View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Lumbung Pustaka UNY (UNY Repository)

P-94

PERAN ALGORITMA *CAESAR CIPHER* DALAM MEMBANGUN KARAKTER AKAN KESADARAN KEAMANAN INFORMASI

Donny Seftyanto, MegaApriani, Tony Haryanto
SekolahTinggi Sandi Negara
donnyseftyanto@gmail.com, akiraauriga@gmail.com,
tonyharyanto7@gmail.com

Abstrak

Caesar cipher adalah algoritma cipher substitusi yang menggunakan konsep pergeseran huruf dengan modulo 26. Secara matematis dapat dirumuskan sebagai berikut S= (T+K) Modulo 26. S= Teks Sandi T= Teks Terang K=Kunci. Algoritma ini biasanya digunakan untuk proses enkripsi suatu informasi yang bersifat khusus atau rahasia pada zaman romawi.

Pada zaman sekarang aspek kesadaran keamanan informasi menjadi suatu yang penting bagi masyarakat dunia. Perkembangan teknologi yang terus meningkat selalu diimbangi dengan kecanggihan tindak kejahatan. Hanya mengandalkan sistem keamanan tanpa disertai dengan pengembangan pola berfikir akan menjadi sia-sia. Pengenalan algoritma *Caesar Cipher* yang mudah dipahami ini kepada guru dan murid akan membangun karakter dan pola berfikir sehingga terciptanya masyarakat kreatif, cerdas, dan sadar akan keamanan.

Kata kunci: Algoritma, *Caesar Cipher*, Karakter, Keamanan

PENDAHULUAN

A. Latar belakang

Jika suatu saat anda ingin berkomunikasi atau berinteraksi melalui media atau alat komunikasi dengan orang lain, maka tentu anda ingin pesan atau informasi yang anda kirim sampai ke pihak yang dituju dengan aman. Ini adalah masalah keamanan pesan yang dinamakan kerahasian (*confidentiality*). Aman bisa berarti bahwa anda pasti ingin pesan yang dikirim sampai ke tujuan dengan utuh, artinya isi pesan yang anda kirim tidak berubah atau dimanipulasi oleh lawan atau pihak yang tidak berkepentingan (*Data Integrity*). Aman bisa juga berarti penerima harus yakin bahwa pesan yang sampai kepadanya adalah pesan yang anda kirim bukan dari orang lain yang berperan seperti anda dan anda yakin bahwa pesan yang anda kirim juga sampai ke penerima yang berhak (*Authentication*). Jika suatu saat anda sebagai penerima pesan, anda tentu tidak ingin pengirim pesan membantah telah mengirim pesan kepada anda. (*Repudiaton*). Padahal anda yakin bahwa anda menerima pesan dari orang tersebut, jika pengirim membantah telah mengirim pesan tersebut kepada anda maka anda perlu membuktikan ketidakbenaran penyangkalan tersebut (*Non Repudiation*).

Masalah masalah keamanan yang telah disebutkan diatas dapat terjadi pada kita semua tanpa terkecuali apalagi di zaman modern seperti saat ini dimana kegiatan sehari-hari sudah banyak menggunakan password. Kebiasaan dalam pembuatan password baik untuk account media social, tempat penyimpanan file penting sampai bank adalah dengan memakai kata-kata yang mudah ditebak seperti nama, tanggal lahir, alamat dan lain-lain. Hal ini sangat rentan terhadap aksi hacker untuk mencari password penting yang kita gunakan.

Dictionary attack salah satu cara hacker untuk mengetahui password penting yang kita miliki. *Dictionary attack* adalah suatu cara pencarian password menggunakan bantuan komputer dengan mencoba segala kemungkinan kombinasi huruf dan angka. Untuk mempercepat penyerangan atau pencarian sandi, kombinasi huruf dan angka akan dirancang sesuai dengan kata-kata yang sering muncul sehingga membentuk suatu kamus.

