Heavy Rotation Cipher, Sebuah Algoritma Multi-Enkripsi Klasik Baru

Ryan Rheinadi / 13508005
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18005@students.if.itb.ac.id
ryanrheinadi@students.itb.ac.id

Abstrak - Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing). Artinya "secret writing". Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996].

Dalam perkembangan sejarah kriptografi klasik, yaitu kriptografi berbasis karakter, telah tercipta banyak algoritma-algoritma kriptografi yang memiliki keunikan masing-masing, baik cipher-cipher yang bersifat substitusi maupun transposisi. Beberapa diantaranya misalnya Caesar Cipher, Vigenère Cipher, Playfair Cipher, Affine Cipher, Hill Cipher, maupun Enigma Cipher.

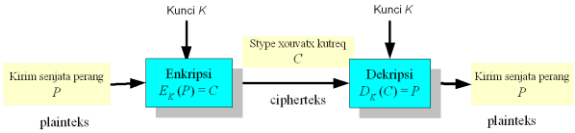
Vigenère Cipher dan rail-fence cipher adalah algoritma-algoritma kriptografi klasik yang telah obsolete karena telah berhasil dipecahkan, bahkan dengan mudah menggunakan tabel frekuensi kemunculan huruf, bigram dan trigram serta tabel anagram dalam suatu bahasa sehingga sudah tidak aman lagi untuk digunakan. Oleh karena itu, saya mencoba membuat algoritma kriptografi klasik baru yang merupakan kombinasi dari kedua algoritma tersebut dengan memanfaatkan prinsip multiple encryption sehingga sulit untuk dipecahkan dan memiliki tingkat keamanan yang tinggi, namun mudah diterapkan.

Kata Kunci : Algoritma Kriptografi Klasik, Vigenère Cipher, rail-fence cipher, Multi Enkripsi

I. PENDAHULUAN

Kata *cryptography* berasal dari bahasa Yunani: *krupto* (hidden atau secret) dan *grafh* (writing), artinya "secret writing". Definisi lama kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam perkembangannya, kriptografi berkembang sedemikan rupa sehingga tidak lagi sebatas mengenkripsi pesan, tetapi juga memberikan aspek keamanan yang lain. Oleh karena itu, tercipta definisi baru kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (message) [Schneier, 1996].

Sistem kriptografi tersusun atas algoritma kriptografi yang akan digunakan untuk penyandian pesan, plainteks yang berperan sebagai teks yang akan disandikan, cipherteks sebagai teks yang telah disandikan, serta kunci yang merupakan parameter dalam proses *enciphering* dan *deciphering*. Penggunaan kunci membuat algoritma kriptografi tidak perlu rahasia atau bersifat publik. Keterkaitan antara plainteks, cipherteks dan kunci dapat dilihat pada gambar berikut ini.



Gambar 1. Gambaran Sistem Kriptografi

Algoritma kriptografi menurut masanya terbagi menjadi dua, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern. Perbedaan mendasar dari kedua jenis algoritma kriptografi ini adalah algoritma kriptografi modern beroperasi dalam mode *bit*, sedangkan algoritma kriptografi klasik masih beroperasi dalam mode karakter. Sehingga jumlah karakter yang dapat digunakan dalam algoritma kriptografi klasik akan lebih sedikit dibandingkan dengan algoritma kriptografi modern.

Secara umum, algoritma kriptografi klasik terbagi atas dua jenis, yaitu algoritma transposisi dan substitusi. Terdapat dua perbedaan mendasar antara kedua jenis algoritma ini. Pada algoritma transposisi, enkripsi dilakukan dengan cara penukaran letak tempat huruf-huruf pada satu kata yang sama, misalnya "KRIPTOGRAFI" menjadi "PRTKIGOFRAI". Pada algoritma *rail-fence* cipher, transposisi dilakukan dengan mekanisme seperti gambar di bawah ini.

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Gambar 2. Contoh Rail-Fence Cipher

Pada gambar di atas, rail fence membagi plainteks menjadi tiga baris, kemudian menyusunnya berdasarkan urutan baris sehingga plainteks awal yaitu "WE ARE DISCOVERED FLEE AT ONCE" menjadi cipherteks "WECRLTEERDSOEEFEAOCAIVDEN".

