Perbandingan Keamanan *Playfair Cipher* dan *Four-Square Cipher*

Tadya Rahanady H - 13509070
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
tadtedtod@gmail.com

Abstrak—Playfair cipher* adalah salah satu metode enkripsi dari *polygram cipher.* Penggunaan metode ini terbukti lebih sulit dipecahkan daripada penggunaan *substitution cipher* sederhana. Jika kita menggunakan analisis frekuensi pada digram, akan terdapat lebih kurang 600 buah digram yang muncul bergantung pada kunci yang digunakan. Meskipun demikian, kita dapat menggunakan satu trik untuk mempermudah pencarian kunci. Digram dan digram yang berlawanan akan menghasilkan pola huruf yang sama pada *plainteks.* Dalam bahasa inggris, terdapat banyak sekali kata-kata yang memuat digram yang berkebalikan seperti *ReceivER* dan *DepartED.

***Four-Square cipher* adalah metode enkripsi yang mirip dengan *Playfair cipher*, tetapi lebih kuat karena analisis frekuensi menjadi jauh lebih sulit. Dibandingkan dengan *Playfair cipher,* metode ini tidak akan memunculkan *cipherteks* dengan bigram berkebalikan. Hal tersebut hanya berlaku jika dua kunci yang digunakan berbeda. Perbedaan lainnya adalah adanya kemunculan huruf ganda di dalam metode ini. Meskipun lebih kuat daripada metode *Playfair cipher,* metode ini lebih rumit karena penggunaan dua buah kunci dan menyiapkan lembar enkripsi/dekripsi dapat membuang banyak waktu.**

Kedua metode diatas memiliki kesamaan, yaitu dapat dengan mudah dipecahkan dengan jumlah *cipherteks* yang mencukupi

Kata Kunci— kriptografi, cipher, Playfair cipher, Four-Square cipher, enkripsi, dekripsi.

I. Pendahuluan

Kata *cryptography* berasal dari bahasa Yunani yang artinya *secret writing.* Kriptografi adalah suatu praktek dan ilmu dari teknik untuk komunikasi yang aman dimana adanya kehadiran dari pihak ketiga. Secara lebih umum, ilmu ini berisi tentang bagaimana membangun dan menganalisis protokol yang menanggulangi keterlibatan dari orang ketiga yang berhubungan dengan berbagai aspek dalam keamanan informasi, seperti kerahasiaan, keutuhan data, dan keotentikan. Kriptografi modern merupakan gabungan dari disiplin ilmu matematika, sains komputer, dan elektroteknik. Definisi baru yang diajukan oleh Schneier yaitu "Kriptografi adalah seni dan ilmu untuk menjaga agar suatu pesan tetap aman".

Pada awalnya, kriptografi hanya mempertimbangkan faktor kerahasiaan dari informasi untuk mencegah pesan agar tidak dapat dibaca oleh pihak lain yang tidak memiliki pengetahuan tentang kunci untuk mendekripsi pesan tersebut. Dalam beberapa dekade terakhir, faktor yang dipertimbangkan menjadi lebih luas dan menambahkan faktor keutuhan pesan, keotentikan pesan, *digital signatures,* bukti interaktif, dan perhitungan komputatif.

Bentuk paling awal dari kriptografi memerlukan tidak lebih dari alat untuk menulis dan juga kertas, karena kebanyakan orang masih belum dapat membaca. Cipher klasik yang paling umum digunakan adalah *transposition ciphers,* yang mengubah urutan huruf-huruf yang ada di dalam pesan, dan *substitution ciphers,* yang secara sistematis mengganti huruf ataupun kumpulan huruf dengan huruf atau kumpulan huruf lainnya. *Substitution cipher* paling awal adalah *Caesar cipher*, dimana setiap huruf yang ada digeser dan menggantikan huruf lainnya. Beberapa contoh algoritma kriptografi klasik lainnya adalah *Playfair cipher, Four-square cipher, ROT13, Vigenere,* dan lain sebagainya.

Dengan perkembangan komputer digital dan elektronik membantu dalam kriptanalisis, memungkinkan untuk dibuatnya *cipher* yang lebih kompleks. Terlebih lagi, komputer memungkinkan enkripsi data jenis apapun yang direpresentasikan dalam format biner. Penggunaan komputer telah menggantikan kriptografi linguistik, baik untuk pembuatan desain *cipher* dan kriptanalisis. Banyak *cipher* yang dapat dikarakteristikkan berdasarkan operasinya dalam urutan bit biner (terkadang dalam grup atau blok), yang secara umum memanipulasi karakter huruf dan digit secara langsung. Selain daripada itu, komputer juga membantu dalam proses kriptanalisis.

