Penerapan Algoritma Kriptografi pada Penyembunyian Konten Eksplisit di Forum Publik

Akeyla Pradia Naufal - 13519178
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
akeylanaufal@gmail.com

***Abstrak*—Dalam sebuah forum publik di internet, seringkali terdapat beberapa konten eksplisit yang seharusnya tidak diakses oleh orang banyak, atau setidaknya untuk kalangan tertentu. Diperlukan adanya mekanisme penyembunyian konten eksplisit tersebut sedemikian hingga konten tersebut ditampilkan dalam bentuk yang tidak dapat dibaca secara sekilas. Makalah ini akan membahas mengenai penerapan algoritma kriptografi klasik dalam menyembunyikan konten eksplisit. Kriptografi klasik yang digunakan adalah ROT13, cipher substitusi homofonik, Playfair cipher, dan Vigenere cipher**

***Kata kunci*—Konten eksplisit, kriptografi klasik, penyembunyian konten, ROT13, cipher substitusi homofonik, playfair cipher, vigenere cipher**

I. PENDAHULUAN

Dalam sebuah forum publik di internet, pengaksesan konten pada umumnya dapat dilakukan berdasarkan ada atau tidaknya akun yang terdaftar saja. Kondisi ini membuat siapapun yang dapat membuat email dan mendaftarkan email tersebut ke forum tersebut akan dapat mengakses konten di forum tersebut. Pendaftaran ini juga pada umumnya tidak dapat membedakan apakah akun tersebut dimiliki oleh orang yang memenuhi kriteria forum. Umumnya, kriteria yang tidak dapat dipenuhi adalah usia.

Eksplisit artinya dinyatakan dalam bentuk yang jelas tanpa membuat kebingungan atau keraguan. Tidak terdapat definisi yang tunggal mengenai konten eksplisit. Konten eksplisit pada umumnya didefinisikan sebagai konten yang berisi setidaknya salah satu dari hal berikut secara jelas: kekerasan fisik dan/atau mental, kegiatan seksual, kata kasar dan jorok, umpatan, hinaan, ujaran kebencian, dan hal yang ofensif ke kalangan tertentu.

Beberapa studi telah menunjukkan bahwa terdapat beberapa akibat negatif dari pembacaan konten eksplisit. Studi telah menunjukkan bahwa waktu yang dihabiskan untuk melihat pornografi terkait dengan seberapa seksis seseorang itu. Sedangkan, seberapa seksis seseorang terkait erat dengan kekerasan dan pelecehan seksual yang akan dia lakukan [1]. Lebih lanjut, semakin muda seorang laki-laki saat mengakses pornografi untuk pertama kali, semakin besar kemungkinan mereka menjadi pelaku pelecehan seksual [2]. Konten yang berisi kekerasan juga memiliki dampak yang negatif. Game yang berisi konten kekerasan, misalnya, dapat membuat perilaku pemainnya menjadi lebih kasar [3]. Selain itu, film yang memuat konten kekerasan dapat meningkatkan kegelisahan kelompok usia dewasa muda (18 – 24 tahun) [4].

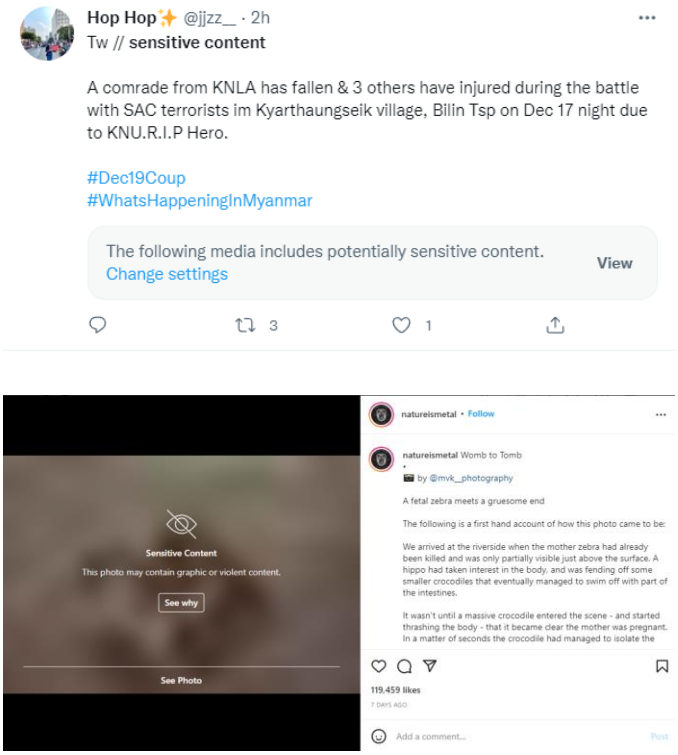
Untuk mengantisipasi dampak negatif dari konten eksplisit ini, terdapat beberapa upaya berbeda yang dilakukan oleh pihak pengelola forum yang bersangkutan. Upaya tersebut dapat berupa larangan untuk konten eksplisit tertentu, penyembunyian konten eksplisit bagi pengguna tertentu, atau pemberian tanda bagi konten eksplisit. Selain itu, juga terdapat forum-forum yang membiarkan beberapa tipe konten eksplisit.

Beberapa media sosial seperti Facebook, Instagram, Twitter, dan Quora memiliki sistem moderasi konten. Terdapat orang-orang yang bekerja sebagai moderator konten yang bertugas melihat unggahan-unggahan pengguna dan akan menghapusnya apabila terbukti melanggar kebijakan komunitas media sosial tersebut. Moderator ini juga bisa saja sedikit atau banyak dibantu oleh kecerdasan buatan dalam memoderasi konten. Permasalahan dari metode ini adalah adanya resiko sangat besar bagi para moderator untuk mengalami stres dan kerusakan mental dikarenakan berinteraksi langsung dengan banyak konten eksplisit.

