PENERAPAN VISUAL BASIC FOR APPLICATION (VBA) SEBAGAI ALAT BANTU AJAR ENKRIPSI DAN DEKRIPSI DES

Yasri

Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Binus University
Jl. KH. Syahdan No. 9, Palmerah, Jakarta Barat 11480.
yasri_rusli@yahoo.com

ABSTRACT

The DES encryption/decryption algorithm is quite a popular algorithm due to ease in learning. Calculations for DES using binary numbers however are very difficult, including 16 rounds required for a full encode. Teaching DES encryption manually is difficult since it requires a long time. It also requires high accuracy for the 64-bit binary numbers, the possibility of mistakes are very high. Besides, the students cannot perform self-check, whether the given task is done correctly. Application of Excel and VBA is used to facilitate observation, comparison, and understanding the DES algorithm. The result is a teaching model using DES for modern encryption.

***Keywords**: encryption, decryption, DES, VBA*

ABSTRAK

Algoritma enkripsi / Dekripsi DES adalah Algoritma yang cukup populer digunakan, sehingga kemudahan mempelajari dan memahaminya sangat perlu dilakukan. Perhitungan menggunakan angka biner sangat menyulitkan termasuk 16 ronde yang diperlukan untuk menyandikan secara lengkap. Pengajaran penyandian menggunakan DES ini mengalami kesulitan karena jika dikerjakan secara manual akan membutuhkan waktu yang sangat lama, baik karena rondenya sangat banyak yaitu 16 ronde, juga menuntut ketelitian tinggi karena dengan bilangan biner sebanyak 64 bit, kemungkinan salah menjadi sangat tinggi; dan selain itu mahasiswa tidak bisa mencek, apakah tugas yang sudah diberikan untuk meningkatkan pemahaman mereka sudah dikerjakan dengan benar. Aplikasi Excel dan VBA digunakan untuk mempermudah melihat, membandingkan dan memahami algoritma DES. Hasil penelitian berupa model pengajaran enkripsi modern menggunakan DES.

***Kata kunci**: enkripsi, dekripsi , DES, VBA*

PENDAHULUAN

Dengan segala kelebihan yang dimiliki, komputer telah digunakan dalam berbagai aspek dan segala lapisan serta umur. Sebagai alat untuk mengolah data, komputer harus dapat merahasaian data-data tertentu yang bersifat pribadi atau penting. Usaha agar data tersebut tidak mudah diakses oleh pihak yang tidak berkepentingan atau berhak sangat perlu dilakukan, salah satunya dengan penyamaran pada data menggunakan algoritma tertentu.

Sudah banyak algoritma untuk menyamarkan data dirumuskan para ahli yang tertarik dengan bidang ini. Istilah yang sering digunakan adalah enkripsi atau dalam bahasa Inggris disebut sebagai *encryption*, yaitu suatu usaha menyamarkan data agar tidak bisa diketahui orang yang tidak berhak karena rahasia, atau tidak bisa dirubah orang karena hanya orang tertentu saja yang berhak melakukan perubahan. Salah satu algoritma yang sangat sering digunakan adalah DES, suatu algoritma yang diadopsi oleh Department of Defense (DoD) Amerika Serikat. Untuk menyamarkan pesan-pesan rahasia yang sering dikomunikasikan dengan pihak-pihak yang perlu mengetahuinya.

Masalah-masalah yang muncul pada peningkatan pemahaman tentang penyandian Simple DES diantaranya: (1) Jika dikerjakan secara manual akan membutuhkan waktu yang sangat lama, baik karena rondenya sangat banyak yaitu 16 ronde, juga menuntut ketelitian tinggi karena dengan bilangan biner sebanyak 64 bit kemungkinan salah menjadi sangat tinggi; (2) Terjadi kesulitan pada dosen saat diperlukan evaluasi terhadap hasil penyandian yang telah dilakukan mahasiswa jika diberikan contoh yang beraneka ragam; (3) Kesulitan lain adalah saat membuat soal, karena sampai saat ini belum ditemukan alat bantu ajar yang bisa digunakan untuk melihat hasil enkripsi untuk tiap langkah; (4) Mahasiswa tidak bisa mencek, apakah tugas yang sudah diberikan untuk meningkatkan pemahaman mereka sudah dikerjakan dengan benar.