Meskipun demikian, perkembangan *cipher* modern yang baik jauh meninggalkan perkembangan kriptanalisis, biasanya terjadi dikarenakan penggunaan *cipher* yang berkualitas sangat efisien, sementara memecahkannya memerlukan usaha yang besar, dan biasanya jauh lebih besar dari usaha yang dibutuhkan untuk pemecahan *cipher* klasik, membuat kriptanalisis sangat tidak efisien dan tidak dapat dipraktekkan secara efektif.

II. Playfair Cipher

A. Enkripsi dan Dekripsi

Playfair cipher adalah salah satu metode enkripsi dari *polygram cipher*. *Playfair cipher* atau *Playfair Square* adalah teknik enkripsi simetri manual dan merupakan *cipher* substitusi digraf pertama. Skema ini ditemukan oleh Charles Wheatstone pada tahun 1854, tetapi menggunakan nama Lord Playfair, yang mempromosikan penggunaan *cipher* ini. *Cipher* ini mengenkripsi pasangan huruf (digram atau digraf), bukan huruf tunggal seperti pada *cipher* klasik lainnya dengan tujuan untuk membuat analisis frekuensi menjadi sangat sulit yang disebabkan frekuensi kemunculan huruf-huruf di dalam cipherteks menjadi datar (*flat*). Penggunaan metode ini terbukti lebih sulit dipecahkan daripada penggunaan *substitution cipher* sederhana. Jika kita menggunakan analisis frekuensi pada digram, akan terdapat lebih kurang 600 buah digram yang muncul bergantung pada kunci yang digunakan.

Playfair cipher menggunakan tabel bijursangkar 5x5 yang memuat suatu kunci. Untuk membuat tabel kunci, pertama kita harus mengisi kotak di dalam tabel dengan kata atau kunci dengan membuang huruf yang berulang. Setelah itu, masukkan huruf alfabet yang tersisa ke dalam kotak yang tersisa secara berurutan (biasanya menghilangkan huruf Q untuk mengurangi alfabet sehingga cukup ke dalam tabel, sementara versi lain menghilangkan huruf J dari tabel).

Untuk mengenkripsi pesan, hal yang pertama dilakukan adalah memecah pesan menjadi digraf. Jika jumlah huruf adalah ganjil, maka tambahkan Z untuk melengkapi digraf. Setiap pasangan digraf merupakan pasangan sudut yang berlawanan dalam persegi yang ada di dalam tabel. Terdapat 4 aturan untuk mendekripsi setiap digraf, yaitu :

1. Jika kedua huruf sama, masukkan huruf X setelah huruf pertama. Beberapa varian *Playfair* menggunakan huruf Q, tetapi huruf lain yang jarang muncul dapat pula digunakan.
2. Jika huruf berada pada baris yang sama, ganti huruf tersebut dengan huruf yang berada tepat di kanannya.
3. Jika huruf berada pada kolom yang sama, ganti huruf tersebut dengan huruf yang berada tepat di bawahnya.
4. Jika huruf tidak berada pada baris dan kolom yang sama, ganti huruf tersebut dengan huruf yang berada pada baris yang sama dengan huruf pertama dan berada pada sudut dari persegi pasangan huruf.

Contoh kunci:

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

Gambar 1. Contoh tabel Playfair

Contoh Plainteks :
GOOD BROOMS SWEEP CLEAN

Karena tidak ada huruf J, maka digraf yang dihasilkan :

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Contohkunci:

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

Gambar 2. Contoh Enkripsi

Cipherteks :