Upaya yang lain dari pihak forum adalah menyembunyikan konten eksplisit bagi pengguna tertentu. Sebagai contoh, media sosial berbagi video Youtube memiliki beberapa aturan mengenai video apa saja yang boleh ditampilkan. Terdapat beberapa kategori video yang tidak melanggar aturan Youtube tetapi dirasa tidak cocok untuk ditampilkan kepada penonton yang berusia di bawah 18 tahun. Contohnya adalah video yang menunjukkan cedera dari penyintas kecelakaan lalu lintas atau video yang menunjukkan tarian erotis. Video ini hanya akan dapat diakses oleh penonton yang sudah masuk ke dalam akunnya. Permasalahan dari metode ini adalah pengguna biasanya dapat menuliskan umur yang tidak sesuai agar dapat mengakses konten tersebut.

Tanda juga bisa diberikan untuk konten yang eksplisit, pada umumnya dilakukan secara otomatis oleh forum. Contohnya adalah pada Twitter dan Instagram, konten-konten eksplisit yang tidak melanggar kebijakan komunitas akan ditandai sebagai konten yang sensitif dan pengguna perlu menekan tombol untuk menyetujui melihat konten tersebut. Permasalahan dari metode ini adalah biasanya hanya dapat

menyembunyikan gambar dan membiarkan teksnya tetap terbaca. Selain itu, penyembunyian gambar dan konten sekaligus dapat membuat pengguna bingung atas konten eksplisit seperti apa yang sedang ia hadapi.



Terakhir, komunitas forum juga dapat memberikan tanda sendiri atas konten eksplisit yang tidak melanggar aturan komunitas tetapi mungkin sensitif bagi sebagian orang. Salah satunya adalah dengan menuliskan frasa “Trigger Warning” atau biasa disingkat “TW” lalu diikuti oleh kategori konten sensitif tersebut. Sebagai contoh, “tw // sexual abuse” yang berarti konten tersebut memuat hal yang tergolong kekerasan seksual. Permasalahan dari hal ini adalah tidak adanya mekanisme menyembunyikan gambar selain menaruhnya di situs web eksternal.

Selain itu, pengguna juga dapat secara manual memblokir atau membatasi akses bagi akun-akun yang disinyalir sering membagikan konten sensitif. Beberapa media sosial, seperti Twitter, juga memfasilitasi pemblokiran konten-konten yang memuat kata-kata pilihan pengguna.

Pada makalah ini akan dibahas mengenai alternatif cara menyembunyikan konten eksplisit, terutama yang tidak melanggar kebijakan komunitas forum, dengan memanfaatkan kriptografi.

II. Dasar Teori

A. *Kriptografi*

Kriptografi adalah seni dan sains dari menjaga pesan agar aman dalam konteks pengiriman pesan [5]. Keamanan pesan dapat dijaga dengan mengubah bentuk pesan dalam bentuk lain yang menyembunyikan bentuk pesan awal. Pesan awal ini disebut sebagai plainteks sedangkan bentuk pesan yang baru disebut sebagai cipherteks. Proses mengubah plainteks menjadi cipherteks disebut sebagai enkripsi dan proses sebaliknya disebut sebagai dekripsi.

B. *Algoritma Kriptografi Simetris dan Asimetris*

Dalam mengenkripsi dan mendekripsi pesan, yang diharapkan adalah hanya kedua pihak yang mengetahui mekanisme enkripsi dan dekripsi pesan. Mekanisme tersebut adalah dengan menggunakan kunci untuk mengenkripsi dan mendekripsi. Sehingga, dalam melakukan enkripsi diperlukan kunci dan plainteks untuk menghasilkan cipherteks. Sementara, untuk mendekripsi diperlukan kunci dan cipherteks. Kunci untuk enksipsi dan dekripsi bisa sama atau berbeda. Algoritma kriptografi yang memanfaatkan dua kunci yang berbeda untuk enkripsi dan dekripsi disebut sebagai algoritma kriptografi asimetris. Algoritma kriptografi yang memanfaatkan dua kunci yang sama untuk enkripsi dan dekripsi disebut sebagai algoritma kriptografi simetris.

C. *Kriptografi Klasik dan Kriptografi Modern*

Kriptografi klasik adalah kriptografi yang bekerja atas karakter alfabet dan bertipe kriptografi simetris. Sementara itu, kriptografi modern adalah kriptografi yang bekerja atas bit atau byte dan dapat bertipe kriptografi simetris atau asimetris. Kriptografi modern lebih unggul dari kriptografi klasik dalam kriteria kesusahan memecahkan cipherteks tanpa mengetahui algoritma dan/atau kunci yang dipakai.

Dalam kriptografi klasik, terdapat dua cara utama untuk menghasilkan cipherteks: substitusi dan transposisi karakter. Substitusi karakter sendiri terdiri dari empat tipe: cipher abjad-tunggal, cipher substitusi homofonik, cipher abjad-majemuk, dan cipher substitusi poligram. Sementara itu, transposisi karakter dilakukan dengan mengubah urutan karakter di plainteks. Transposisi dan substitusi dapat dipakai secara bersamaan untuk meningkatkan keamanan cipherteks.

D. *Caesar Cipher dan ROT13*

Caesar cipher merupakan salah satu algoritma kriptografi klasik yang bertipe cipher abjad-tunggal. Artinya, satu huruf di plainteks akan diganti dengan satu huruf yang sama di cipherteks. Dengan menotasikan huruf-huruf latin ‘a’ hingga ‘z’ secara berturut-turut sebagai bilangan 0 hingga 25, versi asli dari Caesar cipher akan mengenkripsikan huruf dengan urutan p sebagai huruf dengan urutan $p + 3 \pmod{26}$. Untuk mendekripsikannya, cukup ubah huruf dengan urutan p sebagai huruf dengan urutan $p - 3 \pmod{26}$. Sebagai contoh, ‘a’ akan dienkripsikan sebagai huruf dengan urutan $0 + 3 = 3$, yakni ‘d’.

