Algoritma Kriptografi Klasik Baru

William - 13508032
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If18032@students.if.itb.ac.id

Abstrak – Dewasa ini, ilmu kriptografi dan kriptanalisis sudah berkembang dengan sangat pesat. Dimulai dari penyembunyian kode yang masih bisa dilakukan hanya dengan pensil dan kertas atau alat bantu mekanik sederhana saja, dan fokus diberikan pada upaya penyembunyian algoritma yang digunakan beserta kuncinya (dikenal juga dengan masa kriptografi klasik), sampai sekarang, dimana upaya penyembunyian data sudah menggunakan alat bantu elektronik yang canggih seperti perangkat komputer, dengan karakteristiknya adalah algoritma kriptografinya yang disebarluaskan secara bebas, berfokus dengan penggunaan komputasi matematis dengan bilangan yang sangat besar sehingga membutuhkan waktu yang sangat lama bila seluruh kemungkinan kombinasi dicobakan satu persatu, serta operasi dalam bit.

Pada makalah ini, penulis akan berusaha memberikan sebuah algoritma kriptografi klasik yang dapat digunakan dan tidak obsolete pada jaman modern ini, yaitu penyembunyian data yang ada dengan menggunakan operasi – operasi kriptografi klasik seperti pergeseran maupun substitusi huruf dengan operasi sedemikian rupa sehingga relative tidak terlalu sulit dalam upaya dekripsi dan enkripsi, namun sulit dipecahkan bila penyerang tidak mengetahui kunci yang digunakan. Tidak seperti algoritma – algoritma kriptografi klasik lainnya yang bergantung pada kerahasiaan algoritma yang digunakan, algoritma ini walau disebarluaskan algoritmanya tetao cukup aman untuk digunakan karena masih relative sulit untuk melakukan kriptanalisis.

Pembahasan mengenai algoritma yang dimaksud serta alasan mengapa algoritma ini aman akan dijelaskan pada bab berikutnya

Kata Kunci – Kriptografi klasik, Algoritma, Substitusi, Transposisi.

I. PENDAHULUAN

Algoritma kriptografi klasik sangat menarik untuk dipelajari. Karena, selain teknik – teknik yang diperkenalkan cukup unik dan bervariasi, kita juga dapat secara langsung mempraktekkan proses enkripsi dan dekripsinya, serta melakukan kriptanalisis dengan cukup mudah walau hanya menggunakan pensil dan kertas saja. Namun, kemenarikannya itu juga menjadi kelemahannya, yaitu bahwa untuk sebagian besar algoritma kriptografi klasik yang ada, sudah ditemukan semacam *guideline* untuk melakukan kriptanalisis, yang berarti informasi yang seharusnya rahasia tersebut menjadi relative tidak terlalu aman bila dibandingkan dilakukan pengenkripsian dengan algoritma kriptografi modern.

Pada bab ini akan dijelaskan secara singkat jenis – jenis algoritma kriptografi klasik serta istilah – istilah yang digunakan untuk membantu pembaca agar tidak kesulitan dalam membaca makalah ini.

Secara umum, algoritma kriptografi klasik terbagi menjadi 2 bagian besar, yaitu algoritma transposisi dan algoritma substitusi. Algoritma transposisi berarti adalah proses enkripsi dilakukan dengan cara melakukan pergeseran tertentu terhadap urutan huruf – huruf dari teks yang ingin disembunyikan. Sehingga misalnya bila teks yang ada adalah INFORMATIKA, hasil enkripsinya adalah IMFATRNKAOI. Sedangkan algoritma kedua, yaitu algoritma substitusi adalah melakukan enkripsi dengan mengganti suatu karakter dari teks dengan karakter lain tanpa merubah susunan huruf yang ada sesuai kuncinya. Jadi misalnya teks INFORMATIKA, bila dilakukan enkripsi hasilnya dapat menjadi JOGPSNBUJLB. Dapat dilihat bahwa huruf B menggantikan huruf A, dan seterusnya.