FP UT EC UW PO DV TV BV CM BG CS DY

B. Kriptanalisis pada Playfair cipher

Jumlah kunci yang dapat dihasilkan dengan menggunakan tabel tersebut adalah 25! atau 15.511.210.043.330.985.984.000.000. Karena ada 26 huruf abjad, maka terdapat 26 x 26 = 677 bigraf, sehingga identifikasi bigraf secara individual lebih sukar. Sayangnya ukuran poligram di dalam *Playfair cipher* tidak cukup besar, hanya dua huruf sehingga *Playfair cipher* tidak aman. Meskipun *Playfair cipher* sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia dapat dipecahkan dengan analisis frekuensi pasangan huruf. Dalam Bahasa Inggris kita bisa mempunyai frekuensi kemunculan pasangan huruf, misalnya pasangan huruf TH dan HE paling sering muncul. Selain itu, sama seperti *cipher* klasik lainnya, metode ini dapat dipecahkan dengan mudah dengan adanya jumlah teks yang mencukupi. Jika hanya *cipherteks* saja yang diketahui, maka cara *brute force* dapat digunakan.

Pendekatan berbeda yang digunakan untuk memecahkan *cipher* ini adalah dengan metode *shotgun hill climbing*. Dimulai dengan tabel huruf yang acak, lalu mengubah sedikit tabel untuk melihat apakah kandidat *plainteks* terlihat seperti sebuah *plainteks* yang berarti dibandingkan sebelumnya. Jika tabel yang baru merupakan sebuah perkembangan, maka tabel tersebut akan dikembangkan lagi untuk diubah menjadi kandidat yang lebih baik. Secara bertahap, *plainteks* ataupun teks yang sangat mendekati akan ditemukan untuk mencapai nilai yang maksimum dengan apapun metode yang digunakan. Hal ini jelas diluar dari kinerja dan kesabaran dari manusia, tetapi komputer dapat menggunakan algoritma ini dengan jumlah teks yang relatif sedikit.

Aspek lain dari *Playfair* yang membedakannya dari *cipher* lain adalah fakta bahwa *cipher* ini tidak pernah mengandung digraf dengan huruf yang berulang. Jika

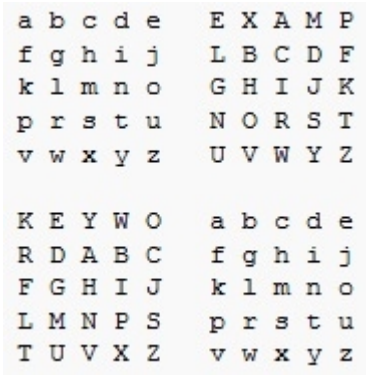
tidak ada huruf yang berulang dalam sebuah *cipherteks* dan pesan cukup panjang untuk membuat hal tersebut signifikan secara statistik, maka dapat dipastikan metode enkripsi yang digunakan adalah *Playfair.*

III. Four-square Cipher

A. Enkripsi dan Dekripsi

Four-square cipher adalah teknik enkripsi simetri manual yang ditemukan oleh kriptografer Prancis terkenal yang bernama Felix Delastelle. Teknik ini mengenkripsi pasangan huruf (digraf), dan karena itu dikategorikan sebagai *polygraphic substitution cipher.* Teknik ini menambahkan kekuatan pada enkripsi jika dibandingkan dengan *monographic substitution cipher* yang beroperasi pada karakter tunggal.

Four-square cipher menggunakan empat buah 5x5 tabel yang digunakan pada *Playfair*. Cara penggunaannya mirip dengan *Playfair,* tetapi dengan algoritma yang sedikit berbeda.



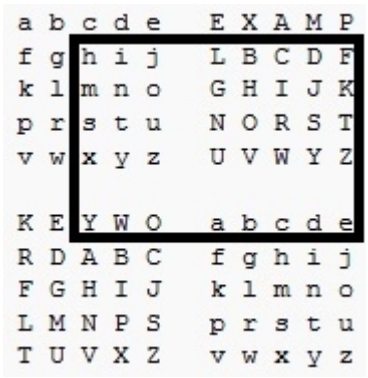
Gambar 3. Contoh tabel Four-square cipher

Contoh plainteks :

HELP ME OBI WAN KENOBI

Bagi pesan yang ada menjadi bigraf.

HE LP ME OB IW AN KE NO BI



Gambar 4. Proses enkripsi Four-square cipher

Cipherteks :

FY GM KY HO BX MF KK KI MD

Seperti yang dapat dilihat, metode enkripsi *cipher* ini hanya menemukan huruf-huruf yang berada pada sudut dari persgi yang terbentuk di dalam tabel, seperti pada *Playfair cipher.* Dekripsi bekerja dengan cara yang sama, tetapi secara terbalik.

