

# Prosiding Seminar Nasional Pengamanan Jaringan (SNiPer)

*by* Ari Eko Wardoyo

---

**Submission date:** 12-Feb-2020 10:08AM (UTC+0700)

**Submission ID:** 1255880517

**File name:** umj-1x-ariekoward-441-1-jurnala-otext.pdf (301.98K)

**Word count:** 1347

**Character count:** 8538

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

Ari Eko Wardoyo<sup>1</sup>, Agung Nilogiri<sup>2</sup>  
Dosen Fakultas Teknik, UNMUH Jember  
Jl. Karimata 49 Jember – 68121  
Email: <sup>1</sup>arieeko319@gmail.com, <sup>2</sup>agung.nilogiri@gmail.com

### ABSTRAK

Hal yang paling sering terjadi pada proses kriptanalisis adalah para kriptanalisis 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 kriptanalisis. Salah satu teknik yang banyak dipakai untuk menentukan cipher key adalah exhaustive attack atau brute force attack. Kelemahan teknik ini adalah hanya 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 kriptanalisis 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 Dekripsi : 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 plaintexts yang berada pada baris paling atas dengan huruf cipher key di kolom paling kiri.

Penggunaan bujur sangkar vigenere untuk memperoleh ciphertext dengan

menggunakan cipher key yang ditentukan memiliki aturan jika panjang karakter kunci lebih pendek dari panjang plaintext, maka kunci diulang penggunaannya secara periodik.

Proses enkripsi sebuah plaintext menjadi ciphertext dengan menggunakan cipherkey "KUNCI" dapat dituliskan sebagai berikut:

Plaintext : PESAN  
Chiperkey : KUNCI  
Ciphertext : ZYFCV

Dapat dilihat bahwa ciphertext yang dihasilkan merupakan pergeseran huruf plaintext sejauh cipher key.

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

Brute force attack atau exhaustive attack adalah salah satu teknik yang dapat digunakan untuk pencarian cipher key.

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 *cipher key* 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 pendekripsian.

## 2. Permasalahan dan batasannya

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

Batasan pemodelan seperti yang dimaksud di atas adalah sebagai berikut :

- Bahasa yang digunakan *plaintext* maupun *cipher key* adalah bahasa Indonesia.
- Selain huruf, *Plaintext* dan *cipher key* 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)

TEKNIKEXHAUSTIVEVIGENERECIPHER  
MEMANFAATKANKAMUS

KAMUSKAMUSKAMUSKAMUSKAMUSKAMUS  
KAMUSKAMUSKAMUSKA

DEWHAUEJBSESFCNOVUAWXEDYUSPTYJ  
WEYUFPAMNCKN WUEES

Pada software yang dibuat disertakan kamus bahasa Indonesia kosakatanya dapat ditambahkan sendiri dapat digunakan sebagai bahan referensi dalam proses kriptanalisis dengan algoritma *Exhaustive Attack* berlangsung.

Dari paparan di atas permasalahan yang harus diselesaikan pada kali adalah pencarian *cipher key* dari *ciphertext* yang diberikan dan dilanjutkan dengan pencocokan *plaintext* dengan menggunakan kamus bahasa Indonesia.

## 3. Metode Pemecahan Masalah

Adapun metode pemecahan masalah ini antara lain :

### 1. Pemecahan masalah.

Pemecahan masalah dinyatakan sebagai vektor dari *n-tuple*:

$Y = (y_1, y_2, \dots, y_n)$ ,  $y_i$  himpunan berhingga  $S_i$ .

Misal:  $S_i = \{0, 1\}$ ,

$y_i = 0$  atau  $1$

diterjemahkan  $y_i =$  benar atau salah

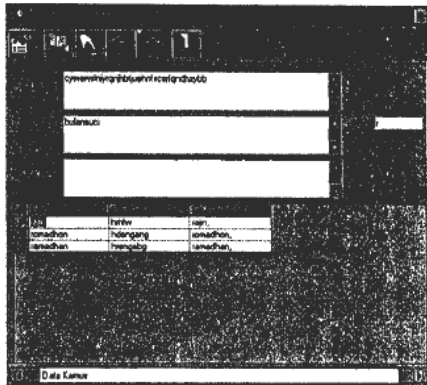
### 2. Pembangkit nilai vektor pemecahan masalah

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

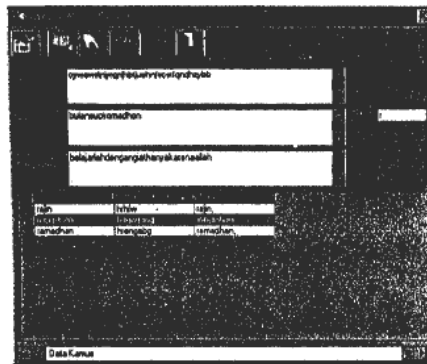
### 3. Pembatas

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.





Gambar 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 :

#### 1. Pemecahan masalah.

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

$X = (y_1, y_2, \dots, y_n)$ , dimana

$Y_i$  adalah 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 plaintext yang dihasilkan sesuai sebagian atau keseluruhan dengan kata yang terdapat dalam referensi kamus.

#### 6. Kesimpulan dan Saran

- Penerapan teknik *exhaustive attack* pada proses kriptanalisis *vigenere ciphertext* menggunakan bantuan kamus bahasa Indonesia memberikan hasil dekripsi *ciphertext* lebih cepat daripada penggunaan *exhaustive attack* konvensional. Semakin banyak kosa kata kamus yang digunakan, waktu yang dibutuhkan untuk mendekripsi *vigenere ciphertext* semakin lama, namun akan mempermudah penemuan *cipherkey* dan *plaintextnya*.
- Proses pendekripsian tidak dibatasi oleh spasi sehingga tidak memerlukan pola perulangan pada *ciphertextnya*.
- Metode ini berhasil mendekripsi *vigenere ciphertext* dimana *cipherkey* dan *plaintextnya* 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 Vigenère 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  
Cryptography, CRC Press, 1997

# Prosiding Seminar Nasional Pengamanan Jaringan (SNIPer)

---

## ORIGINALITY REPORT

---

**22%**

SIMILARITY INDEX

**21%**

INTERNET SOURCES

**1%**

PUBLICATIONS

**1%**

STUDENT PAPERS

---

## PRIMARY SOURCES

---

**1**

**webmail.informatika.org**

Internet Source

**13%**

---

**2**

**digilib.unmuhjember.ac.id**

Internet Source

**8%**

---

**3**

**B. Pfitzmann, M. Waidner. "Analysis of liberty single-sign-on with enabled clients", IEEE**

**Internet Computing, 2003**

Publication

**1%**

---

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off