II. KONSEP

Setelah mengenal mengenak algoritma – algoritma kriptografi klasik, sekarang akan dilakukan pembahasan mengenai algoritma yang saya kembangkan ini. Berbeda dengan algoritma – algoritma standar yang sebagian besar hanya melakukan 1x proses enkripsi, untuk mempersulit kriptanalisis, algoritma ini melakukan kombinasi – modifikasi dari algoritma yang ada untuk menghilangkan kelemahan – kelemahan yang dimiliki setiap algoritma tersebut sehingga algoritma ini dapat bertahan di dunia modern.

Secara umum, langkah – langkah untuk melakukan enkripsi dengan algoritma ini adalah seperti dibawah ini:

1. Tentukan kunci yang ingin digunakan. Kunci dapat sepanjang apapun. Namun, seperti pada metode algoritma kriptografi klasik pada umumnya, karakternya terbatas pada huruf a-z, dan angka 0-9.

2. Lakukan pergeseran Vigenère basis 36.

Pergeseran Vigenère adalah salah satu algoritma enkripsi substitusi, dengan proses enkripsi standarnya adalah sebagai berikut:

- Tuliskan setiap karakter pada plain text di selembar kertas
- Tuliskan kata kunci dibawah setiap karakter pada plain text. Bila kata kuncinya lebih pendek dari plain text, ulangi kata kunci sampai sama panjang dengan plain textnya. (Kunci terbatas pada alphabet a-z)
- Lakukan penomoran dari setiap karakter plain text, dan kunci dengan a bernilai 0, sampai z bernilai 25.
- Lakukan pertambahan antara nilai numeric karakter plain text dan kunci, lakukan dalam modulus 26.
- Hasil dari pertambahan tersebut adalah cipertextnya.

Sehingga, proses enkripsinya adalah: = +

$$C_i = E_k(M_i) = (M_i + K_i) \bmod 26$$

dan proses dekripsinya adalah:

$$M_i = D_k(C_i) = (C_i - K_i) \bmod 26$$

Dimana:

$M = M_0 \ldots M_n$ adalah plain textnya,
$C = C_0 \ldots C_n$ adalah ciphertextnya, dan
$K = K_0 \ldots K_m$ adalah kunci yang digunakan.

Sehingga, untuk mengenkripsi huruf A (bernilai 0) dengan kunci huruf L (bernilai 11), hasilnya adalah nilai 11 (huruf L) dengan: 11 = (0 + 11) mod 26. Sementara, untuk dekripsi misalnya huruf R (bernilai 17) dengan kunci huruf E (bernilai 4), hasilnya adalah nilai 13 (huruf N) dengan prosesnya: 13 = (17 - 4) mod 26.

Pergeseran Vigenère dengan basis 36 adalah sedikit modifikasi dari pergeseran Vigenère tradisional, yaitu dengan menggunakan basis modulus 36. Cara enkripsi maupun dekripsinya sama dengan pergeseran Vigenère modulus 26, dengan angka 0 – 9 diberikan nilai dari 26 sampai 35.

Jadi, untuk mengenkripsi huruf J (bernilai 10) dengan kunci angka 0 (bernilai 26), hasilnya adalah nilai 0 (huruf A) dengan: 0 = (10 + 26) mod 36.

3. Lakukan pergeseran ke kanan dengan basis kunci.

Pada langkah ini adalah dilakukan algoritma transposisi dengan melakukan pergeseran setiap karakter sejauh n karakter ke kanan, dengan n adalah nilai integer dari kebalikan kunci. Nilai integer kunci disini mirip seperti nilai integer kunci pada pergeseran Vigenère, namun semua nilainya ditambah dengan 1 (Jadi, kunci A bernilai 1, bukan 0). Kemudian, pergeseran karakter selanjutnya dimulai pada 1 karakter didepannya. Bila pergeseran sudah lebih jauh dari plain text, kembali ke slot pertama. Pergeseran ini mengindahkan slot yang sudah memiliki isi. Kebalikan kunci disini berarti proses dimulai dari karakter terakhir kunci, berjalan mundur sampai ke karakter pertama.