Pada algoritma substitusi, enkripsi dilakukan dengan

cara mengganti masing-masing huruf pada kata dengan huruf lain sesuai algoritma tertentu. Contoh simpelnya adalah *caesar cipher*, dimana setiap huruf akan diubah dengan cara dilakukan substitusi dengan tiga huruf setelahnya, sehingga "A" menjadi "C", "D" menjadi "F" dan sebagainya.

Vigenere Cipher adalah modifikasi dari *Caesar Cipher*, yaitu *Caesar Cipher* dengan kunci yang berbeda-beda dalam setiap karakternya. Kunci yang berbeda diperoleh dari masukan user yang diterjemahkan menjadi angka per-alfabetnya. Dalam perkembangannya, terdapat banyak varian *Vigenere Cipher*. *Multiple Encryption* adalah metode mengenkripsi kembali pesan yang telah terenkripsi oleh satu algoritma, baik dengan algoritma yang sama maupun berbeda, baik hanya sekali maupun berulang-ulang.

II. KONSEP ALGORITMA HEAVY ROTATION

Setelah mengenali konsep-konsep kriptografi dasar yang digunakan dalam pembuatan algoritma ini, akan dilakukan pembahasan mengenai konsep algoritma heavy rotation ini. Perbedaan mendasar antara heavy rotation dengan algoritma kriptografi klasik lainnya terletak pada penggunaan multi enkripsi menggunakan dua algoritma klasik lain, yaitu *rail-fence* dan *Vigenère*. Penggunaan konsep multi enkripsi dengan multi algoritma dengan satu algoritma adalah algoritma transposisi dan satunya lagi adalah algoritma substitusi ini akan mempersulit usaha-usaha kriptanalis untuk memecahkan algoritma ini. Hal ini akan mengakibatkan untuk memperoleh informasi, perlu dilakukan usaha kriptanalisis yang tidak sebanding dengan nilai informasi yang didapat.

Secara umum, langkah-langkah enkripsi algoritma heavy rotation ini adalah sebagai berikut.

1. Tentukan kunci yang akan digunakan untuk mengenkripsi pesan. Kunci harus terdiri atas alfabet-alfabet A-Z karena algoritma kriptografi masih berbasis karakter, bukan bit.
2. Hitung panjang karakter pada plainteks. Panjang plainteks harus merupakan kelipatan tiga sehingga bisa dilakukan proses dekripsi *rail-fence* yang mudah. Apabila plainteks bukan kelipatan tiga, lakukan penambahan dengan menggunakan bagian awal dari plainteks kembali hingga menjadi kelipatan tiga
3. Lakukan proses enkripsi *rail-fence* tiga baris pada plainteks. Untuk praktisnya, bisa dilakukan split-off alfabet menjadi tiga baris.
4. Lakukan proses enkripsi *Vigenère* standar pada plainteks yang telah di *rail-fence* berdasarkan kunci.. Proses enkripsi adalah sebagai berikut.
   - Berikan enumerasi masing-masing karakter pada plainteks sesuai dengan urutan alfabet, dengan enumerasi 0 dilakukan setelah enumerasi alfabet Z.
   - Lakukan pula enumerasi pada masing-masing karakter kunci dengan cara yang sama dengan enumerasi plainteks.
   - Apabila panjang kunci lebih sedikit daripada panjang plainteks, lakukan pengulangan kunci secara periodik hingga panjang kunci sama dengan panjang plainteks.
   - Apabila panjang kunci lebih panjang daripada panjang plainteks, cukup gunakan n karakter pertama dari kunci, dimana n adalah panjang plainteks.
   - Jumlahkan nilai enumerasi karakter plainteks dengan nilai enumerasi kunci yang bersesuaian.
   - Lakukan operasi modulo 26 pada hasil penjumlahan enumerasi sehingga diperoleh hasil yang merepresentasikan enumerasi dari cipherteks.
   - Terjemahkan enumerasi tersebut sehingga terdapat cipherteks yang dihasilkan.