B. Kriptanalisis pada Four-square cipher

Sama seperti *cipher* pra-modern lainnya, *Four-square* cipher dapat dipecahkan dengan mudah dengan jumlah teks yang mencukupi. Mendapatkan kunci pun akan cukup mudah jika plainteks dan cipherteks diketahui. Jika hanya cipherteks yang diketahui, maka penggunaan *brute force* untuk pencarian plainteks. Kriptanalisis dari *Four-square cipher* secara umum melibatkan pola pencocokkan monograf yang berulang. Kasus ini hanya berlaku saat kedua tabel plainteks (tabel di kiri atas dan kanan bawah) diketahui. *Four-square cipher* biasanya menggunakan urutan alfabet standar dalam tabel, tetapi itu bukanlah suatu keharusan. Dalam kasus tabel plainteks standar, maka kata tertentu akan selalu menghaasilkan pengulangan huruf tunggal. Sebagai contoh, kata MI LI TA RY akan selalu menghasilkan huruf cipherteks yang sama pada posisi pertama dan ketiga apapun kunci yang digunakan. Pola seperti itu dapat dikatalogkan dan dicocokkan dengan pengulangan huruf tunggal dalam cipherteks. Kandidat plainteks lalu dapat dimasukkan dalam usaha untuk mendapatkan tabel *Four-square.*

Tidak seperti *Playfair cipher,* metode ini tidak akan menunjukkan digraf yang berkebalikkan dari plainteks pada cipherteks. Akan tetapi, hal ini hanya berlaku jika kedua kunci yang digunakan berbeda. Perbedaan lain antara *Four-square cipher* dengan *Playfair cipher* yang membuatnya lebih kuat adalah fakta bahwa digraf dengan huruf yang berulang dapat terjadi pada *Four-square cipher.* Dilihat dari berbagai aspek, sistem enkripsi dari *Four-square* lebih kuat jika dibandingkan dengan *Playfair.* Akan tetapi, metode ini jauh lebih rumit karena menggunakan dua buah kunci, dan dalam menyiapkan enkripsi/dekripsi dapat memakan banyak waktu. Mengingat kekuatan enkripsi yang diberikan oleh *Four-square* dibandingkan dengan *Playfair* tidak terlalu besar dan karena keduanya dapat dengan mudah dipecahkan dengan adanya cipherteks yang mencukupi, metoda *Playfair* menjadi lebih umum untuk digunakan.

IV. Perbandingan Keamanan Kedua Algoritma

Untuk membandingkan tingkat keamanan dari kedua algoritma tersebut dengan menggunakan plainteks yang sama dapat kita lihat sebagai berikut :

A. *Plainteks*

Atlantis (in Greek, Ἀτλαντὶς νῆσος, "island of Atlas") is a legendary island first mentioned in Plato's dialogues Timaeus and Critias, written about 360 BC. According to Plato, Atlantis was a naval power lying "in front of the Pillars of Hercules" that conquered many parts of Western Europe and Africa 9,000 years before the time of Solon, or approximately 9600 BC. After a failed attempt to invade Athens, Atlantis sank into the ocean "in a single day and night of misfortune".

Scholars dispute whether and how much Plato's story or account was inspired by older traditions. In Critias, Plato claims that his accounts of ancient Athens and Atlantis stem from a visit to Egypt by the legendary Athenian lawgiver Solon in the 6th century BC. In Egypt, Solon met a priest of Sais, who translated the history of ancient Athens and Atlantis, recorded on papyri in Egyptian hieroglyphs, into Greek. Some scholars argue Plato drew upon memories of past events such as the Thera eruption or the Trojan War, while others insist that he took inspiration from contemporary events like the destruction of Helike in 373 BC[1] or the failed Athenian invasion of Sicily in 415–413 BC.