Sehingga, bila plain textnya (hasil enkripsi dengan pergeseran Vigenère pada poin 2) adalah HELLO dengan kunci DEBA, langkah untuk melakukan pergeseran ini adalah sebagai berikut:

Sediakan slot untuk ciphertext sejumlah huruf pada plain text sebagai berikut:

H E L L O menjadi __ __ __ __ __.

Masukkan nilai integer kebalikan kunci untuk mempermudah proses komputasi, menjadi sebagai berikut:

DEBA kebalikannya adalah ABED; namun karena panjang kuncinya lebih pendek dari plain text, ulangi menjadi: ABEDA, dengan nilai integernya adalah 1,2,5,4,1.

Berarti, masukkan H pada slot pertama yang tersedia, yaitu di slot pertama menjadi: H ___ ___ ___ ___. untuk huruf E, letakkan pada slot kosong ke 2 yang tersedia, menjadi: H ___ E __ __. Ulangi lankah ini sampai semua huruf masuk ke slot yang tersedia, sehingga menjadi:
H O E L L.

Langkah dekripsi untuk proses ini cukup mudah, yaitu dengan mengambil dari slot yang tersedia sejauh kunci, dan meletakkannya berurutan ke slot 1, 2, dan seterusnya. Sehingga, bila ciphertextnya adalah H O E L L, dan kuncinya setelah diproses adalah ABEDA yang bernilai 1,2,5,4,1, langkah – langkahnya adalah:
ambil huruf pada slot pertama tersedia (karena kunci bernilai 1) dan letakkan sebagai huruf pertama menjadi:
plain text: : H __ __ __ __, dan ciphertext tersisa:
__ O E L L. kemudian, ambil huruf pada 2 slot berikutnya, letakkan sebagai huruf kedua dari plaintext. Pada iterasi ini, akan didapat huruf E. Hilangi huruf E dari slot tersedia. Ulangi langkah ini sampai slot tersedia pada plain text terisi semua.

4. Lakukan 1x pergeseran lagi, dengan menggabungkan huruf pertama plain text (hasil enkripsi dari langkah 3) dengan huruf terakhir dari plain text, dilanjutkan dengan huruf kedua dengan huruf kedua terakhir, dan selanjutnya. Sehingga, untuk plain text HOELL, hasil enkripsinya adalah menjadi: HLOLE. Untuk kasus ini, cara dekripsinya juga cukup mudah, yaitu mengambil huruf pertama dari setiap bigram, dan meletakannya sebagai huruf pertama, kedua, dan seterusnya. Kemudian, bila semua bigram sudah diambil huruf pertamanya, gabungkan setengah bagian kedua dari bigram (tang berisi huruf – huruf yang belum diambil) ke rangkaian teks yang dimiliki. Secara otomatis cipherteks akan terbentuk kembali menjadi plain text.

5. Lakukan enkripsi dengan playfair cipher dengan basis 36. Playfair cipher adalah salah satu algoritma kriptografi klasik yang memiliki tingkat kesulitan kriptanalisis yang cukup tinggi. Namun, biasanya, playfair cipher menggunakan basis bujur sangkar berukuran 25, dengan menggunakan huruf alphabet a – z, dan mengganggap karakter j = karakter i. Berikut adalah cara melakukan enkripsi dengan playfair cipher standar:

- Ganti seluruh huruf j pada kunci dengan huruf i.
- Masukkan kata kunci pada slot yang tersedia pada bujur sangkar playfair dengan mengindahkan huruf dengan kemunculan kedua atau lebih.
- Bila masih ada slot kosong pada bujur sangkar tersebut, isikan dengan huruf – huruf alfabet yang tersisa dengan mengindahkan huruf J.