   Secara matematis, proses enkripsi dan dekripsi dapat ditulis sebagai berikut.
   - Enkripsi
     $Ci = Ek(Mi) = (Mi + Ki) \bmod 26$
   - Dekripsi
     $Mi = Dk(Ci) = (Ci – Ki) \bmod 26$

   Dengan pendefinisian :
   M = M0 . . . Mn adalah plain textnya,
   C = C0 . . . Cn adalah ciphertextnya, dan
   K = K0 . . . Km adalah kunci yang digunakan

5. Ulangi langkah dua hingga langkah empat hingga n kali. Pada pembahasan algoritma, pengulangan langkah hanya dilakukan sebanyak 3 kali.

III. PEMBAHASAN ALGORITMA HEAVY ROTATION

Metode algoritma heavy rotation ini menggabungkan beberapa jenis metode algoritma kriptografi klasik terdahulu, dalam hal ini *rail-fence* dan *Vigenère*, serta prinsip multi enkripsi. Dalam satu kali siklus, akan dilakukan satu kali operasi *rail-fence* dan *Vigenère* pada teks. Proses multi enkripsi dua algoritma yang berbeda cara kerja ini akan mempersulit proses penyerangan yang dilakukan oleh kriptanalis. Berikut ini adalah beberapa kelebihan yang diharapkan dapat diperoleh dari algoritma multi rot V-13.

- Mudah diimplementasikan. Algoritma ini cukup mudah untuk diimplementasikan karena hanya menggunakan algoritma yang simpel, yaitu *rail-fence* dan *Vigenère*.
- Penyerangan menggunakan *known-plainteks attack* sulit untuk dilakukan. Sekalipun panjang kunci diketahui, tidak akan terbentuk pola huruf karena dilakukan tiga belas kali perulangan proses enkripsi. Proses multi enkripsi ini

mengakibatkan sekalipun panjang kunci diketahui, hasil cipherteks akan tetap tidak berpola sehingga sulit dilakukan analisis. Tentu saja untuk mengetahui panjang kunci itu cukup sulit karena tidak akan terbentuk pola huruf.

- Kata kunci dapat memiliki panjang yang sama dengan panjang teks. Keistimewaan dari hal ini adalah apabila kata kunci yang dimasukkan memiliki panjang yang sama dengan panjang teks, algoritma ini secara praktis akan menjadi sebuah *one-time pad*.
- Tidak dapat dipecahkan menggunakan metode analisis frekuensi dan analisis anagram. Penggunaan algoritma transposisi yang dikombinasikan dengan substitusi memungkinkan hal ini terjadi.

Tentunya setiap algoritma memiliki kelebihan dan kekurangan masing-masing. Hal ini berlaku pula pada algoritma kriptografi multi rot V-13 ini. Berikut ini beberapa kekurangan dari algoritma kriptografi multi rot V-13.

- Apabila kunci yang digunakan pendek, serangan *exhaustive key search* mudah untuk dilakukan.
- Enkripsi terbatas pada alfabet sehingga angka 0-9 yang tidak dienkripsi akan mengakibatkan angka-angka terlihat dengan jelas pada cipherteks. Hal ini berakibat fatal pada teks-teks yang memiliki informasi dalam angka-angka yang penting.

IV. PROSES DAN IMPLEMENTASI

Pada bab ini akan dijelaskan contoh dari penerapan algoritma heavy rotation untuk mengenkripsi maupun mendekripsi suatu teks. Untuk implementasi ini, hanya dilakukan proses perulangan sebanyak 3 kali

Misalkan plain teks adalah :

Karena kusuka suka dirimu
Kuakan selalu berada disini
Walau didalam keramaian
Tak apa tak kau sadari

Kunci yang digunakan adalah "kimisuki". Berikut ini adalah langkah-langkah penenkripsian dan pendekripsian teks. Tambahkan dua karakter awal pada plainteks, "k" dan "a" agar jumlah karakter menjadi kelipatan 3Proses rail-fence dan vigenere dilakukan menggunakan aplikasi "*cryptohelper.jar*"