Data Encryption Standard (DES)

Data Encryption Standard (DES) merupakan algoritma enkripsi yang paling banyak digunakan orang. DES ini juga diadopsi oleh National Institute of Standards and Technology (NIST) sebagai pengolah informasi Federal Amerika Serikat yang Standar.

Data dienkrip per blok yang berukuran 64 bit yang nantinya akan dienkrip menggunakan kunci berukuran 56 bit. DES akan mengubah masukan sepanjang 64 bit dalam bentuk biner kedalam 16 tahap / ronde / putaran. Dengan demikian, DES termasuk algoritma penyandian yang bersifat *block cipher* (penyandian per blok, bukan per huruf). Dengan jumlah tahapan dan kunci yang sama, maka pesan yang sudah tersandi bisa dikembalikan atau didekrip agar kembali ke bentuk pesan awal yang bisa dimengerti orang.

DES sangat banyak digunakan untuk melindungi data dalam dunia elektronika khususnya di bidang perbankan, finansial dan komersial.

Sejarah DES dimulai pada tahun 60-an, saat IBM memulai riset dibidang kriptografi yang kemudian disebut dengan nama LUCIFER dan dijual kepada sebuah perusahaan di London pada tahun 1971. LUCIFER merupakan cipher block yang beroperasi pada blok masukan 64 bit dan menggunakan kunci 128 bit. Karena kunci terlalu panjang maka dikembangkan versi LUCIFER yang kuncinya lebih pendek, yakni menjadi 54 bit dengan tujuan agar bisa dimasukan kedalam satu chip, disamping untuk meningkatkan kekebalan terhadap analisis kripto.

Sementara itu, Biro Standar Amerika membutuhkan suatu algoritma yang akan digunakan secara standar untuk kepentingan negara. IBM mendaftarkan *cipher*-nya yang akhirnya dijadikan sebagai *Data Encryption Standard* (DES) pada tahun 1977.

Terdapat dua masalah dalam kasus ini, pengurangan kunci menjadi 56 membuat algoritma ini rawan terhadap serangan brute force. Masalah kedua adalah desain struktur internal DES, bagian substitusinya (S-BOX), masih dirahasiakan. S-BOX ini diubah mengikuti saran NSA, akibatnya sulit meyakini struktur ini bebas dari titik lemah yang mungkin sudah ditemukan NSA.

