

Studi dan Eksplorasi Leet Sebagai Salah Satu *Cipher* Substitusi

Mohamad Abdul Kadir 13507134
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganessa 10 Bandung 40132, Indonesia
adi.stei@itb.ac.id

Abstract—The abstract is to be in fully-justified italicized text, at the top of the left-hand column as it is here, below the author information. The abstract is to be in 9-point, single-spaced type, and may be up to 8 cm long. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column. Leave two blank lines after the index terms, then begin the main text. All manuscripts must be in English.

Index Terms—About four key words or phrases in alphabetical order, separated by commas.

I. LATAR BELAKANG

Kemajuan teknologi informasi telah membuat peranan pengamanan computer menjadi semakin penting. Banyak kejahatan cyber yang memanfaatkan celah keamanan yang ada dan melakukan manipulasi. Pada saat ini banyak sekali cara-cara yang ditempuh untuk memperkuat pengamanan, seperti password pada email, nomor PIN pada ATM, keamanan data/informasi rahasia. Usaha yang dilakukan untuk mengurangi kejahatan cyber yaitu dengan memperkuat sistem keamanan komputer, yaitu dengan cara membuat algoritma penyandian (*cipher*) yang lebih kuat terhadap serangan. Ukuran dari kekuatan *chiper* tersebut adalah banyaknya usaha yang diperlukan dalam melakukan pemecahan dari kunci *cipher*.

Penyimpanan dan pengiriman data melalui media elektronik harus dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (*enkripsi* dan *dekripsi*) terhadap data yang akan dikirimkan. *Enkripsi* dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan *dekripsi* dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Algoritma penyandian sudah ada sejak zaman sebelum masehi dan memiliki sejarah yang panjang. Bangsa Mesir diketahui telah menggunakan algoritma penyandian sejak 4000 tahun sebelum masehi, dengan adanya temuan berupa *hyroglyph* yang tidak standar. Bukti lain adalah di Sparta Yunani sekitar permulaan 400 tahun sebelum masehi, yaitu para tentara Sparta menggunakan penyandian dengan alat yang bernama *scytale*. Alat ini merupakan pita panjang pada daun payrus dengan sebatang silinder. Cara kerja alat ini yaitu pita panjang dililitkan pada silinder, kemudian diatas pipa itu ditulis pesan secara horizontal, kemudian pita itu dilepas dari silinder, sehingga huruf-huruf pada pita itu tersusun acak sehingga tidak dapat dibaca. Kemudian pita tersebut dikirim. Setelah sampai tempat penerima, cara membacanya yaitu dengan menggulung kembali pita tersebut ke silinder yang memiliki diameter yang sama sehingga pesan yang semula dapat terbaca sesuai dengan maksudnya. Jadi kunci dari penyandian ini adalah besarnya diameter silinder tempat menggulung.

Selain dengan cara mekanik seperti pada *scytale*, dahulu juga terdapat algoritma kriptografi yang kemudian dikenal sebagai algoritma kriptografi klasik. Algoritma kriptografi klasik pada dasarnya terdiri dari *cipher* substitusi dan *cipher* transposisi. Algoritma klasik melakukan penyandian karakter per karakter. Caesar *Cipher* adalah salah satu dari algoritma klasik. Caesar *cipher* mula-mula digunakan oleh kaisar Romawi, Julius Caesar untuk menyandikan pesan yang ia kirim kepada para gubernurnya. *Cipher* ini diimplementasikan dengan caesar wheel, caranya dengan mengganti setiap karakter dengan karakter lain dalam susunan abjad secara berurutan. Selain caesar *cipher* banyak lagi algoritma klasik seperti *affine cipher* yang merupakan penyempurnaan dari caesar *cipher*, *hill cipher*. Caesar *cipher* merupakan *cipher* yang sangat rentan terhadap serangan karena hanya mensubstitusi per karakter dengan berurutan, sehingga jika diketahui satu karakter bersesuaian dengan huruf tertentu, maka dengan sangat mudah karakter lain pun terlihat. Untuk itu maka *cipher* substitusi pun berkembang, sehingga ditemukan substitusi

homofonik, cipher substitusi abjad majemuk dan substitusi poligram. Banyak lagi jenis cipher yang lain seperti Vigenere cipher yaitu cipher abjad majemuk yang dikembangkan oleh Blaise de Vigenere pada abad ke-16. Cara kerja cipher ini yaitu dengan menggunakan bujur sangkar vigenere untuk melakukan enkripsi. Cipher ini memiliki kunci berupa string. Cipher ini memang lebih sulit dipecahkan daripada caesar cipher, tetapi pada abad ke-19 cipher ini dapat dipecahkan oleh kasiski, yaitu dengan menentukan panjang kunci dengan cara menghitung perulangan dari ciphertekstanya.