- Bentuk seluruh karakter pada plain teks menjadi bigram (kumpulan berukuran 2 karakter). Bila kedua huruf pada bigram tersebut sama, ganti huruf kedua menjadi huruf X, dan karakter pertama bigram berikutnya dimulai dari huruf kedua dari huruf yang sama tersebut.
- Apabila bigram terakhir hanya terdiri dari 1 huruf, tambahkan huruf X sebagai huruf kedua bigram tersebut. Kemudian, lakukan pemetaan pada kunci sesuai aturan yang ada.

Aturan pemetaan kunci pada playfair cipher ini adalah:

- Bila kedua huruf muncul pada baris yang sama pada tabel kunci, ganti pasangan huruf tersebut dengan huruf yang terletak di kanan setiap huruf tersebut.
- Bila pasangan huruf tersebut muncul pada kolom yang sama, ganti dengan huruf yang terletak di bawahnya.
- Bila huruf tersebut terletak pada baris dan kolom yang berbeda, ambil huruf yang terletak pada titik potong antara baris pada huruf pertama dan kolom pada huruf kedua sebagai huruf pertama dari bigram kunci, dan huruf yang terletak pada titik potong lainnya sebagai huruf keduanya.

Untuk mendekripsinya, caranya adalah melakukan inversi dari cara – cara yang ada pada poin kedua sampai keempat, dan, untuk poin pertama adalah dengan mengganti pasangan huruf yang memiliki huruf X yang tidak bermakna dengan huruf yang sama dengan huruf pertama.

Playfair cipher dengan basis 36 berarti bahwa ukuran bujur sangkar yang terbentuk adalah berukuran 6 x 6, yang terbentuk dari 26 huruf alfabet dan 10 angka. Dengan demikian, huruf i dan j pada plain text dapat dianggap sebagai huruf yang berbeda. Sedangkan, untuk melakukan enkripsi, caranya sama dengan cara enkripsi pada playfair standar dengan sedikit perbedaan saja, yaitu bahwa bigram yang berisi pasangan huruf yang sama, huruf keduanya tidak diubah dengan huruf X, dan bigram berikutnya dimulai dari huruf berikutnya. Jadi, enkripsi tidak dilakukan pada bigram tersebut. Alasan untuk hal ini akan dijelaskan kemudian.

Jadi, bila pada playfair cipher biasa kata bassist diubah menjadi bigram BA SX SI ST, pada algoritma ini, bassist diubah menjadi BA SS IS TX.

6. Langkah terakhirnya adalah mengulang langkah 2 - 4 sebanyak n kali, dimana n adalah nilai dari rata – rata nilai integer kunci (huruf a bernilai 1, sampai dengan angka 0 yang bernilai 36) dengan pembulatan kebawah yang berarti ada maksimum 36 x perulangan (bila seluruh kata kunci terdiri dari angka 0). Pada setiap perulangan, lakukan pergeseran huruf pada kunci sejauh n karakter ke kanan.

Untuk melakukan dekripsi, caranya adalah melakukan inverse pada setiap langkah enkripsi. Dimulai dengan mengambil nilai rata – rata dari nilai integer kunci untuk menentukan jumlah pengulangan yang dilakukan. Setelah itu, menggeser karakter pada kunci sejauh n ^ n karakter yang akan digunakan sebagai kunci pada langkah pertama. Kemudian, setelah dilakukan dekripsi pertama, dekripsi diulangi sebanyak n kali lagi, dengan menggeser kunci sejauh n karakter ke kiri pada setiap perulangannya.

Karena enkripsi dilakukan berulang kali, pada tahap pengenkripsian dengan menggunakan playfair cipher, mustahil bagi kita untuk mengetahui apakah huruf X yang didapat adalah hasil dekripsi adalah X akibat bigram berisi huruf kembar atau memang X adalah huruf yang dimaksud. Karena itu, tidak dilakukan substitusi antara pasangan huruf kembar dengan huruf X.