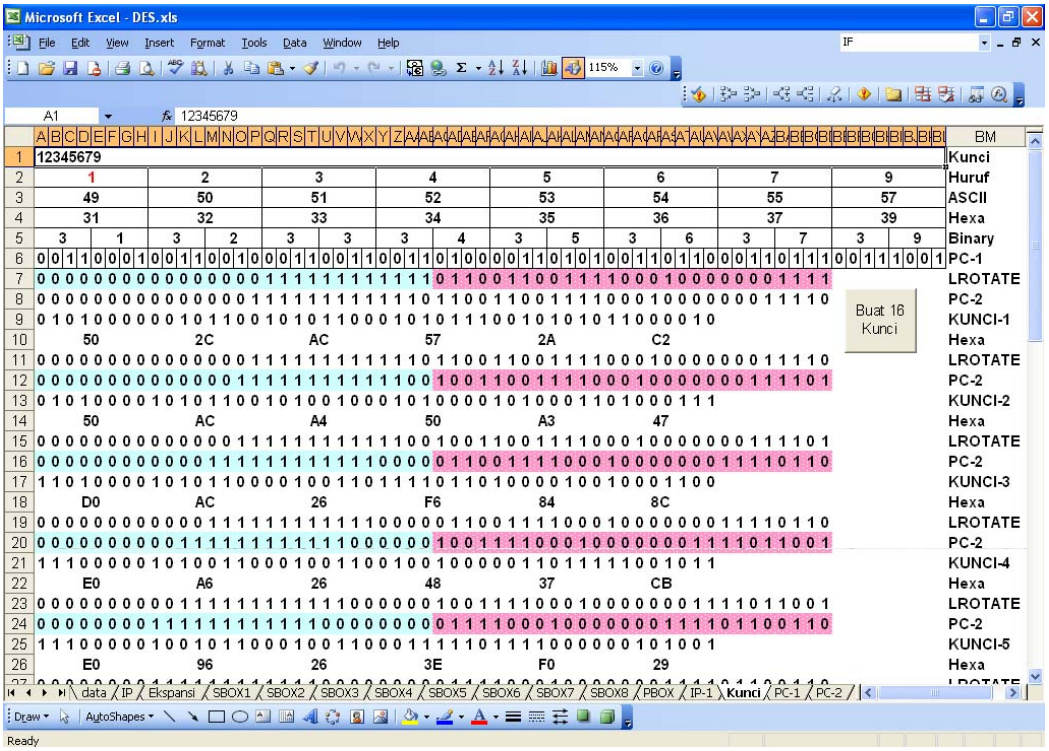
Menurut ahli Kriptologi, DES sudah disusun dengan cermat sehingga pengubahan pada S-BOX akan memperlemah keamanan DES. Hingga kini, tampaknya DES masih kebal terhadap *cryptanalysis* baik yang berjenis *differential* maupun berjenis *linear*, dua teknik yang dikenal sebagai cara yang paling ampuh untuk memecahkan sandi moderen.

METODE

Untuk mewujudkan aplikasi alat bantu ajar ini, dilakukan tahapan-tahapan sebagai berikut: (1)Studi literatur di perpustakaan dan pencarian data dan informasi di internet mengenai perkembangan fungsi-fungsi yang ada pada Excel dan Visual Basic for Application (VBA) yang akan menunjang pembuatan aplikasi; (2) Akan ditentukan fungsi-fungsi apa saja yang akan digunakan sehubungan dengan proses yang harus dilakukan saat melakukan penyandian sebuah pesan sebanyak 64 bit; (3) Pembuatan alur logika sesuai kaidah enkripsi simple DES menggunakan fungsi-fungsi yang sesuai; (4) Membuat prototipe penyandian untuk 1 ronde; (5) Melakukan pengujian dengan cara membandingkan hasil yang diperoleh dengan menggunakan prototipe terhadap hasil manual dan hasil dari contoh-contoh perhitungan yang sudah ada, yang diperoleh saat melakukan pencaian data di buku dan Internet, Jika ada penyimpangan akan segera diperbaki untuk kemudian dilakukan pembandingan ulang sampai diperoleh hasil yang benar; (6) Melengkapi aplikasi untuk 16 ronde yang sudah disyaratkan oleh *Simple* DES; dan (7) Melakukan pengujian terintegrasi untuk mengetahui apakah hasil akhir yang diperoleh menggunakan aplikasi ini sudah benar dengan cara membandingkannya data-data contoh yang bisa diproleh dari internet serta contoh contoh hasil keluaran program-program enkripsi yang sudah dibuat oleh pihak lain. Perbandingan secara manual tidak dilakukan karena akan memakan waktu dan kurang valid karena tingkat kesalahan akan tinggi jika dihitung sampai 16 ronde.