Caesar cipher ini dapat diperumum dengan mengganti bilangan 3 dengan bilangan lain di antara 1 hingga 25. Ketika diganti dengan bilangan 13, diperoleh satu algoritma kriptografi yang memiliki properti yang menarik: rumus untuk mengenkripsi dan mendekripsi sama persis. Artinya, mengenkripsi satu plainteks dengan algoritma ini dua kali berturut-turut akan menghasilkan plainteks yang sama. Hal ini disebabkan oleh $13 + 13 \equiv 0 \pmod{26}$. Algoritma ini disebut

sebagai ROT13, diambil dari kata *rotate* dan 13. ROT13 merupakan algoritma yang sering dipakai di beberapa forum internet untuk membahas solusi teka-teki, *spoiler* untuk suatu film, atau teks yang ofensif.

Algoritma ini sederhana dan tidak memerlukan tenaga komputasi yang besar. Di sisi lain, kesederhanaan algoritma ini juga memudahkan pemecahan cipherteksnya. Salah satu cara yang bisa dipakai adalah dengan analisis frekuensi karakter. Selain itu, kemungkinan pergeserannya juga hanya ada 26 sehingga sangat mudah untuk dipecahkan secara *brute force* semua kemungkinannya.

E. Cipher Substitusi Homofonik

Cipher substitusi homofonik adalah algoritma kriptografi yang memetakan setiap karakter ke dalam satu atau lebih pasangan karakter yang mungkin. Sebagai contoh, huruf 'a' dapat dipetakan menjadi 'BA', 'GT', 'RI', atau 'HY' sedangkan huruf 'l' dapat dipetakan menjadi 'SJ' atau 'XY'. Sehingga, 'lala' dapat dienkripsikan sebagai 'SJBAXYRI' atau 'XYHYSJRI'. Perlu diperhatikan agar suatu pasangan karakter hanya dapat didekripsi ke satu karakter saja.

Cipher substitusi homofonik ini dapat mengurangi kemungkinan pemecahan dengan analisis frekuensi karakter apabila banyak pasangan hasil pemetaan karakternya disesuaikan dengan frekuensi karakter di suatu bahasa. Sebagai contoh, apabila huruf 'a' muncul kira-kira 8 kali lebih sering dari huruf 'x' maka 'a' sebaiknya dipetakan dengan delapan pasangan sedangkan 'x' hanya dengan satu pasangan.

F. Playfair Cipher

Playfair cipher adalah algoritma kriptografi yang memetakan pasangan huruf ke pasangan huruf lain. Algoritma pemetaan ini memanfaatkan sebuah tabel berukuran 5 x 5 yang berisi semua huruf latin kecuali satu (biasanya 'j' atau 'v') dengan urutan tertentu. Pertama, ganti semua huruf yang tidak ada di tabel dengan huruf yang sudah ditentukan (biasanya 'j' menjadi 'i' atau 'v' menjadi 'u'). Setelah itu, huruf-huruf di plainteks akan dibagi sepasang-sepasang secara berurutan. Apabila ada dua huruf kembar berurutan, sisipkan huruf yang jarang dipakai seperti 'x'. Apabila banyak huruf ganjil, sisipkan huruf yang jarang tadi di akhir. Setelah didapat semua pasangan huruf, lihat tabel huruf tadi dan temukan posisi dua huruf yang sepasang ini. Berdasarkan posisinya, hal berikutnya yang dilakukan adalah:

1. Jika kedua huruf berbeda baris dan berbeda kolom, maka pasangan tersebut diganti dengan huruf yang ada di baris seperti baris huruf pertama dan di kolom seperti kolom huruf kedua serta huruf yang ada di baris seperti huruf kedua dan di kolom seperti kolom huruf pertama
2. Jika kedua huruf berada di baris yang sama, maka pasangan tersebut diganti dengan huruf yang persis di kanan huruf pertama dan huruf yang persis di kanan huruf kedua
3. Jika kedua huruf berada di kolom yang sama, maka pasangan tersebut diganti dengan huruf yang persis di bawah huruf pertama dan huruf yang persis di bawah huruf kedua

Perhatikan bahwa sifat 'kanan' dan 'bawah' di sini bersifat siklik.

Dekripsi cipherteks dapat dilakukan dengan tabel yang sama tetapi dengan algoritma yang terbalik. Perhatikan juga bahwa hasil yang diperoleh tidak benar-benar sama karena bisa saja terdapat dua huruf kembar berurutan yang sekarang disisipi huruf 'x', huruf 'x' di akhir teks yang tidak berarti, dan juga huruf 'j' yang dituliskan sebagai 'i' karena 'j' diganti menjadi 'i' di awal algoritma. Permasalahan lain dari Playfair cipher adalah satu pasangan huruf dipetakan ke satu pasangan huruf yang sama. Artinya, hanya terdapat maksimal 26 x 26 = 676 kemungkinan pasangan huruf yang bersesuaian dalam satu tabel. Untungnya, banyak tabel yang tersedia sangat banyak yakni 25!.

G. Vigenere Cipher

Vigenere cipher merupakan sebuah cipher abjad-majemuk yang menggunakan kunci dalam mengenkripsi dan memanfaatkan penjumlahan dalam modulo 26. Pada Vigenere cipher, terdapat sebuah kunci yang merupakan sekumpulan karakter sepanjang plainteks. Cipherteks diperoleh dengan menjumlahkan dalam modulo 26 setiap karakter di kunci dan plainteks yang berada di urutan yang sama. Dengan mengetahui kunci dan cipherteks, plainteks dapat diperoleh dengan mengurangkan keduanya dalam modulo 26.