III. PEMBAHASAN

Metoda algoritma enkripsi ‘baru’ ini, menggabungkan pengembangan beberapa jenis metoda enkripsi serta mengimplementasikan perulangan enkripsi untuk mempersulit penyerangan. Selain itu, kata kunci yang dapat terdiri dari 36 karakter dan terus berubah pada setiap perulangannya, membuat proses penyerangan pada algoritma ini menjadi lebih sulit. Berikut ini beberapa kelebihan yang dimiliki algoritma ini:

- Melakukan perulangan enkripsi. Metoda ini menyebabkan walaupun penyerang berhasil menebak kuncinya, pada percobaan pertama, mereka tetap akan menemukan teks yang masih tidak bermakna. Hal ini melakukan proses kriptanalisis tanpa mengetahui plain teks menjadi sangat sulit.
- Pilihan kombinasi kunci yang lebih banyak. Tidak seperti algoritma kriptografi klasik pada umumnya yang membatasi pilihan kombinasi kunci pada 26 karakter alfabet saja, menjadi 36 karakter dengan tambahan 10 karakter angka. Hal ini menyebabkan penyerangan dengan cara brute force menjadi lebih sulit. Selain itu, kunci yang terus berubah pada setiap perulangan juga mempersulit penyerangan.
- Tidak dapat dipecahkan dengan metoda analisis frekuensi. Metoda analisis frekuensi adalah salah satu metoda yang paling mudah digunakan namun paling efektif untuk membantu penyerangan pada algoritma kriptografi klasik standar. Namun dengan metoda algoritma ini, pada huruf – huruf yang ada dilakukan penggantian dengan jumlah yang cukup banyak, sehingga pada akhirnya akan menghasilkan kumpulan huruf yang acak dan mengakibatkan metoda analisis frekuensi ini menjadi tidak membantu
- Tidak dapat dipecahkan dengan metoda kasiski. Metoda ini adalah salah satu metoda yang paling popular untuk memecahkan algoritma vigenere. Namun, karena pada metoda ini tidak hanya mengimplementasikan metoda vigenere, metoda ini jadi tidak dapat digunakan.
- Tidak dapat dipecahkan dengan metoda analisis frekuensi bigram. Adalah metoda yang digunakan untuk membantu memecahkan metoda playfair. Namun, algoritma ini tidak dapat dipecahkan dengan metoda tersebut. Karena, selain jumlah kemungkinan bigram yang menjadi lebih banyak, urutanya juga sebelumnya sudah

dikacaukan dengan pergeseran vigenere dan metoda transposisi.

- Kata kunci yang boleh sama panjangnya dengan plain text. Walau kemudian menjadi sedikit 'dibatasi' saat mengimplementasikan playfair, tapi kunci yang panjang membantu menguatkan enkripsi dengan metoda vigenere, maupun pada pergeseran ke kanan seperti pada poin nomor 3 pada cara enkripsi.
- Mudah diimplementasikan. Karena seluruh operasinya hanya melibatkan pergeseran ataupun substitusi biasa, sangat mudah membuat aplikasi untuk membantu melakukan enkripsi dan dekripsi dengan algoritma ini. Tidak hanya itu, ukuran teks juga tidak berubah setelah dienkripsi, sehingga untuk teks yang relative panjang tidak mengakibatkan lonjakan akan ukurannya yang mengakibatkan pertukarannya menjadi sulit.
- Sulit diserang walau dengan known plaintext attack. Karena penyerang tidak mengetahui kuncinya, ia menjadi tidak mengetahui jumlah perulangan yang dilakukan. Sehingga, ia terpaksa melakukan perulangan dalam jumlah maksimum yang mungkin karena ia tidak mengetahui kapan harus berhenti. Tidak hanya itu, ia juga tidak dapat melakukan *tracking* terhadap huruf demi huruf karena urutannya sudah diacak dengan melakukan enkripsi playfair, dan dilakukan perulangan.