Walaupun banyak kelemahan dari algoritma kriptografi klasik, namun kriptografi ini masih sering digunakan untuk berbagai hal terutama di dunia internet. Contoh penerapan cipher substitusi yang trend di dunia hacker internet adalah **Leet**.

II. CIPHER SUBSTITUSI

All printed material, including text, illustrations, and charts, must be kept within a print area of 17 cm wide by 25 cm high. Do not write or print anything outside the print area. All *text* must be in a two-column format. Columns are to be 8.25 cm wide, with a 0.5 cm space between them. Text must be fully justified.

The main title (on the first page) should begin 2.5 cm from the top edge of the page, centered, and in Times 20-point, non-boldface type. Capitalize the first letter of nouns, pronouns, verbs, adjectives, and adverbs; do not capitalize articles, coordinate conjunctions, or prepositions (unless the title begins with such a word). Leave a blank line after the title.

Author names and affiliations are to be centered beneath the title and printed in Times 11-point, non-boldface type. Multiple authors may be shown in a two- or three-column format, with their affiliations below their respective names. Affiliations are centered below each author name, italicized, not bold. Include e-mail addresses if possible. Follow the author information by three blank lines before main text.

The second and following pages should begin 2 cm from the top edge. On all pages, the bottom margin should be 2.7 cm from the bottom edge of the page for A4 paper.

Wherever Times is specified, Times Roman, or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times that you have access to. Please avoid using bit-mapped fonts if possible. True-Type 1 fonts are preferred. Type your main text in 10-point Times. Be sure your text is fully justified—that is, flush left and flush right. Please do not place any additional blank lines between paragraphs.

III. LEET

Leet (atau 1337), yang sering disebut juga **eleet** atau **leetspeak**, adalah alternative alphabet dalam bahasa Inggris yang umumnya digunakan di internet [1]. Leet adalah variasi kombinasi dari karakter ASCII untuk menggantikan huruf-huruf Latin [1]. Leet juga dapat dimasukkan dalam kategori cipher substitusi.

Leet telah berkembang sebagai jenis sistem komunikasi pengaburan karakter pada bulletin board user di komputer dan telah menjadi fenomena budaya [2]. Ekspresi dari leet diantaranya akronim sinonim, substitusi dengan nomor, tanda seru, dan kombinasi fonetis [2].

Leet merepresentasikan sikap dan sub-kebudayaan yang berkembang melebihi penggunaan leet sebagai sebuah sistem komunikasi. Leet membuat pola-pola tradisional sistem komunikasi berkembang.

A. Bentuk Komunikasi Baru

Bentuk komunikasi baru leet telah banyak dikembangkan. Pengguna Leet sering kali mengabaikan standard dan inovasi reward. Leet menambahkan penkamusan yang baru dan transposisi sehingga mempersulit proses decipher, terutama hardcore leet yang mentransposisi seluruh huruf asli.

Bentuk Soft Leet hanya dapat mentransposisi satu huruf dalam kata atau frase. Sebuah term soft leet yang cukup populer adalah “pwned” atau “pwn3d” yang aslinya adalah “owned” dan menunjukkan bahwa sudah dikalahkan dalam permainan atau dipermalukan di dalam kehidupan nyata. Dapat juga berarti pengambilalihan komputer seseorang.

Ekspansi offline Leet dibarengi dengan penyebaran leet attitudes dan konsep hacker komputer. Seperti spamming dengan leet, pemasaran dengan leet, berbincang dengan bahasa leet. Kecenderungan menggunakan leet dalam komunikasi semakin meningkat tanpa disadari.

Dengan adanya internet, telah membuat global subkultur penutur non-English, Leet digunakan dengan mengeksplorasinya melalui penyerapan banyak kata dan konsep non-English. Absorpsi kata baru ini dipengaruhi oleh bahasa pengguna baru internet.