Terdapat beberapa tipe kunci yang dapat dipakai. Tipe pertama adalah kunci berulang. Kunci yang berulang adalah kunci yang berasal dari satu string kunci yang lebih pendek dari plainteksnya sehingga string kunci tersebut diulang-ulang agar memiliki total panjang sama dengan plainteksnya. Sebagai contoh, kunci awal bisa berupa 'kunci' dan plainteksnya adalah 'kriptografi' maka kunci yang dihasilkan adalah 'kuncikuncik'. Tipe yang kedua adalah kunci-auto. Kunci ini dihasilkan dari satu string kunci yang lebih oendek dari plainteks yang kemudian disambung dengan bagian awal dari plainteks itu sendiri. Sebagai contoh, kunci awal bisa berupa 'kunci' dan plainteksnya dapat berupa 'kriptografi' maka kunci yang dihasilkan adalah 'kuncikripto'. Terakhir, ada tipe kunci yang disebut sebagai *running-key*. Kunci ini adalah string yang merupakan potongan dari teks yang sangat panjang seperti lirik lagu atau naskah undang-undang.

III. IMPLEMENTASI

Dalam mengimplementasikan algoritma kriptografi dalam menyembunyikan konten eksplisit dari forum publik, penerapannya akan dicoba pada aplikasi Twitter menggunakan berbagai algoritma klasik yang sudah dibahas di dasar teori dan konten yang ditulis berupa tiga teks eksplisit contoh.

A. Contoh Teks Eksplisit

Terdapat tiga teks eksplisit yang kesemuanya membahas mengenai kasus pembunuhan. Ketiga teks ini berbahasa Indonesia dan memiliki panjang teks yang berada di interval.

Teks pertama diambil dari [6]. Teks ini membahas kronologi pembunuhan yang dilakukan oleh Ryan Jombang pada tahun 2008.

Merasa terdesak, Ryan pergi ke dapur dan mengambil pisau dan menusuk Heri tepat di ulu hati. Heri ambruk dan merintih kesakitan. Dalam kondisi tak berdaya, Ryan menyeret Heri ke kamar mandi. Tubuhnya ditelentangkan, kepalanya dihajar dengan tongkat besi.

Teks kedua diambil dari [7]. Teks ini membahas kronologi pembunuhan yang dilakukan oleh Rio Martil di Banyumas pada tahun 2001 silam.

Pukulan yang dilakukan berkali-kali oleh Rio itu menggunakan dua martil, satu di tangan kiri, satunya di kanan. Dalam beberapa pukulan saja, kepala Jeje sudah remuk. Darah dan isi kepala berhamburan. Percikannya mengenai kursi, meja, kasur, bahkan sampai ke dinding.

Teks ketiga diambil dari [8]. Teks ketiga ini membahas mengenai pembantaian warga di Kali Waci, Maluku Utara pada tahun 2019.

Setelah itu, Habel dkk menghujani Habibu dkk dengan anak panah. Banjir darah pun membasahi Kali Waci. Tanpa belas kasihan, Habel dkk menyerbu Habibu dkk dan membacok badan Habibu dkk dengan parang. Bahkan leher dan muka Habel dkk digorok.

Ketiga teks ini secara berturut-turut memiliki 254, 266, dan 238 karakter. Perhatikan bahwa batas banyak karakter yang dapat ditulis dalam sebuah *tweet* di Twitter adalah 280 karakter sehingga masing-masing dari ketiga teks ini dapat ditulis dalam satu *tweet*.

B. Metode Implementasi

Ketiga teks ini akan dienkripsi dengan algoritma-algoritma berikut:

1. ROT13
2. Cipher Substitusi Homofonik
3. Playfair Cipher
4. Vigenere Cipher dengan kunci berulang
5. Vigenere Cipher dengan kunci-auto

Teks yang sudah dienkripsi tersebut akan diunggah di Twitter dengan tetap memberikan info mengenai algoritma dan kunci (jika ada) yang dipakai. Info lain yang perlu diberikan adalah pranala situs web yang dapat mendekripsi *tweet* tersebut dikarenakan tidak semua pengguna memahami algoritma tersebut secara mendalam. Di sini, akan digunakan situs web dcode.fr, rumkin.com, dan boxentriq.com. Hasil unggahan *tweet* akan dianalasis pada bab berikutnya.

C. ROT13

Hanya ada satu versi ROT13 yang umum dipakai yakni yang menggeser setiap huruf sejauh 13 karakter. Hasil yang diperoleh adalah sebagai berikut:

1. Teks 1

   Zrenfn greqrfnx, Elna cretv xr qnche qna zratnzovy cvfnh qna zrahfhx Urev grcng qv hyh ungv. Urev nzoehx qna zrevagvu xrfnxvgna. Qnynz xbaqvfv gnx oreqnln, Elna zralrerg Urev xr xnzne znaqv. Ghohualn qvgryragnatxna, xrcnynaln qvunwne qratna gbatxng orfv.

2. Teks 2

   Chxhyna lnat qvynxhxna orexnyv-xnyv byru Evb vgh zratthanxna qhn znegvy, fngh qv gnatna xvev, fnghaln qv xnana. Qnynz ororencn chxhyna fnwn, xrcnyn Wrwr fhqnu erzhx. Qnenu qna vfv xrcnyn oreunzohena. Crepvxnaaln zratranv xhefv, zrwn, xnfhe, onuxna fnzcnv xr qvaqvat.

3. Teks 3

   Frgrynu vgh, Unory qxx zratuhwnav Unovoh qxx qratna nanx cnanu. Onawve qnenu cha zrzonfnuv Xnyv Jnpv. Gnacn orynf xnfvuna, Unory qxx zralreoh Unovoh qxx qna zrzonpbx onqna Unovoh qxx qratna cnenat. Onuxna yrure qna zhxn Unory qxx qvtbebx.

