Penerapan Teknik Exhaustive Attack Pada Proses Kritanalisis Vigenere Ciphertext Menggunakan Bantuan Kamus Bahasa Indonesia

Ari Eko Wardoyo1. Agung Nilogiri2
Dosen Fakultas Teknik, UNMUH Jember
Jl. Karimata 49 Jember - 68121
Email: 1arieeko3 l 9@gmail.com, 2agung.nilogiri@gmail.com

ABSTRAK

Hal yang paling sering terjadi pada proses kriptanalisis adalah para kritanalis hanya memiliki informasi berupa beberapa ciphertext dari pesan yang dienkripsi dengan menggunakan algoritma yang sama, sehingga ciphertext only-attack merupakan jenis serangan yang paling umum dan paling sulit dilakukan berdasarkan informasi yang diketahui oleh para kritanalis. Salah satu teknik yang banyak dipakai untuk menentukan cipher key adalah exhaustive attack atau bruteforce attack. Kelemahan teknik ini adalah lamanya waktu pencarian karena menggunakan semua kemungkinan karakter yang ada. Salah satu pendekatan yang mungkin dilakukan adalah dengan menambahkan kamus bahasa sebagai sumber referensi. Makalah ini membahas penerapan teknik exhaustive attack pada proses dekripsi Vigenere Ciphertext menggunakan bantuan kamus bahasa Indonesia dengan harapan dapat meningkatkan efektifitas waktu yang digunakan pada proses kritanalisis dibanding dengan teknik exhaustive attack konvensional.

***Kata kunci** : ciphertext, cipher key, exhaustive attack, brute force attack, Vigenere Ciphertext, kamus bahasa Indonesia*

1. Pendahuluan

Proses komunikasi menggunakan teknik kriptografi melibatkan dua subyek pelaku yaitu pengirim dan penerima pesan. Obyeknya adalah pesan yang disampaikan yaitu pesan asli (*plaintext*) dan pesan tersandi (*ciphertext*). Untuk menghasilkan pesan tersandi dari pesan asli dibutuhkan karakter kunci (*cipher key*) Dengan demikian terdapat dua buah proses yang berlaku didalamnya yaitu:

Proses Enkripsi : proses perubahan dari *plaintext* ke *ciphertext*.

Proses Deskripsi : proses perubahan *ciphertext* ke teks semula (*plaintext*).

Salah satu metode implementasi dalam kriptografi adalah menggunakan *vigenere cipher*. Metode ini termasuk dalam kategori kriptografi klasik karena operasinya masih melibatkan karakter.

Pada metode *vigenere cipher*, untuk melakukan proses enkripsi membutuhkan bantuan bujur sangkar *vigenere* yang terdiri dari 26 huruf *cipher* Caesar [ChC06]. Pada bujur sangkar tersebut dihasilkan huruf *ciphertext* yang merupakan perpaduan dari huruf *plainteks* yang berada pada baris paling atas dengan huruf *cipher key* di kolom paling kiri.

Penggunaan bujur sangkar vigenere untuk memperoleh *ciphertext* dengan menggunakan *cipherkey* yang ditentukan memiliki aturan jika panjang karakter kunci lebih pendek dari panjang *plaintext*, maka kunci diulang penggunaannya secara periodik.

Proses enkripsi sebuah *plaintext* menjadi *chipertext* dengan menggunakan *chiperkey* “KUNCI” dapat dituliskan sebagai berikut :

Plaittext : PESAN
Chiperkey : KUNC!
Ciphertext : ZYFCV

Dapat dilihat bahwa *ciphertext* yang dihasilkan merupakan pergeseran huruf *plaintext* sejauh *cipherkey*.