Penutur non-English seringkali lebih cepat untuk mengambil dan memperluas Leet dari penutur English.

B. Asal Mula Leet

Perilaku cultural dan beberapa slang awal dibelakang leet dapat dilacak ke tahun 1970an dan awal 1980an, masa kejayaan era phreak telepon. Selama era tersebut, individu-individu dan kelompok informal berusaha untuk mengeksplorasi sistem telepon public di US, dan sering melakukan panggilan telepon illegal jarak jauh. Individu yang paling mahir dalam subkultur phreak telepon mendapat pengakuan dan status yang memungkinkan mereka untuk menjadi *bellwethers* budaya.

Ketika komputer bulletin board systems (BBSs) tersedia pada 1980an, budaya telepon phreak memperoleh

media tertulis di bursa online yang sering begitu lambat dan kaku karena pengguna akan mempersingkat frase untuk dapat mengirim pesan lebih cepat dan nyaman. Misalnya, 'you are' atau 'your' bisa disingkat menjadi "u r" atau "ur".

Bentuk Leet yang pendek umumnya dapat dilihat pada pesan SMS (Short Message Service) pada telepon selular. Popularitas bahasa yang leetish pada SMS didorong oleh desain keyboard pada kebanyakan ponsel. Ketika pengguna komputer mendapatkan keyboard QWERTY, pada ponsel kebanyakan keypad dibagi kedalam 3 huruf. Keypad mendorong penggunaan leet oleh pengguna ponsel.

Penggunaan Leet yang mengganti angka dan tanda baca pada huruf dapat ditelusuri dari tahun 1980-an ketika buletin administrator board berusaha untuk mencegah penggunaan BBSs untuk penyimpanan dan distribusi pornografi dan software yang dicuri. Untuk menghindari pembatasan BBS, ejaan dan kata-kata telah diubah oleh beberapa pengguna BBSs. Yang masih bertahan dari peninggalan masa itu adalah istilah Leet "pr(n)" dan "prOn", yang menunjukkan pornografi.

Peninggalan lain adalah terjemahan dari kata hacker, yang dilarang oleh beberapa administrator BBS. Terjemahan leetspeak awal untuk hacker atau h4cker menyebabkan penyaringan dan larangan istilah Leet, mendorong leetspeakers untuk mengembangkan bahasa yang lebih tidak jelas, terjemahan yang kurang dikenal seperti h4x0r dan |-|^><()| z.

Status pengguna BBS yang memperoleh akses ke daerah-daerah elit atau fitur dari sistem BBS mengarah pada penciptaan label "elit". Selanjutnya disingkat menjadi Leet atau "el Leet," tetap slang dan sikap anti-otoriteratas status elit unsur komunikasi Leet sebagai BBS pengguna bermigrasi ke Internet pada 1990-an dan Leet diperluas ke komunitas game online.

Polimorfik dari Leet serta penggunaannya oleh hacker dan gamer internet telah membuat popularitas Leet meningkat.

C. Perilaku Gaming

Tahun 1980-an dan awal 1990-an adalah masa kejayaan online multiplayer game berbasis teks, khususnya peran game fantasi yang disebut MUDs, untuk dungeon multi-user, domain, atau dimensi. MUDs menggabungkan aspek aksi permainan dengan teks pesan instant chatting. MUDs telah menciptakan *social universe* dimana istilah khusus dan konvensi linguistik dikembangkan. MUDs sedikit yang masih dimainkan pada hari ini karena telah terpinggirkan oleh munculnya game komputer grafis online.

Lingkungan game online dipenuhi oleh anak-anak muda yang berjuang untuk membedakan diri dari pesaing mereka dengan menciptakan dan menampilkan bentuk komunikasi yang inovatif. Ini merupakan lahan yang baik bagi perkembangan Leet. Leet adalah ekor merak dari generasi game.

D. Isu Keamanan

Perusahaan keamanan internet telah belajar mencari Leet sebagai indikator dari upaya penyusupan. Menggunakan ejaan alternatif untuk Leet, Jamal Khan, CEO perusahaan keamanan computer yang berbasis di Connecticut berkata:

L33t trapping through IDS/IPS mechanisms is simple. It is a matter of applying the correct transformation rules. However, the belief that a single L33t rule applies to the hacking community is wrong. Select groups structure and develop their own iterations of L33t speak.