Contoh penggunaan ROT13 dalam menuliskan *tweet* mengenai teks 1 ditunjukkan pada gambar di bawah ini.

D. Cipher Substitusi Homofonik

Cipher substitusi homofonik ini menggunakan tabel di bawah ini. Dalam mengenkripsi plainteks, apabila terdapat lebih dari satu pilihan pasangan huruf hasil enkripsi maka akan dipilih satu secara acak. Tabel ini dibangun berdasarkan frekuensi kemunculan huruf di teks sampel Bahasa Indonesia di [9] dengan banyak pasangan huruf hasil enkripsi bersesuaian dengan persentase kemunculan huruf, dibulatkan ke bilangan asli terdekat.

A	RN, BO, DY, XM, JZ, BD, EO, GD, EC, GY, XY, EB, UX, UR, RS, KW, ND, SL, KE, NA
B	PT, DN, OG
C	HQ
D	LN, KR, KP, NT
E	XF, GA, FZ, ME, WF, BS, OH, FM
F	VG
G	SG, YY, EQ, CW
H	ZP, AG
I	TF, BN, CM, OK, OO, OI, IX, ZG
J	PQ
K	GT, AS, XV, FV, WX
L	VS, LT, GF, SY
M	VZ, BM, SE, BA, KX
N	JI, ZT, IR, HA, VY, OF, RI, RB, UJ, OZ
O	QR, BK
P	NN, FD, NY
Q	GQ
R	JM, GL, CG, MT, WU
S	CC, UZ, JD, IE
T	OM, JF, DT, LC, UE
U	GB, MG, WO, IP, VO, AE
V	NU
W	QF
X	JN
Y	PV, ST
Z	BC

Berikut adalah hasil enkripsinya:

1. Teks 1

   bmmejmebjdec dtfmjmlnohccjzas, mtpvecha fdfzmtyyoi xvme ntnanywomt lnkeoz bafmrieqecbmdnzglt nntfccndgb krslji vzfzujaeccmggt aggacgok jfohfdurjf krix voltip agdydtcm. zpwfcgzg kwbmdnjmipgt krgdji kxwfjmixrblcokzp fvfmccnaasbndteooz krrnvsjzbm fvbkjilnoouzok lcgywx ogfzmtkrjzpveo. wupvrsrb segavystbsjmfmue zpgajmix gtxf asbdbmrsgl segyrikrbn. omgbptipagristgd lnoolcxfvswfujjfebozsgfvrsji, gtxfnyxyvsuxvystgd krbnzpdypqxycg lnwfozsggdzt ueqrozyygtkejf ptbsietf

2. Teks 2

   nyvoasmgvsdyvy pvxyvyyy ntokltdyasgbxvjzji dngawuasxyltbnfvrngfzg qrvsohag jmoobk zglcwo bmxfricwsgipirdyasndha kpvona vzdyjmjftfvs uzsljfae ntix dturozyybdir xvbncgok ccuromipristxy lnzg wxnaofslvy kpbdlturbm dnmeptgajmecfdur nnvowxaeltdyof ieecpqnd wxxfnnecgfxy pqfzpqoh ccgbkpurag wuohkxwogt lnkwcgnaag lnnduj cmjdbn xvmenybdvskw ptmejmagslbaptwocggdha nyfmcghqzgasboozirpvxm vzwfrbcwxfozeboo gtvocgiecm bafmpqxy fvndjdgbwu ptecagasslha jdkwbanynaoo wxwf lnzgvyntzgjieq

3. Teks 3

   ccxflcxfgfbozp oojfae zprsptmesy kpgtas bmfzujcwzpwopqkeirzg zpbdptoodnae krxvfv lngahaeqjzir urztrnxv fdbdriebag dnbdofpqcmjm krxmglgdag nnmgha kxohseoggdieboagtf gtkevsoo qfxmhqtf lcbdztnybo dnxflturuz xvdyuzbnzpslri zpndptohgf kpgtgt kxxfvypvwfjmptwo agxyogcmptgb kpgtxv lnbouj kxwfbmogslhqbkxv ogjzkpxmri agnadnbndnvo ntxvfv lnohozeqgyuj nykemtkeirsg ogjzagfvecrb ltbszpbswu kpgdof vzwowxjz aggdptfmgf ntxvxv kpoisgbkglqrgt

Contoh penggunaan cipher substitusi homofonik pada penulisan *tweet* mengenai teks 1 ditunjukkan pada gambar di bawah ini.

E. Playfair Cipher

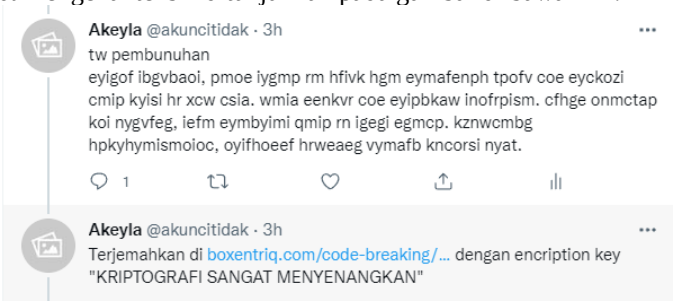
Di kasus ini, tabel yang akan digunakan adalah

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

Tabel ini juga dapat diperoleh dengan menggunakan kunci enkripsi ‘Kriptografi sangat menyenangkan’. Digunakan versi huruf ‘J’ digantikan dengan ‘I’ dan apabila ada dua huruf kembar berurutan atau banyak huruf ganjil, maka akan disisipkan huruf ‘X’ sebelum dienkripsi. Hasil yang diperoleh adalah sebagai berikut