Perkembangan kriptografi diiringi dengan perkembangan suatu komunitas yang bertujuan untuk melakukan suatu usaha dalam memecahkan *ciphertex* hasil proses enkripsi. Hal utama yang dilakukan dalam proses ini adalah berusaha memecahkan *cipherkey* yang dipakai selama proses enkripsi suatu *plaintext*. Selanjutnya apabila *cipherkey* sudah diperoleh maka *ciphertext*-nya dapat dikembalikan dalam bentuk *plaintext*-nya. [JTH08]

Brute force attack atau *exhaustive attack* adalah salah satu teknik yang dapat digunakan untuk pencarian *cipherkey*

Permasalahan yang terjadi jika menggunakan pendekatan ini adalah lamanya proses pencarian yang terjadi karena akan dilakukan pengecekan terhadap semua kemungkinan karakter yang muncul. Salah satu solusinya adalah teknik *exhaustive attack* menggunakan bantuan kamus (*dictionary attack*) yang dalam hal ini adalah kamus bahasa Indonesia. Selama pencarian *cipherkey* digunakan kamus sebagai sumber referensi dengan demikian tidak semua kombinasi karakter yang dicoba.

Untuk itulah pada makalah ini akan dibahas penggunaan kamus bahasa Indonesia sebagai salah satu strategi dalam membantu proses kriptanalisis dengan harapan dapat mempercepat proses pendeskripsian.

2. Permasalahan dan batasannya

Bahasa yang digunakan pada *plaintext* memegang peranan yang sangat signifikan pada proses deskripsi yang terjadi. Untuk membatasi permasalahan yang ada, maka dilakukan pemodelan secara umum dan khusus.

Batasan pemodelan seperti yang dimaksud di atas asalah sebagai berikut :

- Bahasa yang digunakan *plaintext* maupun *cipherkey* adalah bahasa Indonesia.
- Selain huruf, *Plaintext* dan *cipherkey* boleh mengandung unsur angka, tanda baca, operator, dan spasi.

Dengan batasan pemodelan di atas, maka dapat dicontohkan suatu model masalah jelaskan sebagai berikut :

Plaintext:
TEKNIKEXHAUSTIVEVIGENERECIPHER
MEMANFAATKAN KAMUS

Cipherkey:
KAMUS

Dari *plaintext* (cetak miring) dan *cipherkey* di atas dengan menggunakan *vigenere cipher* dihasilkan proses sebagai berikut : *ciphertext* (cetak tebal)

TEKNIKEXHAUST/VEVIGENERECIPHER
MEMANFAATKANKAMUS

KAMUSKAMUSKAMUSKAMUSKAMUSK
AMUS KAMUSKAMUSKAMUSKA

DEWHAUEJBSESFCNOVUAWXEDYUSP
TYJ WEYUFPAMNCKN WUEES

Pada *software* yang dibuat disertakan kamus bahasa Indonesia dengan kosakatanya dapat ditambahkan sendiri sehingga dapat digunakan sebagai bahan referensi selama proses kriptanalisis dengan algoritma *exhaustive attack* berlangsung.

Dari paparan di atas tadi permasalahan yang harus diselesaikan pertama kali adalah pencarian *cipherkey* dari *ciphertext* yang diberikan dan dilanjutkan dengan pencocokan *plaintext* dengan menggunakan; kamus bahasa Indonesia.

3. Metodc Pemccahan Masalah

Adapun metode pemecahan masalah im antara lain :