1. Perulangan Pertama
   - Rail fence

     Cipherteks sementara

     KEKUS ARUAN LURAS ILDAM RANKA KUDIA NUKUD IKKSA BADIW AILKA ITATK SAKRA SAKIM UAELE DINAU DAEMA APAAA RA

     Kunci : kimisuki
   - Vigenere

     Cipherteks sementara

     UMWCK UBCKV XCJUC QVLMU JUXSK SGLAU XCUCP QCECI LIPQO USTUI UBSNU AKSDI KUUQW CMMDY NQXIG LSYWI KXMIS LK

     Kunci : kimisuki
2. Perulangan Kedua
   - Rail fence

     UCBVJ QMUKL XCCIP UUBUS KQMYX LWXSM KCXUV UXSAC PELQS ISADU WMNIS IMLWU KCCLJ SGUUQ CIOTU NKIUC DQGYK IK

     Kunci : kimisuki
   - Vigenere

     EKNDB KWCUT JKUCZ CEJGA CKWGH TIFKG UKHCH CPMKK ZMXYK CCINC IUFCC QWTIC CWMTT ASCMK MQYBG VCCEK NYSGC CU

     Kunci : kimisuki
3. Perulangan Ketiga
   - Rail fence

     EDWTU CGKHF UCPKX CNUCT CTSKY VEYCK BCJCE AWTKK HMZYC CFQIW TCMBC KSCNK UKZJC GIGHC KMKII CWCMA MQGCN GU

     Kunci : kimisuki
   - Vigenere

     OLIBM WQSRN GKHEH KXCOB UNCSI DQGUE LKTKQ IONUS RULGU WPYSE FKEVM SCKZS MEJRM OUOZW UUUQU KOWWI WYSKF AE

     Kunci : kimisuki

Untuk proses dekripsi, cukup membalikkan proses enkripsi. Lakukan vigenere decipher terlebih dahulu, kemudian lakukan rail fence ulang. Ulangi proses selama n kali.

Dari proses enkripsi di atas, diperoleh cipherteks

OLIBM WQSRN GKHEH KXCOB UNCSI DQGUE LKTKQ IONUS RULGU WPYSE FKEVM SCKZS MEJRM OUOZW UUUQU KOWWI WYSKF AE

Bandingkan dengan plainteks semula, yaitu

Karena kusuka suka dirimu
Kuakan selalu berada disini
Walau didalam keramaian
Tak apa tak kau sadari

Sedangkan dari hasil perhitungan frekuensi kemunculan huruf, bigram dan trigram diperoleh data seperti berikut.

- Frekuensi kemunculan huruf
  - A = 1 = I
  - B = 2 = II

- C = 3 = III
- D = 1 = I
- E = 6 = IIIIII
- F = 2 = II
- G = 3 = III
- H = 2 = II
- I = 4 = IIII
- J = 1 = I
- K = 8 = IIIIIIII
- L = 3 = III
- M = 4 = IIII
- N = 3 = III
- O = 6 = IIIIII
- P = 1 = I
- Q = 4 = IIII
- R = 3 = III
- S = 7 = IIIIIII
- T = 1 = I
- U = 10 = IIIIIIIIII
- V = 1 = I
- W = 6 = IIIIII
- X = 1 = I
- Y = 2 = II
- Z = 2 = II