Password atau sandi yang mudah ditebak sangat berbahaya jika orang yang tidak berhak mengetahuinya. Sebagai contoh jika password cloud storage yang berisi data-data pekerjaan atau hasil karya kita diketahui, maka orang lain bisa menyalahgunakan hal tersebut atau yang parah adalah terjadinya aksi pembajakan hasil karya. Masalah tersebut dapat diselesaikan dengan kriptologi dalam hal ini kriptologi yang paling mudah dipahami oleh orang awam adalah kriptografi substitusi dengan algoritma *Caesar cipher*.

B. Rumusan masalah

Bagaimanakah peran *Caesar cipher* dalam membangun karakter akan kesadaran keamanan informasi?

C. Tujuan

1. Mengenalkan *Caesar cipher* pada masyarakat umum.
2. Menggunakan *Caesar cipher* untuk membangun karakter akan kesadaran keamanan informasi.

D. Manfaat penelitian

1. Memberikan kesadaran informasi kepada masyarakat.
2. Mengenalkan kepada pembaca tentang kriptologi khususnya Caesar cipher.
3. Meningkatkan penggunaan persamaan matematika dalam membangun karakter.
4. Mengenalkan bahwa matematika dapat diimplementasikan secara mudah dalam kriptografi.

PEMBAHASAN

A. Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu *autentikation, data integrity, confidentiality* dan *non repudiation.*

Suatu kriptografi mempunyai elemen elemen dasar yang perlu diketehui.

Plaintext	Ciphertext

1. Enkripsi
   adalah sebuah proses yang dapat dibaca

Paper	Sdshu
Uny	Xqb

Enkripsi (*Encryption*) menjadikan pesan (*plaintext)* menjadi pesan acak yang tidak dapat dibaca (*ciphertext*). Berikut adalah contoh enkripsi yang digunakan oleh Julius Caesar, yaitu dengan mengganti masing-masing huruf dengan 3 huruf selanjutnya

2. Dekripsi
   Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah *ciphertext* menjadi *plaintext* dengan menggunakan algortima 'pembalik' dan *key* yang sama.
   Contoh:

Ciphertext	Plaintext
Sdshu	Paper
Xqb	uny

3. Plaintext
   Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.
4. Ciphertext
   Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah.
5. Kunci

a. Kunci Simetris
   Skema enkripsi akan disebut symmetric-key apabila pasangan kunci untuk proses enkripsi dan dekripsinya sama

b. Kunci Asimetris
   Skema ini adalah algoritma yang menggunakan kunci yang ber beda untuk proses enkripsi dan dekripsinya

B. Algoritma Sandi

Algoritma sandi adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut harus memiliki kekuatan untuk melakukan (dikemukakan oleh Shannon):

1. konfusi/pembingungan (*confusion*), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya.
2. difusi/peleburan (*difusion*), dari teksterang sehingga karakteristik dari teksterang tersebut hilang. Sehingga dapat digunakan untuk mengamankan informasi.

Pada implementasinya sebuahal goritmas sandi harus memperhatikan kualitas layanan/*Quality of Service* atau QoS dari keseluruhan sistem dimana dia diimplementasikan. Algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itusendiri. Teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa. Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunanyaitu yang berisi elemen teks terang/*plaintext* dan yang berisi elemen teks

sandi/*ciphertext*. Enkripsi dan dekripsi merupakan fungsitransformasiantara himpunan - himpunan tersebut.

C. Chiper Substitusi

Chiper Substitution adalah sandi dimana setiap karakter dari *plaintext* (huruf atau angka) diganti atau di substistusi dengan karakter lain dalam susunan abjad. Tidak ada perubahan dalam susunan abjad asli yang digunakan pada *plaintext*. Contoh dari *Chiper Substitusi* adalah sandi Caesar, sandi Vigenère.