1. Teks 1
   eyigof ibgvbaoi, pmoe iygmp rm hfivk hgm eymafenph tpofv coe eyckozi cmip kyisi hr xcw csia. wmia eenkvr coe eyipbkaw inofrpism. cfhge onmctap koi nygvfeg, iefm eymbyimi qmip rn igegi egmcp. kznwcmbg hpkyhymismoioc, oyifhoeef hrweaeg vymafb kncorsi nyat.
2. Teks 2
   kxokhfm boem vphoikooe nyirfhp-rfhk ahyd ika pkv nymfvoveoiom cwo egikph, ofkz hr ismooe rpip, ofkzmbg hp roeoe. hghfe nynmifif ikoxcoe ofae, inifhf ahah ozhgd iyeko. hgigl hoe tap ryifhs emiweenvkoe. iykdproembg eymameop rvkat, eyae, ioozt, mewiob ogeifp rm hkehrmo.
3. Teks 3
   abibhfw akz, wenyq hpur nymadwkoea wsetev cpur cymafe oeor toeew. esekpi hgigl ikc eyenfoewp rfha iohp. koeif nyhfo tfoawoe, wenyq hpur nymbytmw csetev cpur coe eyenohno eshge csetev cpur cymafy kgioes. mewioy chwmi hgm ekoe wseyh crr cragkno.

Contoh penggunaan Playfair cipher dalam menuliskan *tweet* mengenai teks 1 ditunjukkan pada gambar di bawah ini.



F. Vigenere Cipher dengan Kunci Berulang

Di kasus ini, akan digunakan kunci dengan sembilan karakter yakni ‘taksonomi’. Hasilnya yang diperoleh adalah sebagai berikut:

1. Teks 1
   Febsgn hqzwecsy, Emmv iebyw xs piiub voa aqvzawtwy duatu nsb zszcluu Zsew fmiad vw hzg ptts. Zsew muurec rnb ymkixlwu yqatksloa. Rmttm ugbqweq mau tsermgt, Risb zszgxrol Vrfu sx kkeoe amvwi. Dmphvzgt dslsyszbtnqcoa, yqxtlkfmn ruptjkj rrbsig tyfuxof jxss.
2. Teks 2
   Iuumznb kigg naznygstn lwfxoxq-dava cyst Zbo sli zszozuxsynb pct mkjhvz, eimu na hnbsig ksjw, fofcgyk vw xozig. Dkdoz pqjxrkho ciwceax kowo, wmiavs Xrxq andkz frags. Wabsv qoz qli uwdnzm jxrrsaoidig. Pojqvymvgyk esauqvti umffw, ymca, usghf, niakkf gnabib ko vwaruvz.
3. Teks 3
   Ledwznv ubn, Hktsy rws fexyvhxmvb Hktwoi psd dofunb mvtk zsbnv. Nigjsj rnfmp iux eszpmaths Coyw Iivi. Dsbco nmeac cofwtig, Hktsy rws fexqsepg Ptbsti qyw ltn wwaooowd bkvoa Vmjbbe vyx rqvzax hoeozo. Uarcoa zqpxr nsb ziwi Aalwz qyw lbgyjcx.

Contoh penggunaan Vigenere cipher dengan kunci berulang dalam menuliskan *tweet* mengenai teks 1 ditunjukkan pada gambar di bawah ini.

G. Vigenere Cipher dengan Kunci-auto

Di kasus ini, akan digunakan kunci dengan sembilan karakter yakni ‘taksonomi’. Hasilnya yang diperoleh adalah sebagai berikut:

1. Teks 1

   Febsgn hqzpijac, Rree sijgs bc dneyi jix qhnvudeiy bmfgu pbv xtvmson Hrdm gyhud km ltn lptb. Kmlt utbkcr hrv mqszhdlh xqwrsvmiu. Nedaw shnqlst tmu prulsgt, Ribr dhnweict Uqvv ii befhv dixhs. Tgbltnld lbnfflaraqodey, oriaygxyn nmwauae beqohn coejonz brlw.

2. Teks 2

   Iuumznb kica ncwaxsknt emckkfs-knmm fves Zso tbi xiuxoivtemr qag gnrdiy, vutg dz miyyag elzb, snzuaii uq cagua. Baoiw brbruaaa bvovprn hayu, uyaays Jnjo wjdlh aivyc. Xdrhy hmh svi bewdln jwzrebbfrbr. Glrojernane dgvqeang kgvfo, qrji, uujmz, neqkkn kudqap ue qanpxno.

3. Teks 3

   Ledwznv ubm, Ltfpl ksd glnhlfmkxu Lnhpvd dxs keoobh dxkn tntau. Bnntxr qaybh cdv dhmsazpbv Wexj Wscp. Bknai xenil knhiiey, Hsled lrk zlnzicee Rmfvzy ule kao ufgekmrk omhmo Hcpscu gkx keoobh skbdrt. Hauzae lrnfr kkn zfoh Lreey peu dpgpvzn.

Contoh penggunaan Vigenere cipher dengan kunci-auto dalam menuliskan *tweet* mengenai teks 1 ditunjukkan pada gambar di bawah ini.

IV. Analisis dan Kesimpulan

Dalam melakukan analisis, perlu disepakati terlebih dahulu mengenai kriteria algoritma kriptografi yang baik untuk penyembunyian konten eksplisit tersebut. Kriteria yang akan diperhatikan dalam makalah ini adalah:

1. Pembaca tidak dapat mendekripsi cipherteks secara manual dalam waktu yang singkat
2. Informasi yang perlu dimasukkan ke dalam aplikasi pendekripsi konten tidak banyak
3. Pembaca yang telah melihat banyak cipherteks dan plainteks yang bersesuaian tidak dengan mudah dapat mengenali kata-kata di cipherteks yang baru

Kriteria 1 adalah kriteria yang paling penting. Contoh transformasi teks yang tidak memenuhi kriteria 1 adalah penyisipan karakter tertentu seperti “dia telah gantung diri” menjadi “dnina tnelnanh gnannntnunnng dninrni”. Pembaca yang sekilas melihat kalimat tersebut akan menyadari bahwa kalimat tersebut tidak normal dan polanya dapat langsung dipahami.