The possible existence of a genuine Atlantis was discussed throughout classical antiquity, but it was usually rejected and occasionally parodied by later authors. Alan Cameron states: "It is only in modern times that people have taken the Atlantis story seriously; no one did so in antiquity".[2] The Timaeus remained known in a Latin rendition by Calcidius through the Middle Ages, and the allegorical aspect of Atlantis was taken up by Humanists in utopian works of several Renaissance writers, like Francis Bacon's New Atlantis. Atlantis inspires today's literature, from science fiction to comic books to films. Its name has become a byword for any and all supposed advanced prehistoric lost civilizations

B. Cipherteks dengan Playfair

Kunci CRYPTOGRAPHY

Bynosykq (fq Egnnd, Ἀτλαντὶς νῆσος, "klmfwl dn Fcsbn") kq o nmefmfoyp kqnolf iktmr sfmpkalfe fq Cqbyb'l ekongavdz Beqgfzl fwl Opepkbn, vykprkw fogzc 360 OT. Oyodcefqb rh Cnocb, Bynosykq yfn b wfwgq caumg ncfqh "ew ncgsy ad pbi Rdqnotm ad Giyrcukm" pbby odqsvdgme lfwp tgybz ad Vfzbmgm Fvchcf glf Fnpeyo 9,000 rfgyz kfigck rgi pkvm ad Lbudl, ay gbbcgpqngrknc 9600 OT. Fnrky g nfdqfe byrkqro oh dmwoff Gpbfmn, Bcsfwpku ufwd ksyb cgi dofgq "fw f qkmamd foa flf qfabc be nkqdaycwlk". Mpodugyl kkqcxrk xakrgiy glf bgv ncoi Hnocb'u ucbyp gc oyodwly zbn fqqtepfe at duefy cygekpkalq. Kl Ypepkbn, Cqbyd onoeqz bbhp bkq oyodwlbz ad fwpdfmy Bpbfmn blf Bynosykq zbmv eygl g wkqkp cb Meptb kp cgi mdemlfgya Fpbfmfhq mfyhermt Mdual fq pbk 6ro pfmczyp OT. Fq Meptb, Zdual vmy b tykfzb ad Nbkq, xab cygqlnorkk cgi iqzbgcc an flykfsy Bygiql fwf Ocsfwpkm, tdrgcefl dq yhypys sm Fartcfhq akfcgomptbq, fqcb Egnns. Zglk mpodugyn bgevd Cqbyd lgmx vchq nmvgckfl bi ybnr krmsyu ucob hz bgi Pbmgg fcvtcdhl ay cgi Cyhdfw Yfy, viqmd bcgitm fqqkzb pbby gi cbbd fqqtepbydhw ncgl ralrkqrgcgyr frmsyl mkdk rgi efzbcvrcdhl ai Admkdf ks 373 AO[1] dy cgi nfdqfe Bygiqffw fqwgqkal ad Qkpdnc fq 415–413 OT. Pbi rblqkosn npqzbfmrd ad h afmxdmf Bynosykq yfl kkqocuufe pbcgvobgzc oubnqkyon osyqxxdcp, ozp ky zbn zlwovvp yfkdrrkf olf doyoqkalonnc yhcgekfe at norky gzcbgtm. Onfw Yovmcgq lybrkq: "Kp kl bqmp fq ndlmgs yeqkm pbby rihcmd bhrm ybdfs ygi Bynosykq zbgct nmgdhzlnc; la alf eke lb fq fwpklxkpp".[2] Cgi Pkngdvm tmvhfmfe dlayw fq o Nbyfq gmlfkpdhs ap Ronpdekzl pbcgvob pgi Qemmmd Hakm, fwk cgi onmdagpeyon oqtdrc bn Fcsfwpkn zbn ybdfl wt hp Avlfwkqbz fq zchcfhw ygcsz ad mkrmygm Cfmhfuufwrd vykpmgl, mkdf Iyglykq Ohodq'l Mfy Fcsfwpkn. Bcsfwpkq kqlhqgmz bdlfa'l mkpmgbyvcf, icgn lpdfmrd ikrcdhs yd ogldp ogbdz ba ddqnl. Kpl qgni gbn gkodvm h oaygce igc fwa flf onm lxcchmkf oeufwrdi cgmiqzbgcdp udzb pdxeqdwbpkalqZ