Khan menemukan gaya leet yang berbeda yang digunakan oleh hacker cliques untuk membedakan diri dari script kiddies. Khan mengatakan bahwa ahli-ahli hacking kultur memandang rendah script kiddies, yang dipandang sebagai penyebab kerusakan dengan tools hacking dan script.

Dalam pembalikan ironis, sistem administrator dan pengguna komputer biasa semakin menggunakan Leet untuk menggagalkan hacker. Kamus otomatis program yang digunakan oleh hacker untuk menghasilkan sejumlah besar kombinasi login sampai ditemukan yang memungkinkan akses ke dalam sistem target. Memasukkan Leet ke password dapat membuat program kamus menjadi tidak berguna.

Seorang system administrator di pengadilan U.S. bankruptcy, Seattle dilaporkan membantu pengguna sistem memasukkan transposisi Leet di password mereka. Sebagian besar pengguna sistem memiliki pemahaman yang sedikit bahkan tidak ada tentang Leet, meskipun mereka sekarang menggunakan setiap hari di tempat kerja.

E. Mekanisasi Leet

Leet dapat degenerate dengan menghapus satu atau lebih huruf-huruf dan menggantinya dengan karakter, number, atau fonetik yang ekuivalen, semisal "eye" atau "3y3" untuk "T". Random kapitalisasi seperti "sUch aS tHiS" dapat pula digunakan.

Kosakata Leets seringkali diperluas dengan penambahan portmanteaus, yaitu kata-kata yang dibuat dengan menggabungkan kata-kata yang sudah ada,

seringkali dengan pemotongan.

leet-to-english dan English-to-leet online translator sudah ada di LearnLeetSpeak.com. Soft English-to-leet translator terdapat di AlbinoBlackSheep.com.

F. Leet Substitusi

Berikut ini beberapa substitusi pada leet untuk huruf-huruf dalam alphabet:

A

4, /, @, /-, ^, ä, a, aye

B

8, 6, |3, ß, P>, |:

C

[, ç, <, (

D

), o|, D), l>, |>, ð

E

3, &, £, ë, [-, €, ê, |=-

F

|=, ph, |#

G

6, &, (-, 9, C-, gee, (,

H

#, /-, [-, {=}, <~>, |-|,]-[,]{,]-[, ? , }-{-

I

1, !, |, &, eye, 3y3, i,][, i

J

.|, _|, ;, -)

K

X, |<, |{,]{, }<, |{

L

1 (1 can be used for either L or T), 7, 1_, |, |_, #, l

M

//., ^ ^, |v|, [V], {V}, |V|, /^^, (u), [JV[] , (V)

N

//, ^/, |\\, /\\, [\\], , <\\>, {\\}, [\\[] , n, /V,

O

0, 0), ?p, , *, ö

P

ph, |^, |*, |o, |^(o), |>, |", 9, [D, |?, |7

Q

9, (, <|, |^(o)|, ¶, O_

R

|2, P\\, |?, |^, lz, [z, 12, |2,

S

5, \$, z, §, ehs

T

7, +, -|-, 1, ']['

U

(_), |_, µ, v, ü

V

v

W

\\V, vv, '//' , \\^/, (n), \\V/, \\/, \\X/

X

><, +, ecks,)(, _

Y

Y, '/, `/, V/, \\-/ , j, ¥, %

Z

2, z, -_, -/_

|\\|0\\V ¥0µ @|2€ |2€@p¥ 70 |-|@V€ fµ|\\| \\V/i7|-| €€€7!

IV. PENGUJIAN LEET

Berikut ini contoh penggunaan leet dalam mensubstitusi huruf-huruf pada artikel tertentu.