IV. PROSES

Dibawah ini akan dijelaskan langkah demi langkah yang dilakukan pada proses enkripsi maupun dekripsi dengan algoritma ini.

Misalkan plain text-nya adalah:

IF08ITB

Dan kunci yang digunakan adalah:

GAJAH

Karena kata kuncinya adalah GAJAH, yang memiliki nilai rata – rata: (7 + 1 + 10 + 1 + 8) : 5 = 27 : 5 = 5.4, berarti, pengulangan dilakukan sebanyak 5 kali.

1. Lakukan pergeseran vigenere. Sehingga, kuncinya menjadi GAJAHGA untuk menyamai panjang dari IF08ITB. Lakukan operasi untuk menggeser, sehingga langkahnya adalah:

I F 0 8 I T B + G A J A H G A = O F 9 8 P Z B

8 5 26 34 8 19 1 + 6 0 9 0 7 6 0 = 14 5 35 34 15 25 1

2. Lakukan pergeseran kekanan sesuai nilai kunci, yang mengakibatkan hasil pergeserannya menjadi:

F 8 B P Z 9 O

3. Lakukan penyatuan huruf pertama dan terakhir, dan seterusnya. Sehingga, hasilnya adalah:

FO 89 BZ P

4. Lakukan enkripsi dengan playfair. Namun untuk itu, terlebih dahulu harus dibentuk bujur sangkarnya, yang bentuknya adalah:

G A J H B C
D E F I K L
M N O P Q R
S T U V W X
Y Z 0 1 2 3
4 5 6 7 8 9

Karena bigram terakhir hanya berisi huruf P, maka tambahkan huruf X agar menjadi bigram yang utuh. Dengan ini, hasil enkripsinya mengikuti aturan yang ada adalah menjadi:

OU 94 A2 RV

5. Pada langkah ini, seharusnya, pada kunci GAJAH dilakukan pergeseran pada setiap huruf sejumlah 5 karakter. Namun, karena secara kebetulan panjang kuncinya juga 5 karakter, kunci jadi tidak mengalami perubahan untuk pengulangan-pengulangan berikutnya.
6. Masuk ke pengulangan pertama. Plain text yang dimiliki sekarang adalah:

O U 9 4 A 2 R V

Dengan kunci yang masi sama seperti sebelumnya, adalah:

G A J A H

7. Lakukan pergeseren vigenere. Seperti biasa, kunci gajah diulang untuk menyamai panjang plain text, menjadi GAJAHGA. Kemudian, operasi vigenerenya:

O U 9 4 A 2 R V + G A J A H G A J = U U J 4 H 8 R 4

14 20 35 30 0 28 17 21 + 6 0 9 0 7 6 0 9 = 20 20 9 30 7 34 17 30

8. Lakukan pergeseran kekanan sesuai nilai integer kunci. Hasil dari pergeseran ini menjadi:

R 4 H J 4 8 U U

9. Kemudian, lakukan penyatuan huruf pertama dan terakhir sehingga hasilnya menjadi:

RU 4U H8 J4

10. Kemudian, lakukan enkripsi playfair pada bigram tersebut. Karena kata kuncinya tidak mengalami perubahan dari pengulangan sebelumnya, kita masih dapat menggunakan bujur sangkar yang sama. Selain itu, karena sekarang bigram terakhirnya sudah lengkap, plain text bisa langsung dienkripsi. Hasilnya enkripsi tersebut adalah:

OX 6S B7 G6

11. Masuk ke pengulangan kedua (kata kunci masih sama). Lakukan pergeseran vigenere pada plain text OX6SB7G6 sehingga menjadi:

O X 6 S B 7 G 6 + G A J A H G A J = U W F S I 7 G F

14 23 32 18 1 33 6 32 + 6 0 9 0 7 6 0 9 = 20 23 5 18 8 33 6 5

12. Lakukan pergeseran kekanan. Hasil dari pergeseran ini adalah:

G F I F S 7 U W

13. Satukan huruf pertama dan terakhir, menjadi:

GW FU I7 FS

14. Lakukan enkripsi dengan playfair cipher. Hasilnya adalah:

BS O0 PH DU

15. Masuk ke pengulangan ketiga. Sekarang, plain text yang digunakan adalah BS O0 PH DU. Lakukan pergeseran dengan algoritma vigenere menjadi:

B S O 0 P H D U + G A J A H G A = H S Z 0 U N C 3

1 18 14 26 13 7 3 20 + 6 0 9 0 7 6 0 9 = 7 18 25 26 20 13 3 29

16. Dengan pergeseran kekanan, hasilnya menjadi:

C 3 U Z 0 N H S

17. Satukan huruf pertama dan terakhir. Menjadi:

CS 3H UN Z0

18. Dilakukan enkripsi playfair, hasilnya menjadi:

GX 1C TO 01

19. Pengulangan ketiga selesai. Masuk ke pengulangan keempat. Dengan plain text yang digunakan sekarang adalah GX1CTO01. Lakukan pergeseran dengan vigenere, sehingga diperoleh hasilnya adalah:

G X 1 C T O 0 1 + G A J A H G A J = M X A C 0 U 0 A

6 23 27 2 19 14 26 27 + 6 0 9 0 7 6 0 9 = 12 23 0 2 26 20 26 0

20. Geser kekanan, menjadi:

0 A 0 A C U M X

21. Satukan huruf pertama dan terakhir menjadi:

0X AM 0U AC

22. Lakukan enkripsi degan playfair, didapat:

3U GN 60 JG

23. Pengulangan keempat selesai, lakukan pengulangan vigenere terakhir dengan plain textnya adalah 3UGN60JG. Hasilnya adalah:

3 U G N 6 0 J G + G A J A H G A J = 9 U P N D 6 J P

29 20 6 13 32 26 9 6 + 6 0 9 0 7 6 0 9 = 35 20 15 13 3 32 9 15

24. Geser kekanan, didapat:

J P D P N 6 9 U

25. Satukan huruf pertama dan terakhir, menjadi:

JU P9 D6 PN

26. Terakhir, lakukan enkripsi dengan playfair cipher sehingga hasilnya akhirnya adalah:

F0 R7 F4 QO

Jadi, teks IF08ITB setelah dienkripsi dengan kunci GAJAH dengan algoritma ini, hasilnya ciphertextnya adalah F0R7F4QO.

Untuk melakukan dekripsi, langkahnya adalah membalik apa saja yang sudah dikerjakan. Namun yang perlu diingat adalah, pada pengulangna terakhir, setelah dilakukan playfair decipher, bila didapat hasil huruf terakhirnya adalah X, berarti ada 2 kemungkinan apakah X nya adalah memiliki arti atau tidak. Lakukan dekripsi berikutnya (pemisahan huruf pertama dan terakhir, pergeseran ke kiri, dan dekripsi pergeseran vigenere) dengan menghilangkan X tersebut terlebih dahulu, karena kemungkinan kemunculan X disana sebagai 'pelengkap' bigram lebih besar daripada kemungkinan kemunculan huruf X sebagai plain teks (1:2 dengan 1:15 pada kasus terbaik). Bila hasil dekripsinya tidak memiliki arti, lakukan pengulangan dengan menyertakan X tersebut pada langkah – langkah terakhir tersebut.

V. IMPLEMENTASI

Dibawah ini adalah rancangan antar muka untuk aplikasi ini. Antar muka aplikasi ini didesain dan diimplementasi-kan menggunakan Microsoft visual studio, dengan bahasa C#.