C. Cipherteks dengan Four-square

Kunci CRYPTOGRAPHY dan KEYWORD

PLDEIPAPHIGMTOAPDEIWDCPLDEKYJEBEIW
RLXBLHPFCBGPNNJYIPBIJWPBDPDESINYOWJG
BMYSNBDYTSKYIWRNHPOWLVNDNPPJRKJSYE
YKTHNEHIHMDSDESIPLDEIPAPUEKYDWUKDM
EZRSIUHIDBSGIPDCMBCSGIDEMMDCBYMELJY
SMBPLTHSOSEYIPFUPRLMPDCZENNRSJWLSDS
COIWCRNDCYZWRLLYCCESPSBYNBJYDCSHJGJ
IKEKLSGXADYSWIUYECRSWKEOKGIPOPLSWD
NNPICDXPKCOMBPJKYLIPFNBMNPFIRIPISBYFO
CODWNAEBJECWUWIWIBADSIAFAPBFNMNJYA
EJRLNYAPSLSWWDPSBYKEIWBHWGMOONDESI
MNSINUESYKTHNJLXYLHIKNGPPOPUEJTWNM
KEPBNBIJNAFWNDNBYLLFPLFODEAINNOYMB
APYKTHNJMPDCPFPAPJKWMBPJKYIWPLDEIPA
PNNYJGLFJCTAPHPSIRCUPLWXPBYJEBEIWRLU
WMBPJOWEIRTHDZKMMEJIJHIMBMBTYIPLSV
WPAJWHUNLSHJGFIPSCLNDYSSIALPRLVBHLPP
FLHPLPOMBYCAPSINUDCPFPAPJKWMBPJKYIW
PLDEIPAPSETHNEPOIJKKNTNDHIRCUPNBPFHA
RSECIUMRNAIPECSECJSHJYMYBHDEMMRLBM
CSDESIRPRZKSIJJYJHNDYSDCKKNNCZPJMPSNY
AYLMBPSBYKERSKSNBIJESMBPSSGOOEXRLWD
GITJMBRSNAFPAPNPOYMBPSJJIRFPNRKENBIJG
LFJTHIPYJSFKENUCZPJMPIDJKMBPOYSLPMON
BIJDCBYIDJKHIESMBCCPRJECWMBPJOWIBDXY
LBIJIALAWGIXBYEMBCSFSNARGTOXANNPJTY
DCRRPJNCJWPLDEIPAPUENYAPTNMNPOMBSGL
CBHNSRHYLNACYDEIPNCNXTMNBLXYLMSKO
EGVPTCYOSWCWIWFOCYNAIJRFIUKKSGPBPOP

UDESWKENSBHMMRFPFCYJYSGFPKWSWHPAPI
JIUHIJHTWNGNBJYNNOYKPTJLFYCCTPSCFPJM
BCOLIPFNBMNSINUSYNDJSLHJIIJPOHWSHHIPF
NBHPMBPSAITKMSSEDYHIPOIFEZIBDWDENBEP
PJPBNBIJPUCYFEHWBPNNGNJSADMBYJHWRIC
OBEKYIWMBCOEGRCESAWRFYLSKPNDCPLDEI
PAPUENNCFPJKSPUBNDYIBNNNAJPSINRPFZGK
GSHALCZRSRFSEDWAPKYFWRZNDSWMMIDJK
GLPFPALYYKIJNHRZPLDEIPAPPLDEIPAPHIKNG
PYSSICWIDSWKESPSEGLFJMYBWFWCCAWNBIJ
SITHIARYJJFLSIHRFGNAMPDWJYOYLYYOFJCO
PUZGNEBFKEIXPFCWEGSNKLFSPOPKUKFWPOL
LYCAPSINDRHFSMWOXGIBXPLBIFP

D. Kriptanalisis pada Playfair Cipher

Playfair cipher dapat dipecahkan dengan analisis frekuensi pasangan huruf, karena terdapat tabel frekuensi kemunculan pasangan huruf dalam Bahasa Inggris.

Langkah awal yang digunakan adalah penghitungan frekuensi huruf tunggal dan juga digraf. Alasan untuk menghitung frekuensi kemunculan huruf tunggal adalah karena huruf pada cipherteks dengan frekuensi kemunculan yang tinggi merepresentasikan huruf pada plainteks dengan frekuensi kemunculan yang sama.