HASIL DAN PEMBAHASAN

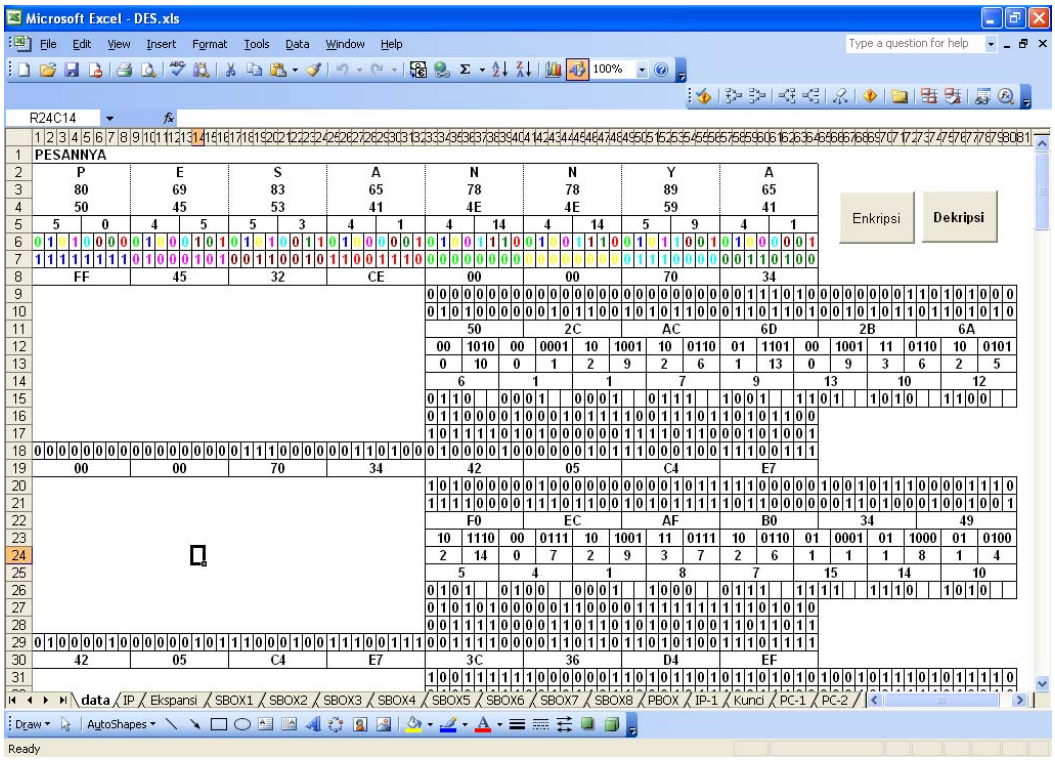
Langkah pertama yang dilakukan untuk menyandikan data masukan adalah mendapatkan kunci ronde 1 dengan langkah- langkah sebagai berikut: (1) Mengubah tiap huruf yang ada pada kunci ke bentuk heksadesimal; (2) Mengubah bentuk heksadesimal ke bentuk biner, dimana tiap huruf heksadesimal berubah menjadi 4 bit biner; (3) Menggunakan Tabel PC-1 untuk mengubah susunan urutan kunci dalam bentuk Biner dan hanya diambil sebanyak 56 bit; (4) Membagi dua hasil PC-1 dan mengelompokkan yang pertama sebagai C_0 dan yang kedua sebagai D_0; (5) Memutar kedua bagian, yakni C_0 dan D_0 ke kiri sesuai aturan yang ada pada ronde yang ada pada *Key Schedule*. Hasilnya disebut C_1 dan D_1; (6) Gabungkan C_1 dan D_1 , lalu gunakan Tabel PC-2 untuk mengacak hasil pemutaran data pada kedua bagian, data yang diambil dari 28x2 ini hanya 48 bit. Dan ini disebut sebagai kunci ronde 1; (7) Ulangi langkah langkah dari e. sampai f. sebanyak 16 kali untuk 16 ronde. Pada Microsoft Excel, tampilan *sheet* yang digunakan untuk memproses kunci akan terlihat seperti pada Gambar 1.