Gambar 1. Langkah awal enkripsi

Gambar 2. Perulangan pertama enkripsi

Gambar 3. Perulangan kedua enkripsi

Gambar 4. Perulangan ketiga enkripsi

Gambar 5. Perulangan keempat enkripsi

Gambar 6. Perulangan terakhir enkripsi

VI. KESIMPULAN

Algoritma baru ini merupakan penggabungan modifikasi dari algoritma – algoritma kriptografi klasik standar. Namun, dengan dilakukannya penggabungan tersebut, algoritma ini menjadi sulit untuk dilakukan penyerangan karena dapat mematahkan cara – cara yang biasa digunakan oleh kriptanalis untuk memecahkannya.

Keunggulan dari algoritma ini adalah mungkinnya pemilihan kunci yang lebih beragam dibandingkan algoritma kriptografi klasik lainnya (dapat memilih kombinasi dari 36 karakter), panjang kunci yang tidak dibatasi, enkripsi yang dilakukan berulang kali, kunci yang terus berubah untuk setiap perulangan yang dilakukan, serta kombinasi dari algoritma – algoritma yang ada membuat algoritma ini menjadi sangat sulit untuk diserang oleh penyerang baik ia memiliki plain textnya ataupun tidak.

Walau demikian, keunggulan itu tentu memiliki kelemahan yakni proses enkripsi maupun dekripsinya bila dikerjakan secara manual dengan pensil dan kertas walau tidak sulit, tapi cukup merepotkan dan melelahkan. Karena, setiap tahap enkripsi yang terdiri dari beberapa algoritma enkripsi harus diulang berkali – kali. Walau, bila dilakukan dengan bantuan komputer, enkripsinya maupun dekripsinya menjadi sangat mudah dan cepat.

Tidak seperti metoda kriptografi klasik lainnya yang dapat dipecahkan hanya dengan pensil dan kertas, metoda ini bahkan sulit dipecahkan dan akan membutuhkan waktu yang lama untuk dipecahkan menggunakan perangkat modern seperti komputer (dengan asumsi penyerang menggunakan metoda brute force dengan mencoba setiap kemungkinan kunci satu – persatu) karena jumlah kemungkinan kombinasi kunci yang sangat banyak, dengan worst case scenario yang harus dicobakan oleh si penyerang adalah 36^n, dimana n adalah jumlah karakter pada plain teks.

Untuk mencoba satu persatu kemungkinan, pada enkripsi yang bahkan hanya terdiri dari 24 karakter saja, jumlah kemungkinan yang ada (maksimum) adalah $36 + 36^2 + 36^3 + ... + 36^{24}$ yang nilai 36^{24} nya saja setara dengan 2.25×10^{37} kemungkinan yang berarti, bahkan untuk sebuah super komputer yang dapat mencoba 1.000.000.000.000 kemungkinan per detiknya, komputer itu tetap membutuhkan waktu 2.25×10^{25} detik (7.13×10^{17} tahun).

Hal ini membuktikan, tidak hanya sulit dipecahkan dengan kertas karena metodanya yang masih belum ada, bahkan kemungkinan ditemukan metodanya jgua sangat kecil akibat tingkat kerumitan yang tinggi. Algoritma ini juga sulit untuk dipecahkan bahkan dengan sebuah super komputer yang berarti algoritma ini sangat aman untuk digunakan.

REFERENSI

[1] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", 1997, CRC Press

[2] Christof Paar and Jan Pelzl, "Understanding Cryptography – A Textbook for Students and Practioners", 2009, Springer

[3] http://en.wikipedia.org/wiki/Cryptography

[4] http://www.fortunecity.com/skyscraper/coding/379/lesson1.htm

[5] http://www.kryptographiespielplatz.de/

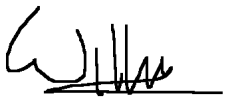
[6] http://www.ridex.co.uk/cryptology/

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, 22 Maret 2011

ttd



William

13508032