Frekuensi kemunculan huruf tunggal :

A = 48
B = 102
C = 85
D = 84
E = 42
F = 124
G = 90
H = 33
I = 35
J = 0
K = 94
L = 68
M = 78
N = 68
O = 71
P = 69
Q = 84
R = 42
S = 29
T = 25
U = 21
V = 26
W = 37
X = 10
Y = 91
Z = 36

Bigraf yang paling sering muncul adalah FW, KQ, FQ, dan BY. Dapat kita asumsikan bahwa 12 huruf yang paling sering muncul adalah ETAOIN SHRDLU. Dengan membandingkan monograf dan bigraf kita mendapatkan kandidat bahwa huruf F pada cipherteks adalah huruf E pada plainteks. Dengan asumsi tersebut kita dapat berasumsi lebih lanjut bahwa huruf berada pada baris yang sama dengan huruf E atau berada tepat dibawah huruf E. Dengan cara yang sama, kita dapat mengasumsikan perkiraan letak huruf- huruf lainnya pada tabel. Selain itu, ada beberapa fakta yang dapat membantu kita untuk memecahkan *Playfair cipher,* yaitu :

1. Setiap huruf plainteks akan diubah menjadi tidak lebih dari lima huruf cipherteks yang berbeda.
2. Huruf yang berada pada baris yang sama dengan huruf yang sering muncul akan memiliki frekuensi yang tinggi pada cipherteks
3. Jika *Playfair* mengenkripsi AB menjadi XY, maka BA akan dienkripsi menjadi YX

Dengan asumsi-asumsi yang sudah kita dapatkan, kita akan membuat sebuah . Setelah membuat kandidat tabel, lalu lakukan perubahan kecil pada tabel. Perubahan kecil ini digunakan untuk melihat perubahan pada plainteks yang dihasilkan. Penemuan tabel kunci akan jauh lebih mudah dengan *known-plaintext attack.*

Tabel kunci :

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

E. Kriptanalisis pada Four-square Cipher

Dengan menggunakan metode yang sama dengan yang digunakan pada *Playfair cipher,* didapatkan data sebagai berikut :

A = 49
B = 78
C = 62
D = 66
E = 74
F = 49
G = 33
H = 48
I = 104
J = 79
K = 53
L = 64
M = 59
N = 98
O = 42
P = 147
Q = 0
R = 44
S = 96
T = 24
U = 25
V = 4
W = 63
X = 14
Y = 78
Z = 13

Bigraf yang palin sering muncul adalah IP, MB, AP, dan DE. Pada metode ini kita tidak dapat langsung berasumsi karena huruf yang sama dapat memiliki banyak sekali huruf yang berkorespondensi pada cipherteksnya. Dapat dilihat dari kemunculan monograf dan bigraf yang terlihat tidak cocok, yaitu huruf A yang kemunculannya sedang, tetapi sering sekali muncul dalam digraf AP. Proses pemecahan *cipher* ini lebih lama jika dibandingkan dengan *Playfair cipher*. Akan tetapi, jika plainteks diketahui, pemecahan metode ini cukup mudah seperti pada *Playfair cipher*.

Tabel kunci :

a b c d e	C R Y P T
f g h i k	O G A H B
l m n o p	D E F I K
q r s t u	L M N Q S
v w x y z	U V W X Z

K E Y W O	a b c d e
R D A B C	f g h i k
F G H I L	l m n o p
M N P Q S	q r s t u
T U V X Z	v w x y z

V. KESIMPULAN

Melihat dari perbandingan yang sudah dilakukan, maka kesimpulan yang dapat diambil adalah :

- *Four-square cipher* memiliki keunggulan yaitu tingkat keamanan yang lebih tinggi jika dibandingkan dengan *Playfair cipher*.
- *Four-square cipher* memiliki kelemahan yaitu proses dekripsi/enkripsi yang memakan waktu lebih lama
- *Four-square* dan *Playfair cipher* dapat dipecahkan dengan mudah jika memiliki jumlah teks yang mencukupi.
- *Playfair cipher* lebih umum digunakan karena lebih praktis daripada *Four-square* cipher.

REFERENSI

[1] Munir, Rinaldi, Slide Kuliah IF3058, Kriptografi, bagian Algoritma Kriptografi Klasik, 2012.
[2] Munir, Rinaldi, Slide Kuliah IF3058, Kriptografi, bagian Kriptanalisis, 2012.
[3] http://practicalcryptography.com/ciphers/classical-era/playfair/
[4] http://practicalcryptography.com/ciphers/classical-era/four-square/
[5] http://en.wikipedia.org/wiki/Cryptography
[6] http://en.wikipedia.org/wiki/Playfair_cipher
[7] http://en.wikipedia.org/wiki/Four-square_cipher
[8] http://en.wikipedia.org/wiki/Atlantis

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, 19 Maret 2012

Tadya Rahanady H (13509070)