Kriteria 2 juga perlu diperhatikan terutama dalam teks yang sangat panjang. Meskipun sudah ada situs web yang dapat membantu pengguna mendekripsikan konten, akan sangat melelahkan bagi pengguna untuk memasukkan lebih dari 10 informasi agar dapat mendekripsi konten tersebut. Perlu diperhatikan bahwa setidaknya terdapat satu informasi yang selalu dimasukkan yakni konten yang terenkripsi itu sendiri. Pengguna tidak perlu menulis ulang konten tersebut karena dapat digunakan fitur salin-tempel.

Kriteria 3 adalah kriteria yang perlu dipertimbangkan. Apabila seorang pengguna telah melihat beberapa konten dalam bentuk terenkripsi dan terdekripsi dan ia sudah mengamati bahwa frasa sering berarti “nujilon yoyo” berarti “menikam dada” maka saat ia melihat frasa tersebut pada konten terenkripsi yang baru, ia dapat tahu secara sekilas bahwa konten tersebut memuat frasa “menikam dada” tersebut.

Sekarang, kelima algoritma tersebut akan dianalisis secara kualitatif berdasarkan kriteria yang sudah diberikan.

A. ROT13

Saat pertama kali melihat hasil enkripsi konten, pengguna awam mungkin tidak akan mengenali isi konten asli. Akan tetapi, inspeksi lebih mendalam, terutama untuk konten yang panjang, akan membuat pengguna mendapati frasa-frasa yang muncul berulang kali. Ambil contoh string ‘qna’ di ketiga konten dan ‘xr’ serta ‘qv’ yang ada di konten 1 dan 2. Pengguna yang teliti akan dapat menebak bahwa kata-kata dua dan tiga huruf yang sering ditemui dalam Bahasa Indonesia adalah ‘dan’, ‘ke’, dan ‘di’. Sehingga tebakan singkat akan dapat membuat pengguna mendapat terjemahan dari karakter ‘q’, ‘n’, ‘a’, ‘x’, ‘r’, dan ‘v’. Jadi, disimpulkan bahwa kriteria 1 belum dapat terpenuhi dengan baik tetapi tidak dapat ditebak secara trivial juga.

Lebih lanjut, kriteria 3 tidak dapat terpenuhi dengan baik karena ROT13 hanya memiliki satu versi saja. Artinya, pengguna dapat (secara tidak sengaja dan karena terbiasa) mengingat kata-kata tertentu. Sebagai contoh, ‘qnenu’ bisa diingat sebagai ‘darah’. Enkripsi yang sama untuk tiap karakter juga memperburuk hal ini. Jadi, dapat disimpulkan bahwa ROT13 bersifat buruk dalam kriteria 3.

Hal yang positif dari ROT13 adalah kesederhanaannya. Dikarenakan hanya ada satu versi ROT13, informasi yang diperlukan oleh pengguna hanyalah konten terenkripsi itu sendiri. Tidak perlu ada kunci yang perlu dimasukkan.

B. Cipher Substitusi Homofonik

Cipher substitusi homofonik memenuhi kriteria 1 dengan baik karena konten yang telah terenkripsi memiliki kata-kata yang dua kali lebih panjang dari konten asli. Terlebih lagi, pemilihan pasangan huruf yang baik akan membuat tidak terlihat adanya pola yang mencuat dari deretan huruf tersebut.

Kriteria 3 juga dapat dipenuhi dengan baik dikarenakan sifat homofonik yang alamiah dari algoritma ini. Satu kata yang sama dapat dienkripsikan menjadi string-string yang berbeda. Penghafalan kata-kata tertentu juga tidak berarti karena terdapat banyak terjemahan yang berbeda yang perlu dihafalkan.

Kelemahan muncul di kriteria 2. Banyak informasi yang perlu dimasukkan sangatlah banyak. Setidaknya diperlukan konten terenkripsi dan 26 pasangan huruf hasil enkripsi setiap huruf. Selain itu, memasukkan manual pasangan-pasangan huruf ke aplikasi pendekripsi akan membuat pengguna secara tidak sadar menghafalkan pasangan huruf dan hasil enkripsinya. Sehingga, kriteria 2 ini sangat tidak dapat dipenuhi oleh cipher substituti homofonik.

C. Playfair Cipher

Playair cipher dapat memenuhi kriteria 1 dengan cukup baik dikarenakan sifatnya yang mengenkripsi pasangan huruf alih-alih mengenkripsi huruf. Satu kata yang sama dapat dienkripsikan secara berbeda tergantung dari letaknya di paragraf dan huruf yang berada di depan atau belakangnya. Meskipun begitu, beberapa frasa tertentu dapat dienkripsi ke string yang sama apabila jarak keduanya genap.

Playfair cipher juga dapat memenuhi kriteria 3 dengan baik dikarenakan terdapat 25! kemungkinan kunci berbeda

yang dapat digunakan untuk konten yang berbeda. Sehingga, kecil kemungkinan pengguna menemukan kunci yang sama dan akan memberikan enkripsi yang sama atas kata yang sama.

Terakhir, kriteria 2 dapat terpenuhi meskipun masih kurang. Pengguna dapat memasukkan kunci dalam bentuk tabel 5 x 5 atau dalam bentuk kalimat yang dapat membangkitkan tabel tersebut. Beberapa situs web dapat mendukung bentuk kedua sehingga lebih memudahkan pengguna memasukkan kunci.

Masalah utama dari Playfair cipher justru muncul dari selain tiga kriteria tersebut. Masalah tersebut adalah ketidakmampuannya mengenkripsi seluruh isi konten dan mendekripsikannnya kembali secara sempurna. Pertama, hanya ada 25 huruf yang dapat dibangkitkan dari pendikripsian konten sehingga pasti ada huruf yang hilang. Kedua, huruf kembar berurutan ditampilkan dengan huruf tertentu tersisip di antara keduanya. Hal ini tidak masalah dalam kata umum tetapi akan menjadi masalah dalam singkatan-singkatan atau nama tempat, orang, atau organisasi.

