDMAOUHVUTXGAWUPHFAMURDHYDHGGCTDEUWCOOYH
VYTLUPVCSZUKDLEQUDLUNJAASNEUFAOOSXFIWONWOKGCPHFAMUR
LJAGUHDFKDFAXXIWYRDJKDHDDFAPUPOCKDMINYHLXUSUNDEAQM
AQAAWGEQSEQUNJEAQXAQMEPUKLHMXXAKONWOKGCPDBAPC

Proses Langkah Pertama:

Huruf-huruf dalam teks sandi dikelompokkan menjadi *m* kolom dan dicari nilai I_c masing-masing kolom. Nilai I_c untuk *m* panjang kata kunci dapat di lihat di Tabel 2.3.

Tabel 2.3. Nilai I_c tiap kolom

Panjang Kunci (*m*)	**I_c (*x*)**			
	Kolom 1	**Kolom 2**	**Kolom 3**	**...**
2	0.04188	0.05069		
3	0.08173	0.09423	0.10665	
...	...	...	...	...

Berdasarkan tabel 2.3, nilai I_c (*x*) yang mendekati I_c bahasa indonesia = 0.0786 adalah *m* = 3. Sehingga diperoleh bahwa panjang kata kuncinya adalah *m* = 3.

Proses Langkah Kedua:

Menghitung MI_c (y_i , y_j^g) dengan $1 \leq i < j \leq m$, dan $0 \leq g \leq 25$. Sehingga diperoleh hasil MI_c seperti dalam Tabel 2.4.

Tabel 2.4. Nilai MI_c (y_i , y_j^g)

i	**j**	**Nilai MI_c (y_i , y_j^g)**				
1	2	0.02249	0.05254	0.05799	0.03290	0.02864
		0.03598	0.03124	0.02438	0.02698	**0.09088**
		0.03195	0.03337	0.03479	0.03432	0.03077
		0.04095	0.03408	0.05681	0.04166	0.02533
		0.04521	0.03408	0.04615	0.02769	0.04734
		0.03148				
1	3	0.02091	0.03029	0.02596	**0.08918**	0.02764
		0.02885	0.04447	0.03774	0.03077	0.03630
		0.03496	0.04279	0.04784	0.02500	0.04856
		0.03918	0.05673	0.01899	0.03414	0.04495
		0.02091	0.03293	0.07212	0.04279	0.01995
		0.04615				
2	3	0.02837	0.03966	0.05817	0.02356	0.03558
		0.06082	0.02909	0.04760	0.02332	0.02764
		0.0478	0.02813	0.03966	0.04904	0.04784
		0.02212	0.04567	0.02428	0.04087	0.01851
		0.09519	0.03293	0.02260	0.04327	0.03990
		0.02837				

Berdasarkan Tabel 2.4, dipilih nilai MI_c yang mendekati I_c bahasa Indonesia = 0.0786, sehingga diperoleh 3 *relative shift* yang dapat dibentuk sistem persamaan linier seperti berikut:

$$\left.\begin{aligned} k_1 - k_2 &= 9 \\ k_1 - k_3 &= 3 \\ k_2 - k_3 &= 20 \end{aligned}\right\} \bmod 26$$

Proses Langkah Ketiga:

Berdasarkan Langkah kedua dihasilkan persamaan linier

$$\left.\begin{aligned} k_1 - k_2 &= 9 \\ k_1 - k_3 &= 3 \\ k_2 - k_3 &= 20 \end{aligned}\right\} \bmod 26$$

Dari persamaan linier tersebut dibuat matriks perluasan dengan variabel k_1, k_2, dan k_3 sehingga diperoleh persamaan matriks sebagai berikut:

$$\begin{bmatrix} 1 & -1 & 0 & 9 \\ 1 & 0 & -1 & 3 \\ 0 & 1 & -1 & 20 \end{bmatrix} \bmod 26$$

Selanjutnya menyelesaikan persamaan matriks tersebut dengan Eliminasi Gauss Jordan.

Eliminasi 1: Mengeliminasi k_1 dengan 2 persamaan terakhir, sehingga diperoleh matriks

$$\begin{bmatrix} 1 & -1 & 0 & 9 \\ 0 & 1 & -1 & -6 \\ 0 & 1 & -1 & 20 \end{bmatrix} \bmod 26$$

Eliminasi 1: Persamaan ketiga dikurangi persamaan kedua, sehingga matriksnya menjadi

$$\begin{bmatrix} 1 & -1 & 0 & 9 \\ 0 & 1 & -1 & -6 \\ 0 & 0 & 0 & 26 \end{bmatrix} \bmod 26$$

Sehingga diperoleh persamaan setelah eliminasi, yaitu

$$\left.\begin{aligned} k_1 - k_2 &= 9 \\ k_2 - k_3 &= -6 \end{aligned}\right\} \bmod 26 \;=\; \left.\begin{aligned} k_1 &= k_2 + 9 \\ k_3 &= k_2 + 6 \end{aligned}\right\} \bmod 26$$

Berdasarkan hasil akhir persamaan tersebut, dapat ditentukan 26 kemungkinan kata kunci.

Misalkan $k_2 = h$, untuk $0 \le h \le 25$, maka kemungkinan kata kunci dapat dihitung sebagai $K_h = (h+9, h, h+6) = (k_1, k_2, k_3)$ dan hasilnya dikorespondensikan menjadi huruf-huruf *alphabet*.

Kemungkinan kata kunci ke-1 ($h = 0$) :

K_1 = (0+9,0,0+6)=(9,0,6) = (J,A,G)
Kemungkinan kata kunci ke-2 (h = 1) :
K_1 = (1+9,1,1+6)=(10,1,7) = (K,B,H)
Kemungkinan kata kunci ke-2 (h = 2) :
K_2 = (2+9,2,2+6)=(11,2,8) = (L,C,I)
dan seterusnya sampai h = 25.

Secara lengkap 26 kemungkinan kata kunci nya adalah
JAG, KBH, LCI, MDJ, NEK, OFL, PGM, QHN, RIO, SJP, TKQ, ULR, VMS, WNT, XOU, YPV, ZQW, ARX, BSY, CTZ, **DUA**, EVB, FWC, GXD, HYE, IZF

Proses Langkah Keempat:
Berdasarkan hasil 26 kata kunci yang diperoleh dari Langkah ketiga, dilakukan proses penguraian Vigenere menggunakan salah satu kata kunci yang sesuai sehingga diperoleh hasil teks asli yang dapat dibaca dalam bahasa Indonesia.
Untuk kasus ini kata kuncinya adalah **DUA**.

Sehingga proses penguraian teks sandinya sama seperti terlihat dalam Tabel 2.2. dan diperoleh hasil akhirnya (teks asli) sebagai berikut:

MATEMATIKASALAHSATUMATAPELAJARANYANGDITAKUTIOLEHSETI
APSISWAKARENADIANGGAPTERLALUSULITUNTUKDIPELAJARIPADAHA
LKALAUDITERAPKANDALAMAPLIKASIKEHIDUPANAKANSANGATMENY
ENANGKANDANSEMAKINMUDAHUNTUKDIPAHAMI