BANDUNG, itb.ac.id - Pesatnya perkembangan teknologi satelit mendorong kemajuan pada bidang telekomunikasi. Pada saat ini, satelit menjadi bagian penting dalam penyebaran arus informasi di seluruh dunia. ITB berkesempatan untuk menjadi salah satu perguruan tinggi di mana riset mengenai teknologi satelit dilakukan. Bertempat di Laboratorium Telekomunikasi Radio dan Gelombang

Mikro (LTRGM) kampus ITB, Kantor Berita ITB berkesempatan untuk mewawancarai beberapa peneliti yang tergabung dalam proyek penelitian WINDS pada Jumat. *Wideband Inter Networking engineering test and Demonstration Satellite* atau disingkat dengan WINDS, adalah program penelitian yang diprakasai oleh *Japan Aerospace Exploration Agency (JAXA)*. Penelitian WINDS dimulai sejak tahun 2008, diawali dengan peluncuran satelit ini oleh roket H2A pada tanggal 23 Februari 2008. Satelit berteknologi Ka band ini, memiliki cakupan di wilayah Asia Pasifik dan khususnya Asia Tenggara. Pada saat ini terdapat sepuluh lokasi penelitian tersebar di seluruh Asia Pasifik. Masa kerja satelit ini sepanjang lima tahun, terhitung sejak Oktober 2008 hingga Maret 2013.

dalam Leet:

B4NDµN9, 17b.4(.1D - P3\$47n¥4
p3r|{3mb4n94n 73|{n0£091 \$473£17
m3n£0r0n9 |{3m4ju4n p4D4 b1D4n9
73£3|{0mµn1|{4\$1. P4D4 \$447 1n1,
\$473£17 m3nj4D1 b4914n p3n71n9 D4£4m
p3n¥3b4r4n 4rµ\$ 1nf0rm4\$1 D1 \$3£µrµh
Dµn14. 17B b3r|{3\$3mp474n µn7µ|{
m3nj4D1 \$4£4h \$47µ p3r9µrµ4n 71n991 D1
m4n4 r1\$37 m3n93n41 73|{n0£091 \$473£17
D1£4|{µ|{4n. B3r73mp47 D1 £4b0r470r1µm
73£3|{0mµn1|{4\$1 R4D10 D4n 93£0mb4n9
M1|{r0 (£7R9M) |{4mpµ\$ 17B, |{4n70r
B3r174 17B b3r|{3\$3mp474n µn7µ|{
m3w4w4n(4r41 b3b3r4p4 p3n3£171 ¥4n9
73r94bµn9 D4£4m pr0¥3|{ p3n3£1714n
W1ND\$ p4D4 Jµm47
W1D3b4nD 1n73r N37w0r|{1n9 3n91n33r1n9
73\$7 4nD D3m0n\$7r4710n \$473££173 474µ
D1\$1n9|{47 D3n94n W1ND\$, 4D4£4h
pr09r4m p3n3£1714n ¥4n9 D1pr4|{4\$41
0£3h J4p4n 43r0\$p4(3 3xp£0r4710n
493n(¥ (J4X4). P3n3£1714n W1ND\$
D1µµ£41 \$3j4|{ 74hµn 2008, D14w4£1
D3n94n p3£µn(µr4n \$473£17 1n1 0£3h
r0|{37 H24 p4D4 74n994£ 23 f3brµ4r1
2008. \$473£17 b3r73|{n0£091 |{4 b4nD
1n1, m3m1£1|{1 (4|{µp4n D1 w1£4¥4h
4\$14 P4\$1f1|{ D4n |{hµ\$µn¥4 4\$14
73n994r4. P4D4 \$447 1n1 73rD4p47
\$3pµ£µh £0|{4\$1 p3n3£1714n 73r\$3b4r D1
\$3£µrµh 4\$14 P4\$1f1|{. M4\$4 |{3rj4
\$473£17 1n1 \$3p4nj4n9 £1m4 74hµn,
73rh17µn9 \$3j4|{ 0|{70b3r 2008 h1n994
M4r37 2013.

V. KESIMPULAN

Leet adalah substitusi cipher sederhana yang dapat digunakan untuk mempermudah hacker mendapatkan password. Dapat juga menjadi bahasa komunikasi di internet baik untuk gaming maupun hacking.

Leet terbukti baik digunakan dalam pembuatan password user.

REFERENCES

[1] Leet, <http://en.wikipedia.org/wiki/Leet>, diakses tanggal 6 Maret 2011 pkl 23.00 WIB.

[2] A Leet Primer, <http://www.technewsworld.com/story/47607.html>, diakses tanggal 6 maret 2011 pkl 23.15

Leet translator<http://www.albinoblacksheep.com/text/leet>, diakses tanggal 23 Maret 2011 pkl 11.00

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

ttd

Mohamad Abdul Kadir 13507134