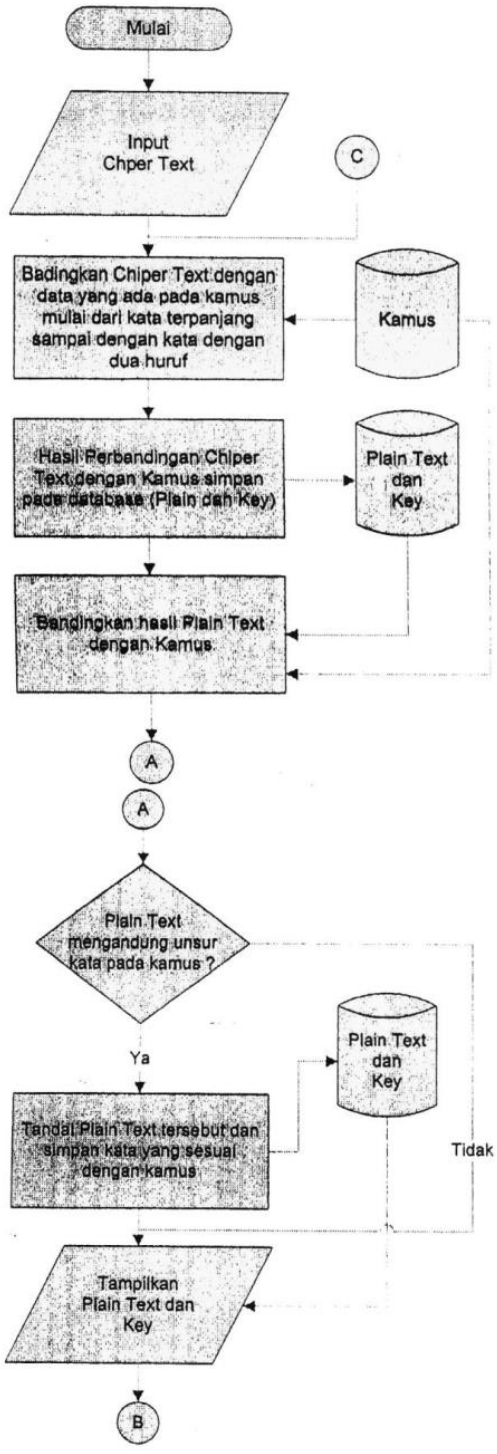
1. Pemecahan masalah.
Pemecahan masalah dinyatakan sebagai vektor dari *n-tuple*:
Y = $(y_1, y_2,...y_n)$, y_1, himpunan berhingga S,.
Misal: $S_1 = \{0,1\}$.
$y_1 = 0$ atau 1
diterjemahkan y_1 = benar atau salah.

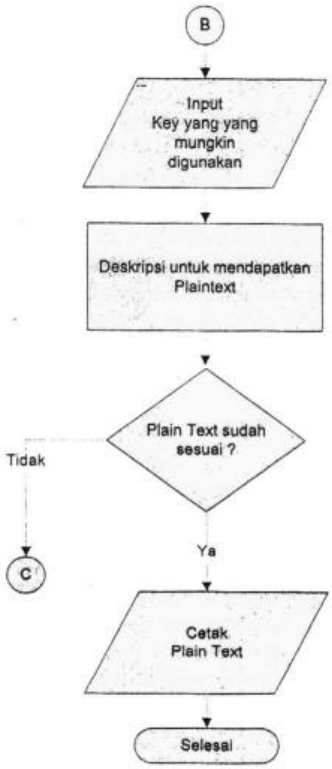
2. Pembangkit nilai vektor pemecahan masalah
Dinyatakan sebagai *Generate*(k) yaitu membangkitkan nilai untuk komponen vekror pemecah masalah.

3. Pembatas

Menentukan apakah pembangkit nilai vektor: mengarah ke pemecahan masalah. Jika ya. maka pembangkitan nilai dilanjutkan, tetapi jika tidak nilai vektor pemecah masalah yang dibangkitkan tidak digunakan lagi dalam pencarian solusi