D. Vigenere Cipher dengan kunci berulang

Kriteria pertama dapat terpenuhi dengan baik karena satu kata yang sama belum tentu dienkripsi sebagai kata yang sama pula. Meskipun vigenere cipher tipe ini dapat dipecahkan dengan menggunakan metode Kasiski, pengguna yang melihat sekilas konten terenkripsi seharusnya tidak punya waktu yang cukup untuk memecahkannya.

Kriteria kedua juga dapat terpenuhi dengan baik karena hanya perlu memasukkan konten yang terenkripsi dan kata kuncinya yang seharusnya jauh lebih pendek dari panjang konten.

Kriteria ketiga juga dapat terpenuhi dengan baik dikarenakan terdapat banyak versi kunci yang ada. Sehingga, penggunaan kunci yang berbeda pada konten yang berbeda dapat memperkecil kemungkinan pengguna menemukan terjemahan kata terenkripsi yang sama dan akibatnya mengurangi kemungkinan pengguna mengenali kata-kata di konten terenkripsi yang baru.

E. Vigenere Cipher dengan kunci-auto

Analisis di algoritma ini hampir sama dengan analisis di algoritma sebelumnya. Sedikit perbedaan terletak di metode Kasiski. Algoritma Vigenere cipher dengan kunci auto dapat membuat metode Kasiski lebih sulit dikarenakan kunci yang dipakai adalah potongan dari plainteks itu sendiri.

Kepantasan setiap algoritma yang dibahas diringkas dalam tabel di bawah ini.

	Kriteria 1	Kriteria 2	Kriteria 3
ROT13	Medium	Bagus	Buruk
Substitusi Homofonik	Bagus	Buruk	Bagus
Playfair	Bagus	Bagus	Bagus
Vigenere kunci berulang	Bagus	Bagus	Bagus
Vigenere kunci-auto	Bagus	Bagus	Bagus

Sehingga, dapat disimpulkan bahwa algoritma yang sesuai untuk dipakai dalam menyembunyikan konten eksplisit di forum publik adalah Playfair cipher dan Vigenere Cipher (dengan kunci berulang atau kunci-auto).

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen penulis, Dr. Ir. Rinaldi Munir, MT., karena telah membantu penulis dalam memahami materi kriptografi. Penulis juga mengucapkan terima kasih kepada orang tua penulis karena sudah mendukung penulis untuk menuliskan makalah ini. Penulis juga berterima kasih kepada semua orang lain karena sudah membuat penulis bisa berada di momen ini baik secara langsung maupun sangat tidak langsung.

REFERENSI

[1] Ortiz, R.R. and Thompson, B. (2017). Content Effects: Pornography and Sexually Explicit Content. In The International Encyclopedia of Media Effects (eds P. Rössler, C.A. Hoffner and L. Zoonen). https://doi.org/10.1002/9781118783764.wbieme0122

[2] Brown, J. D., & L'Engle, K. L. (2009). X-rated: Sexual attitudes and behaviors associated with US early adolescents' exposure to sexually explicit media. Communication Research, 36(1), 129–151. doi: 10.1177/0093650208326465

[3] Huesmann L. R. (2007). The impact of electronic media violence: scientific theory and research. The Journal of adolescent health : official publication of the Society for Adolescent Medicine, 41(6 Suppl 1), S6–S13. https://doi.org/10.1016/j.jadohealth.2007.09.005

[4] Madan, A., Mrug, S., & Wright, R. A. (2013). The Effects of Media Violence on Anxiety in Late Adolescence. Journal of Youth and Adolescence, 43(1), 116–126. doi:10.1007/s10964-013-0017-3

[5] Schneier, B. (1963). Applied Cryptography : Protocols, Algorithms, and Source Code in C. New York :Wiley, 1996.

[6] Irfani, F. (2018). Motif pembunuhan sadis Ryan Jombang & skandal salah tangkap polisi. https://tirto.id/c8pf diakses pada 20 Desember 2021

[7] Asyhad, M.H. (2017). [Cerita kriminal] Kisah Rio Martil, senjatanya dua martil. https://intisari.grid.id/read/0390970/cerita-kriminal-kisah-rio-martil-senjatanya-dua-martil?page=all diakses pada 20 Desember 2021

[8] Saputra, A. (2020). Bantai warga di Kali Waci Maluku Utara, 2 pelaku dihukum mati. https://news.detik.com/berita/d-5009968/bantai-warga-di-kali-waci-maluku-utara-2-pelaku-dihukum-mati diakses pada 20 Desember 2021

[9] Andana, G. (2009). Analisis frekuensi pada teks Bahasa Indonesia dan modifikasi algoritma kriptografi klasik. Program Studi Teknik Informatika, Institut Teknologi Bandung.

[10] Munir, R. (2021). Kriptografi klasik (bagian 1). https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Klasik-Bagian1.pdf diakses pada 20 Desember 2021

[11] Munir, R. (2021). Kriptografi klasik (bagian 2). https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Klasik-Bagian2.pdf diakses pada 20 Desember 2021

[12] Munir, R. (2021). Kriptografi modern (bagian 1). https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Kripto-modern-2021.pdf diakses pada 20 Desember 2021

[13] dcode.fr diakses pada 20 Desember 2021

[14] http://rumkin.com/tools/cipher/vigenere-autokey.php diakses pada 20 Desember 2021

[15] https://www.boxentriq.com/code-breaking/playfair-cipher diakses pada 20 Dsemeber 2021

Medan, 20 Desember 2021

Akeyla Pradia Naufal 13519178

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.