D. Caesar Cipher

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah table substitusi sebagai berikut:

```
Alfabet Biasa: 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
Alfabet Sandi: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut.

Teks Terang : JANGAN MENDEKATI BLOK D
Teks Sandi : MDQJD QPHQG HNDWL EORNG

Dengan mengkodekan setiap huruf alfabet dengan integer : ‘A’= 0 , ‘B’= 1,…, ‘Z’= 25, maka secara matematis pergeseran 3 huruf alfabetik ekivalen dengan melakukan operasi modulo terhadap plainteks P menjadi cipherteks C dengan persamaan

$$C = E(P) = (P + 3) \bmod 26 \qquad (1)$$

Karena ada 26 huruf didalam alphabet. Penerima pesan mengembalikan lagi cipherteks dengan operasi kebalikan, secara matematis dapat dinyatakan dengan persamaan

$$P = D(C) = (C - 3) \bmod 26 \qquad (2)$$

Dapat diperhatikan bahwa fungsi D adalah balikan (invers) dari fungsi E , yaitu :

$$D(C) = E^{-1}(P) \qquad (3)$$

Penggunaan dari Caesar cipher ini dapat dimodifikasi dengan mengubah jumlah gesaran (bukan hanya 3) dan juga arah geseran. Jadi kita dapat menggunakan Caesar cipher dengan geser 7 ke kiri, misalnya. Hal ini dilakukan untuk lebih menyulitkan orang yang ingin menyadap pesan sebab dia harus mencoba semua kombinasi (26 kemungkinan geser).

Salah satu pengembangan dari *Caesar cipher* adalah ROT13. Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai:

$$C = ROT13(M) \qquad (4)$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali.

$$M = ROT13\ (\ ROT13\ (M))\qquad (5)$$

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

ROT13 memang tidak didesain untuk keamanan tingkat tinggi. ROT13, misalnya digunakan untuk menyelubungi isi dari artikel (posting) di Usenet news yang berbau ofensif. Sehingga hanya orang yang betul-betul ingin membaca dapat melihat isinya. Contoh penggunaan lain adalah untuk menutupi jawaban dari sebuah teka teki (puzzle) atau jika kita ingin marah marah (memaki) akan tetapi ingin agar orang lain tidak tersinggung. (Orang yang ingin membaca makian kita harus melakukan konversi ROT13 sendiri.)

E. Cipher dan Matematika

Dasar keilmuan dari *Caesar cipher* sebagian besar adalah matematika yang antara lain mencakup teori bilangan, aljabar dan fungsi. Subbab matematika tersebut sudah diajarkan sejak pendidikan sekolah bahkan diperluas lagi di perguruan tinggi. Rumus *Caesar cipher* secara umum :

$$C = E(P) = (P + k) \bmod 26\qquad (6)$$

Dan Fungsi Dekripsi adalah

$$P = D(C) = (C - k) \bmod 26\qquad (7)$$

Catatan:

1. Pergeseran 0 sama dengan pergeseran 26(susunan huruf tidak berubah).
2. Pergeseran lain untuk k>25 dapat juga dilakukan namun hasilnya akan kongruen dengan bilangan bulat dalam modulo 26. Misalnya k=37 kongruen dengan 11 dalam modulus 26, atau $37 \equiv 11 \pmod{26}$.

Persamaan di atas menggunakan subbab matematika teori bilangan khususnya dengan modulus. Operasi modulus adalah sebuah operasi yang menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lainnya.

Contoh modulus :

$1 = 7 \bmod 2$

$2 = 5 \bmod 3$

Sebenarnya operasi modulus sudah dikenalkan sejak dini hanya saja banyak yang tidak tahu nama operasi tersebut. Selain menggunakan operasi modulus, *Caesar cipher* juga menggunakan aljabar dalam pengerjaannya. Aljabar dasar, yang mencatat sifat-sifat operasi bilangan riil, menggunakan simbol sebagai "pengganti" untuk menandakan konstanta dan variabel, dan mempelajari aturan tentang ungkapan dan persamaan matematis yang melibatkan simbol-simbol tersebut.

Diketahui : $r + 3 = 10$