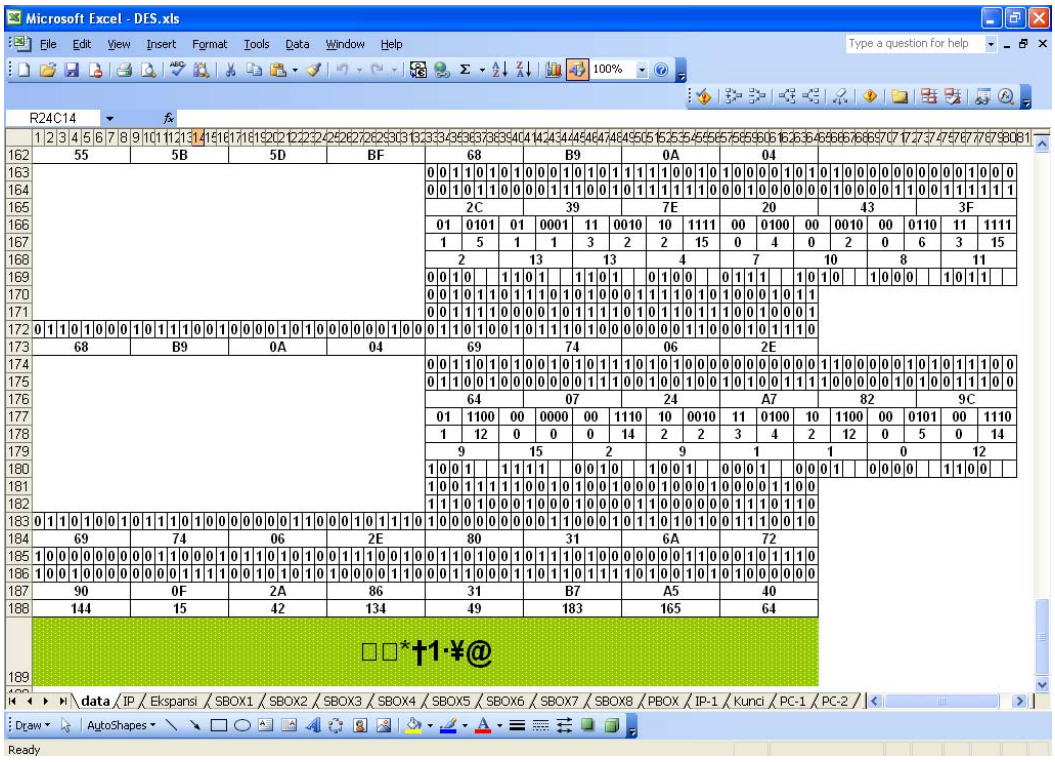
Gambar 1. Screen capture untuk pembuatan kunci.

Sedangkan data yang akan di-enkripsi akan mengalami perubahan perubahan sebagai berikut: (1) Mengubah tiap huruf yang ada pada data ke bentuk heksadesimal; (2) Mengubah bentuk heksadesimal ke bentuk biner, dimana tiap huruf heksadesimal berubah menjadi 4 bit biner; (3) Menggunakan Tabel IP untuk mengubah susunan urutan data dalam bentuk Biner sebanyak 56 bit; (4) Membagi 2 hasil IP dan mengelompokkan yang pertama sebagai L_0 dan yang kedua sebagai R_0; (5) Karena akan dilakukan operasi XOR antara data bagian Kanan atau R_0, sementara R_0 hanya 32 bit sedangkan kunci berjumlah 48 bit, R_0 dimekarkan menggunakan Tabel Ekspansi menjadi 48 bit; (6) Lakukan operasi XOR antara hasil ekspansi R_0 dengan kunci. Proses ini akan menghasilkan data sebanyak 48 bit; (7) Bagi hasil langkah f menjadi 8 kelompok sehingga didapatkan 6 bit untuk tiap kelompok, lalu gunakan tabel S-BOX; (8) Lakukan permutasi pada data hasil operasi nomor 7 menggunakan table P-BOX; (9) Lakukan operasi XOR pada data terakhir dengan L_0 yang diperoleh sebagai hasil proses langkah 4. Proses ini menghasilkan data tersandi ronde 1; (10) Ulangi langkah langkah dari 5 sampai 6 sebanyak 16 kali untuk 16 ronde. Pada Microsoft Excel, tampilan pada sheet yang memproses kunci akan terlihat seperti pada Gambar 2 dan 3.

