METODE KASISKI

Analisi Metode Kasiski dengan Contoh

Muchammad Husni
Nafia Rizky Yogayana - 5114100017
Keamanan Informasi Jaringan (C)

1. **Apa itu Metode Kasiski?**

Friedrich Kasiski adalah orang yang pertama kali memecahkan Vigènere cipher pada tahun 1863. Metode Kasiski membantu menemukan panjang kunci Vigenere cipher.

Metode Kasiski memanfaatkan keuntungan bahwa bahasa Inggris tidak hanya mengandung perulangan huruf, tetapi juga perulangan pasangan huruf atau tripel huruf, seperti TH, THE, dan sebagainya. Perulangan kelompok huruf ini ada kemungkinan menghasilkan kriptogram yang berulang.

Langkah-langkah metode Kasiski:

1. Temukan semua kriptogram yang berulang di dalam cipherteks (pesan yang panjang biasanya mengandung kriptogram yang berulang).

2. Hitung jarak antara kriptogram yang berulang

3. Hitung semua faktor (pembagi) dari jarak tersebut (faktor pembagi menyatakan panjang kunci yang mungkin)

4. Tentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut . Nilai tersebut mungkin adalah panjang kunci. Hal ini karena string yang berulang dapat muncul bertindihan (*coincidence*).

2. Analisis Metode Kasiski dengan Contoh

Contoh 1:

DYDUXRMHTVDV**NQD**QNW**DYDUXRM**HARTJGW**NQD**

Kriptogram yang berulang adalah DYUDUXRM dan NQD. Jarak antara dua buah perulangan DYUDUXRM adalah 18. Semua faktor pembagi 18 adalah {18, 9, 6, 3, 2}. Jarak antara dua buah perulangan NQD adalah 20. Semua faktor pembagi 20 adalah {20, 10, 5, 4, 2}.

Irisan dari kedua buah himpunan tersebut adalah 2. Panjang kunci kemungkinan besar adalah 2. Setelah panjang kunci diketahui, maka langkah berikutnya menentukan kata kunci. Kata kunci dapat ditentukan dengan menggunakan *exhaustive key search.*

Jika panjang kunci = *p*, maka jumlah kunci yang harus dicoba adalah 26^p . Namun, kita akan mencoba dengan analisa frekuensi.

Langkah-langkahnya sbb:

1. Misalkan panjang kunci yang sudah berhasil dideduksi adalah *n.* Setiap huruf kelipatan ke-*n* pasti dienkripsi dengan huruf kunci yang sama. Kelompokkan setiap huruf ke-*n* bersama-sama sehingga kriptanalis memiliki *n* buah “pesan”, masing-masing dienkripsi dengan substitusi alfabet-tunggal (dalam hal ini *Caesar cipher*).

2. Tiap-tiap pesan dari hasil langkah 1 dapat dipecahkan dengan teknik analisis frekuensi.

3. Dari hasil langkah 3 kriptanalis dapat menyusun huruf-huruf kunci. Atau, kriptanalis dapat menerka kata yang membantu untuk memecahkan cipherteks

Contoh 2:

LJVBQ STNEZ LQMED **LJV**MA MPKAU FAVAT **LJV**DA YYVNF JQLNP **LJV**HK VTRNF **LJV**CM LKETA **LJV**HU YJVSF KRFTT WEFUX VHZNP

Kriptogram yang berulang adalah **LJV**.

Jarak **LJV** ke-1 dengan **LJV** ke-2 = 15

Jarak **LJV** ke-2 dengan **LJV** ke-3 = 15

Jarak **LJV** ke-3 dengan **LJV** ke-4 = 15

Jarak **LJV** ke-4 dengan **LJV** ke-5 = 10

Jarak **LJV** ke-5 dengan **LJV** ke-6 = 10

Faktor pembagi 15 = {3, 5, 15}

Faktor pembagi 10 = {2, 5, 10}

Irisan kedua himpunan ini = 5. Jadi, panjang kunci diperkirakan = 5

Kelompokkan "pesan" setiap kelipatan ke-5, dimulai dari huruf cipherteks pertama, kedua, dan seterusnya.

Kelompok	**Pesan**	**Huruf yang paling sering muncul**
1	LSLLM FLYHL VLLLY KWV	L
2	JTQJP AJYQJ TJKJJ REH	J
3	VNMVK VVVLV RVEVV FFZ	V
4	BEEMA ADNNH NCTHS TUN	N
5	QZDAU TAFPK FMAUF TXP	A

Dalam Bahasa Inggris, 10 huruf yang yang paling sering muncul adalah E, T, A, O, I, N, S, H, R, dan D. Triplet yang paling sering muncul adalah **THE**. Karena **LJV** paling sering muncul di dalam cipherteks, maka dari 10 huruf tersebut semua kemungkinan kata 3-huruf dibentuk dan kata yang yang cocok untuk LJV adalah THE.

Jadi, kita dapat menerka bahwa LJV mungkin adalah THE.

Dari sini kita buat tabel yang memetakan huruf plainteks dengan cipherteks dan huruf-huruf kuncinya (ingatlah bahwa setiap nilai numerik dari huruf kunci menyatakan jumlah pergeseran huruf pada Caesar cipher):

Kelompok	Huruf Plaintext	Huruf Ciphertext	Huruf Kunci
1	T	L	S (=18)
2	H	J	C (=2)
3	E	V	R (=17)
4	N	N	A (=0)

5	O	A	M (=12)

Jadi, kuncinya adalah **SCRAM**.

Dengan menggunakan kunci SCRAM cipherteks berhasil didekripsi menjadi:

THEBE ARWEN TOVER THEMO UNTAI NYEAH

THEDO GWENT ROUND THEHY DRANT THECA

TINTO THEHI GHEST SPOTH ECOUL DFIND

atau dalam kalimat yang lebih jelas:

THE BEAR WENT OVER THE MOUNTAIN YEAH

THE DOG WENT ROUND THE HYDRANT THE CAT INTO THE HIGHEST SPOT HE COULD FIND

Sumber

http://haryanto.staff.gunadarma.ac.id/Downloads/files/7285/7.Algoritma+Kriptografi+Klasik+(bag+4).ppt

http://rahmanhidayat3.blogspot.co.id/2013/05/metode-kasiski.html

Tugas 3 – KIJ, Dimas Yoas Shailendra, Teknik Informatika FTIf ITS