Ditanyakan : $r = ?$

Penyelesaian :

$r + 3 - 3 = 10 - 3$

(sama sama dikurangi dengan bilangan yang sama yaitu3)

$r = 7$

Masih banyak lagi penggunaan matematika dalam *Caesar cipher*, kedua contoh di atas sudah kita pelajari di sekolah

F. Caesar Cipher dan Karakter Kesadaran Keamanan

Caesar cipher mengaplikasikan pelajaran matematika yang didapatkan pada kehidupan yang sebenarnya. Banyak sekali contoh penggunaannya antara lain dalam merahasiakan password Facebook, ATM, Yahoo, Gmail, dan lain-lain.

Langkah preventif yang paling mudah agar terhindar dari terbobolnya kata sandi yang dimiliki adalah dengan mengaplikasikan algoritma *Caesar cipher* sebagai pengacak password yang kita miliki. Sebagai contoh :

Password yang belum dienkripsi :

AKUSA YANGK AMU

Password yang sudah dienkripsi :

DNXVD BDQJN DPX

(*Caesar cipher* dengan kunci=3 / ROT 3)

Password yang mudah (akusayangkamu) berubah menjadi kata yang acak dan tidak memiliki makna (dnxvdbdqjndpx), hanya dengan algoritma yang sederhana yaitu *Caesar cipher*.

Ketika kita sudah terbiasa dalam merahasiakan sesuatu maka kita akan secara otomatis mengamankan data pribadi ataupun sesuatu yang dianggap penting agar terhindar dari ancaman keamanan informasi. Meskipun kita sudah mengamankan password kita, ada saatnya dimana kita lupa atau memberitahukan password yang kita punya. Kesalahan seperti itu harus diminimalisir. Saat kita belajar untuk mengatasi kelemahannya dan memperbaiki kelemahannya dan memunculkan kebiasaan positif yang baru maka inilah yang disebut dengan karakter. Karakter tidak bisa diwariskan, karakter tidak bisa dibeli dan karakter tidak bisa ditukar. Karakter harus dibangun dan dikembangkan secara sadar hari demi hari dengan melalui suatu proses yang tidak instan**.** Karakter bukanlah sesuatu bawaan sejak lahir yang tidak dapat diubah lagi seperti sidik jari. Untuk membangun karakter yang sadar akan keamanan informasi maka sejak dini harus sudah dikenalkan mengenai pengamanan kriptografi. Untuk mewujudkan hal tersebut, diperlukan adanya pengenalan kriptografi khususnya caesar cipher kepada anak.

Akan sangat baik jika ada sebuah bagian dari pelajaran yang memungkinkan murid untuk mengaplikasikan pelajaran matematika yang telah mereka dapatkan. Dan akan lebih baik bagi jika para guru dapat mengajar dalam cara yang menyenangkan para murid dan membuat mereka melihat kebutuhan akan pelajaran yang mereka dapatkan dalam hidup ini. Murid akan lebih ingin menguasai pelajaran jika mereka mengetahui cara untuk mengaplikasikan pengetahuan mereka dalam kehidupan sehari-hari. Untuk itu, salah satu cara yang dapat dilakukan adalah dengan memperkenalkan murid kepada kriptografi khususnya *Caesar cipher*.

Para murid seringkali melihat matematika sebagai sesuatu yang membosankan, dan hanya bisa dinikmati oleh mereka – mereka yang sudah terlebih dahulu diklasifikasikan sebagai "orang – orang matematika" Di SMA, matematika menja disemakin rumit, dan para murid sering kali melihatnya sebagai sebuah kumpulan rumus yang mungkin bisa digunakan dalam berbagai macam situasi masalah. Situasi – situasi seperti ini secara teoritis dapat diaplikasikan dalam sains, namun para murid biasanya jarang mengetahui aplikasi – aplikasi tersebut. Karena pada kenyataannya, kurikulum tidak memfokuskan aplikasi penyelesaian masalah pada situasi yang lebih rumit. Para murid baisanya mempelajari dan memodelkan kemampuan ini setelah diajarkan contoh-contoh sebelumnya. Banyak sikap negatif yang berkembang dari para murid terhadap matematika karena mereka tidak mengetahui keterhubungan matematika itu sendiri dengan cabang ilmu lainnya. Diharapkan pengenalan kriptografi ini akan meningkatkan ketertarikan para murid terhadap matematika karena melibatkan