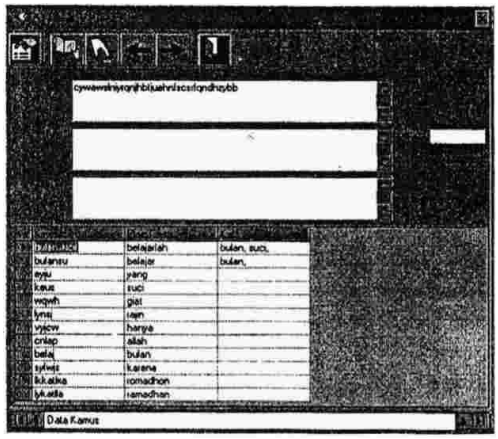
4. Algoritma Exhaustive yang digunakan



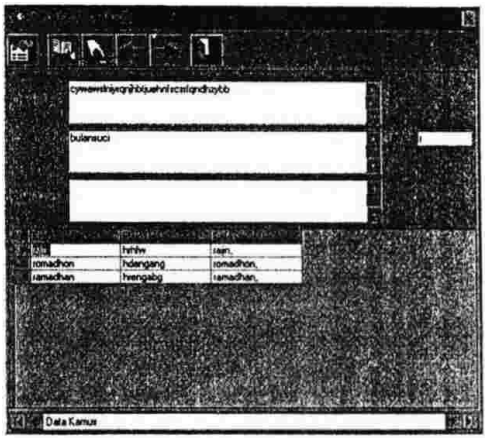


Gambar 1. Flowchart *Exhaustive attack* menggunakan kamus bahasa Indonesia

5. Penerapan *Exhaustive Attacking* Berbantuan Kamus



Gambar 2. Pencarian Key awal



Garnbar 3. Pencarian Key berikutnya berdasar kamus dengan huruf awal sesuai huruf atau kata pada temp.

Gambar 4. setelah *key* ditemukan maka *plaintext* akan ditemukan

Dengan . hasil yang telah dikemukakan sebelumnya, kita dapat menentukan elemen persoalan yang bersesuaian dengan metode pemecahan, yaitu :

l .Pemecahan masalah.

Solusi dari permasalahan ini adalah suatu vektor dengan n-tuple :

$X = (y_1, y_2,...y_n)$, dimana

y_i, himpunan berhingga S_i

S_i adalah himpunan huruf, angka, tanda baca, operator, dan spasi.

Kombinasi elemen-elemen Y secara berurutan membentuk kata yang ada ataupun bersesuaian dengan referensi kamus.

Sesuai dengan model masalah maka solusi yang diharapkan.

2. Pembangkit nilai vektor pemecahan masalah

Dinyatakan sebagai *Generate*(k) yaitu membangkitkan nilai untuk komponen vektor pemecah masalah, Pembangkit didasarkan pada referensi kamus yang ada.

3. Pembatas

Menentukan apakah pembangkit nilai vektor mengarah ke pemecahan masalah. Jika ya, maka pembangkitan nilai dilanjutkan, tetapi jika tidak, nilai vektor pemecah masalah yang dibangkitkan tidak digunakan lagi dalam pencarian solusi. Yang dimaksud dengan solusi adalah *plainteks* yang dihasilkan sesuai sebagian atau keseluruhan dengan kata yang terdapat dalam referensi kamus.

6. Keslmpulan dan Saran

- Penerapan teknik *exhaustive attack* pada proses kriptanalis *vigenere ciphertext* menggunakan bantuan kamus bahasa Indonesia memberikan hasil deskripsi *ciphertext* lebih cepat daripada penggunaan *exhaustive attack* konvensional. Semakin banyak kosa kata kamus yang digunakan, waktu yang dibutuhkan untuk mcndeskripsi *vigenere ciphertext* semakin lama, namun akan mempermudah penemuan *cipherkey* dan *plaintext*-nya.
- Proses pendeskripsiannya tidak dibatasi oleh spasi sehingga tidak memerlukan pola perulangan pada *ciphertext*-nya.
- Metode ini berhasil mendeskripsi *vigenere ciphertext* dimana *cipherkey* dan *plaintext* nya mengandung huruf, angka, spasi, operator, dan tanda baca.

Algoritma *Exhaustive Attack* (*brute force*) menggunakan bantuan kamus bahasa Indonesia ini dapat dijadikan sebagai salah satu solusi dalam melakukan kriptanalisis. Hal ini lebih baik daripada penggunaan metode *brute force* konvensional yang memproses seluruh karakter dari seluruh kata dalam kamus dalam mencari kunci yang sesuai,

7. Daftar Pustaka

[ChC06] Christensen, Chris, Cryptography of the Vigenere Cipher, 2006

[JTH08] Joel THP Hutasoit, Penerapan Algoritma Backtracking pada Proses Kriptanalisis terhadap Hasil Enkripsi Vigenere Cipher dengan Menggunakan Pendekatan Dictionary Attack, 2008

[MOV97] A. Menezes, P. v. Oorschot, and S Vanstone, Hand-book of Applied Crypthography, CRC Press, 1997