- Frekuensi bigram
  - OL = 1 at positions 0
  - LI = 1 at positions 1
  - IB = 1 at positions 2
  - BM = 1 at positions 3
  - MW = 1 at positions 4
  - WQ = 1 at positions 5
  - QS = 1 at positions 6
  - SR = 2 at positions 7,39
  - RN = 1 at positions 8
  - NG = 1 at positions 9
  - GK = 1 at positions 10
  - KH = 1 at positions 11
  - HE = 1 at positions 12
  - EH = 1 at positions 13
  - HK = 1 at positions 14
  - KX = 1 at positions 15
  - XC = 1 at positions 16
  - CO = 1 at positions 17
  - OB = 1 at positions 18
  - BU = 1 at positions 19
  - UN = 1 at positions 20
  - NC = 1 at positions 21
  - CS = 1 at positions 22
  - SI = 1 at positions 23
  - ID = 1 at positions 24
  - DQ = 1 at positions 25
  - QG = 1 at positions 26
  - GU = 2 at positions 27,43
  - UE = 1 at positions 28
  - EL = 1 at positions 29
  - LK = 1 at positions 30
  - KT = 1 at positions 31
  - TK = 1 at positions 32
  - KQ = 1 at positions 33
  - QI = 1 at positions 34
  - IO = 1 at positions 35
  - ON = 1 at positions 36
  - NU = 1 at positions 37
  - US = 1 at positions 38
  - RU = 1 at positions 40
  - UL = 1 at positions 41
  - LG = 1 at positions 42
  - UW = 1 at positions 44
  - WP = 1 at positions 45
  - PY = 1 at positions 46
  - YS = 2 at positions 47,81
  - SE = 1 at positions 48
  - EF = 1 at positions 49
  - FK = 1 at positions 50
  - KE = 1 at positions 51
  - EV = 1 at positions 52
  - VM = 1 at positions 53
  - MS = 1 at positions 54
  - SC = 1 at positions 55
  - CK = 1 at positions 56
  - KZ = 1 at positions 57
  - ZS = 1 at positions 58
  - SM = 1 at positions 59
  - ME = 1 at positions 60
  - EJ = 1 at positions 61
  - JR = 1 at positions 62
  - RM = 1 at positions 63
  - MO = 1 at positions 64
  - OU = 1 at positions 65
  - UO = 1 at positions 66
  - OZ = 1 at positions 67
  - ZW = 1 at positions 68
  - WU = 1 at positions 69
  - UU = 1 at positions 70
  - UQ = 1 at positions 72
  - QU = 1 at positions 73
  - UK = 1 at positions 74
  - KO = 1 at positions 75
  - OW = 1 at positions 76
  - WW = 1 at positions 77
  - WI = 1 at positions 78
  - IW = 1 at positions 79
  - WY = 1 at positions 80
  - SK = 1 at positions 82
  - KF = 1 at positions 83
  - FA = 1 at positions 84
  - AE = 1 at positions 85

- Frekuensi Trigram
  - OLI = 1 at positions 0
  - LIB = 1 at positions 1
  - IBM = 1 at positions 2
  - BMW = 1 at positions 3
  - MWQ = 1 at positions 4
  - WQS = 1 at positions 5

- QSR = 1 at positions 6
- SRN = 1 at positions 7
- RNG = 1 at positions 8
- NGK = 1 at positions 9
- GKH = 1 at positions 10
- KHE = 1 at positions 11
- HEH = 1 at positions 12
- EHK = 1 at positions 13
- HKX = 1 at positions 14
- KXC = 1 at positions 15
- XCO = 1 at positions 16
- COB = 1 at positions 17
- OBU = 1 at positions 18
- BUN = 1 at positions 19
- UNC = 1 at positions 20
- NCS = 1 at positions 21
- CSI = 1 at positions 22
- SID = 1 at positions 23
- IDQ = 1 at positions 24
- DQG = 1 at positions 25
- QGU = 1 at positions 26
- GUE = 1 at positions 27
- UEL = 1 at positions 28
- ELK = 1 at positions 29
- LKT = 1 at positions 30
- KTK = 1 at positions 31
- TKQ = 1 at positions 32
- KQI = 1 at positions 33
- QIO = 1 at positions 34
- ION = 1 at positions 35
- ONU = 1 at positions 36
- NUS = 1 at positions 37
- USR = 1 at positions 38
- SRU = 1 at positions 39
- RUL = 1 at positions 40
- ULG = 1 at positions 41
- LGU = 1 at positions 42
- GUW = 1 at positions 43
- UWP = 1 at positions 44
- WPY = 1 at positions 45
- PYS = 1 at positions 46
- YSE = 1 at positions 47
- SEF = 1 at positions 48
- EFK = 1 at positions 49
- FKE = 1 at positions 50
- KEV = 1 at positions 51
- EVM = 1 at positions 52
- VMS = 1 at positions 53
- MSC = 1 at positions 54
- SCK = 1 at positions 55
- CKZ = 1 at positions 56
- KZS = 1 at positions 57
- ZSM = 1 at positions 58
- SME = 1 at positions 59
- MEJ = 1 at positions 60
- EJR = 1 at positions 61
- JRM = 1 at positions 62
- RMO = 1 at positions 63
- MOU = 1 at positions 64
- OUO = 1 at positions 65
- UOZ = 1 at positions 66
- OZW = 1 at positions 67
- ZWU = 1 at positions 68
- WUU = 1 at positions 69
- UUU = 1 at positions 70
- UUQ = 1 at positions 71
- UQU = 1 at positions 72
- QUK = 1 at positions 73
- UKO = 1 at positions 74
- KOW = 1 at positions 75
- OWW = 1 at positions 76
- WWI = 1 at positions 77
- WIW = 1 at positions 78
- IWY = 1 at positions 79
- WYS = 1 at positions 80
- YSK = 1 at positions 81
- SKF = 1 at positions 82
- KFA = 1 at positions 83
- FAE = 1 at positions 84