pengacakan password dan penghitungan matematika. Hampir semua murid mempunyai pengalaman dengan permainan dan puzzle yang melibatkan petunjuk – petunjuk untuk menyelesaikan suatu masalah. Banyak yang bahkan sudah mencoba untuk mengembangkan kode mereka sendiri untuk berkomunikasi dengan teman – teman mereka sendiri tanpa ada yang dapat mengetahui pesan mereka.

Dalam pelajaran ini, para murid berperan dalam penemuan informasi, sementara guru bertindak sebagai fasilitator. Para guru hanya membutuhkan pemahaman khusus tentang materi, dan bisa ikut bersama-sama belajar dalam proses. Dalam pelajaran ini, para murid akan memiliki kesempatan untuk merundingkan matematika dan menemukan peraturan kriptografi mereka sendiri. Cara ini akan mendorong mereka untuk berpikir kreatif. Kriptografi bergantung pada kombinasi, topik yang muncul sebagai bagian dari kurikulum. Murid juga akan menggambarkan dan mengobservasi data dalam menghasilkan suatu kesimpulan. Pada kenyataannya, matematika sering kali memunculkan suatu masalah yang membutuhkan waktu berhari – hari, bahkan bertahun – tahun untuk dipecahkan. Bekerja secara kolaboratif sebagai satu tim untuk kemudian menghasilkan cara penyelesaian masalah bukan hanya cara pembelajaran yang berharga, tapi menjadi lebih realistis dalam hubungannya dengan cara memecahkan masalah matematika di kehidupan sehari – hari. Pelajaran kriptografi khususnya caesar cipher ini juga akan menyediakan kesempatan unik bagi para murid untuk melihat bagaimana matematika dan sains bisa bersama mengubah sejarah. Jika sejak dini sudah ditekankan untuk sadar akan keamanan informasi maka ketika sudah dewasa akan terbentuk karakter yang sadar akan keamanan informasi.

KESIMPULAN

Pembahasan yang kami lakukan berupa studi literatur, dapat ditarik beberapa kesimpulan bahwa :

`Karakter tidak bisa diwariskan, karakter tidak bisa dibeli dan karakter tidak bisa ditukar. Karakter harus dibangun dan dikembangkan secara sadar hari demi hari dengan melalui suatu proses yang tidak instan**.** Karakter bukanlah sesuatu bawaan sejak lahir yang tidak dapat diubah lagi seperti sidik jari. Untuk membangun karakter yang sadar akan keamanan informasi maka sejak dini harus sudah dikenalkan mengenai pengamanan kriptografi. Kriptografi yang mudah di implementasikan pada kehidupan sehari hari secara nyata dengan rumus matematika yang tidak sulit untuk di mengerti dan untuk mewujudkan hal tersebut, diperlukan adanya pengenalan kriptografi khususnya *Caesar cipher*. Pembentukan karakter kesadaran keamanan informasi yaitu dengan menerapkan *Caesar cipher* untuk menyembunyikan data teks yang bersifat rahasia atau penting.

DAFTAR PUSTAKA

LSN.2007.*Jelajah Kriptologi*.jakarta:LSN

Munir, Rinaldi. 2007.*Kriptografi.* Bandung : Informatika.

Namiesyva. *Kriptografi Sebagai Media Pembelajaran Dalamstudi Matematika Tingkat Sekolah,*. Bandung : ITB.

http://www.pendidikankarakter.com/peran-pendidikan-karakter-dalam-melengkapi-kepribadian/

http://edukasi.kompasiana.com/2012/09/30/membangun-karakter-melalui-sains/

http://id.wikipedia.org/wiki/Sandi_Caesar

http://codeindesign.com/dasar-kriptografi-enkripsi-dan-dekripsi/
http://www.scribd.com/doc/77585742/Kriptografi-Sebagai-Media-Pembelajaran-Dalam-Studi-Matematika-Tingkat-Sekolah