Pada tabel frekuensi kemunculan alfabet, dapatdilihat kemunculan huruf “U” pada cipherteks ada sebanyak 10 kali. Oleh karena panjang teks yang sedikit, dapat kita analisis kemunculan huruf “U” tersebut, mengikuti sebuah pola atau tidak.

Huruf K dapat kita lihat berkorespondensi dengan plainteks sebagai berikut.

```
cipherteks OLIBM WQSRN GKHEH KXCOB
plainteks  KAREN AKUSU KASUK ADIRI
kunci      KIMIS UKIKI MISUK IKIMI
```

Gambar 2. Plainteks, Cipherteks dan Kunci

Dapat kita lihat plainteks “A” yang dienkripsikan dengan kunci “I” menghasilkan hasil cipherteks yang berbeda, pada karakter kedua menghasilkan cipherteks L, sedagkan pada karakter keduabelas menghasilkan cipherteks K. Hal ini menunjukkan bahwa walaupun plainteks didekripsikan dengan kunci yang sama, akan tercipta cipherteks yang berbeda disebabkan oleh cipher transposisi, sehingga metode kasiski maupun metode analisis frekuensi tidak dapat digunakan untuk memecahkan algoritma ini, karena cipherteks yang sama tidak memetakan tepat satu plainteks yang sama, meskipun menggunakan kunci yang sama.

Untuk metode anagram, karena plainteks telah dienkripsi menggunakan kunci, maka penggunaan tabel anagram tidak mungkin dilakukan.

Analisis trigram dan bigram juga tidak dapat dilakukan. Satu-satunya cara yang mungkin dilakukan adalah *exhaustive key search* dan mengetahui kunci dari pesan.

V. SIMPULAN

Algoritma Heavy Rotation Cipher memiliki tingkat keamanan yang mencukupi untuk menjadi solusi algoritma klasik yang dapat mengatasi metode kasiski dan

analisis frekuensi sebagai metode pemecah algoritma substitusi. Selain itu, Heavy Rotation Cipher juga mampu mengatasi analisis anagram yang merupakan kelemahan cipher transposisi

Untuk memperoleh algoritma yang dapat mengatasi serangan terhadap algoritma substitusi, dibutuhkan kombinasi dengan algoritma transposisi. Penggabungan beberapa algoritma substitusi tidak akan mampu mengatasi serangan-serangan kriptanalis yang secara spesifik mampu memecahkan algoritma substitusi.

Penggunaan multi enkripsi akan efektif apabila digunakan dua buah algoritma dengan jenis yang berbeda, dalam algoritma Heavy Rotation ini adalah kombinasi dari substitusi dan transposisi.

Untuk menghasilkan hasil yang aman pada Heavy Rotation dari *exhaustive key search*, dibutuhkan kunci yang panjang serta tidak mudah untuk ditebak.

REFERENSI

[1] Kahn, David. The Codebreakers: The Story of Secret Writing. Rev Sub. Scribner, 1996.

[2] Yardley, Herbert. The American Black Chamber. Bobbs-Merrill, 1931.

[3] http://www.cimt.plymouth.ac.uk/resources/codes/codes_u1_text.pdf tanggal akses 5 Maret 2013

[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/Algoritma%20Kriptografi%20Klasik_bag1%20(2013).ppt Tanggal akses 5 Maret 2013

[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/Algoritma%20Kriptografi%20Klasik_bag2%20(2013).ppt

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

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, 26 Maret 2012

Ryan Rheinadi / 13508005