Jika proses enkripsi lengkap sampai 16 ronde, akan diperoleh hasil enkripsi dalam bentuk Cipher Text yang akan sulit dipecahkan para penyerang. Hasil akhir dapat dilihat pada gambar 3, dimana hasil ini bisa dikirim menggunakan berbagai media pengiriman data. Baik berupa email, surat atau bentuk lainnya. Tabel-tabel yang harus digunakan saat melakukan enkripsi dimasukan ke dalam Excel secara linier. Ini bisa dilihat pada bagian bawah tiap sheet, akan ada sheet yang berisi semua tabel yang dibutuhkan selama proses enkripsi sebanyak 16 ronde.

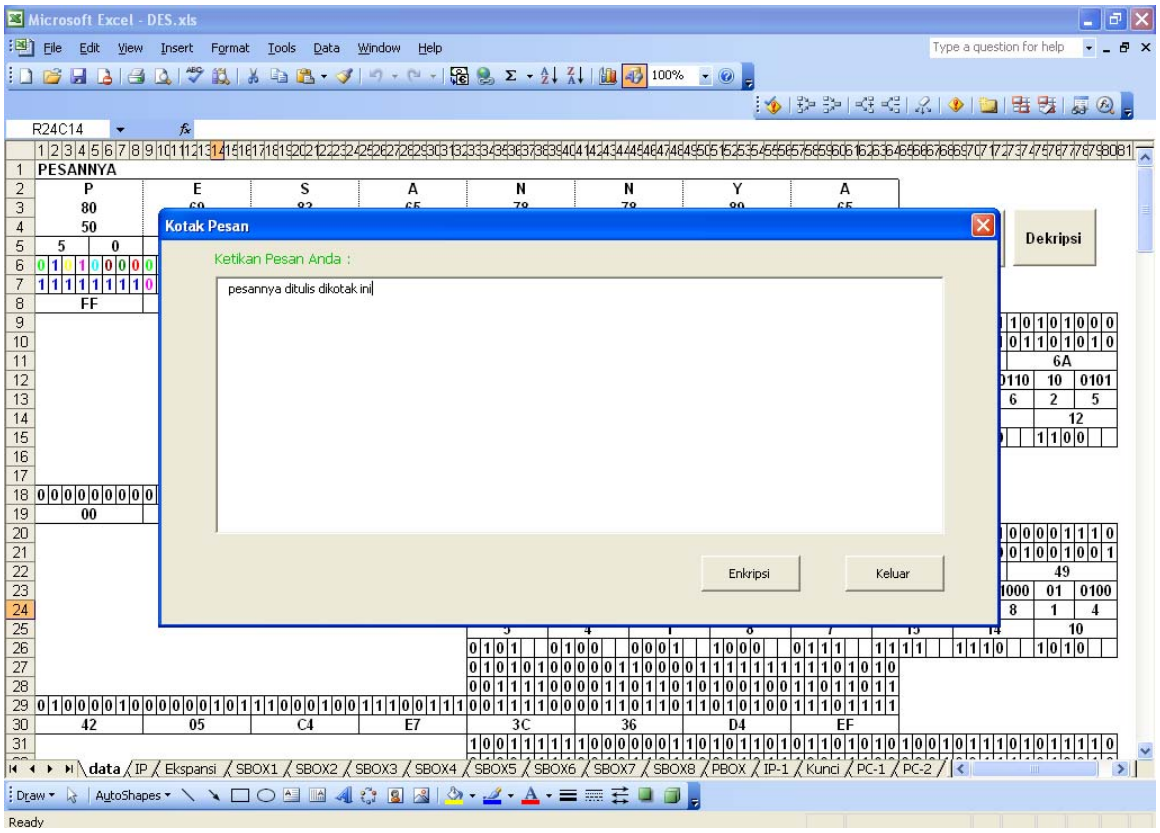


Gambar 2. Screen capture untuk enkripsi ronde 1.

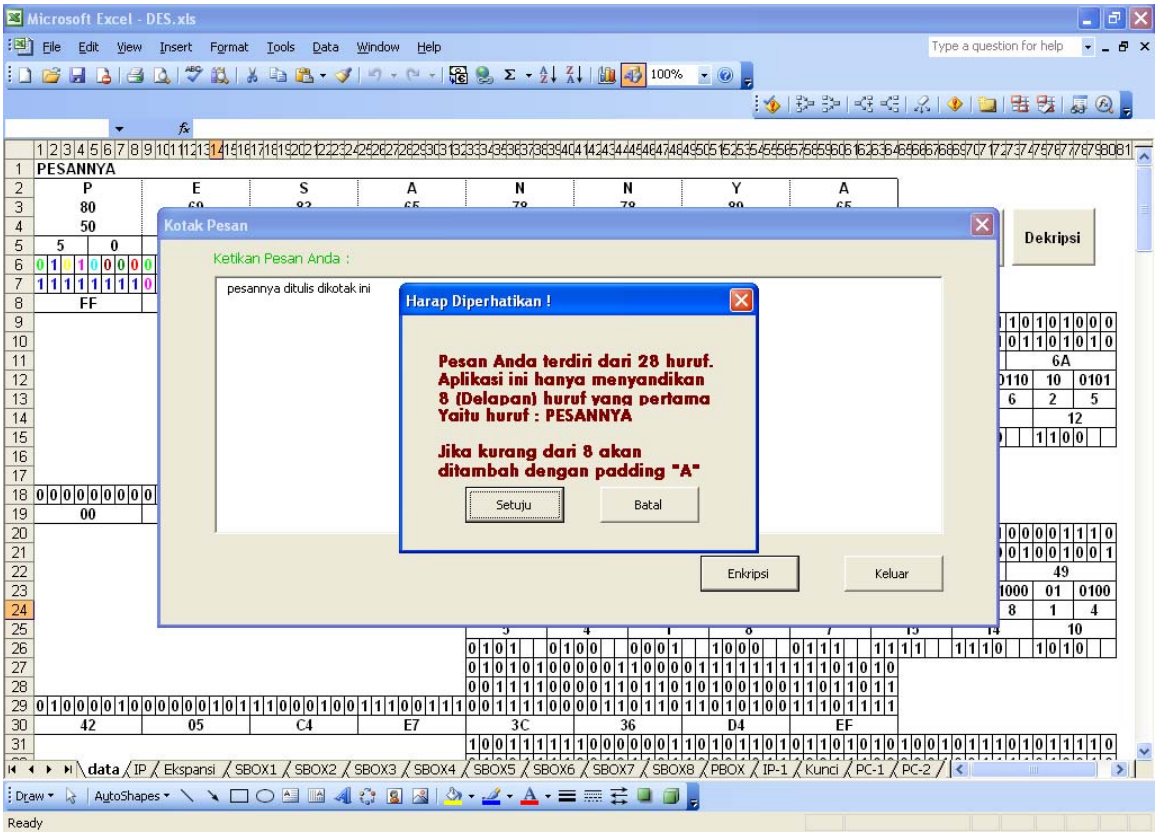


Gambar 3. Screen capture untuk 16 ronde proses enkripsi.

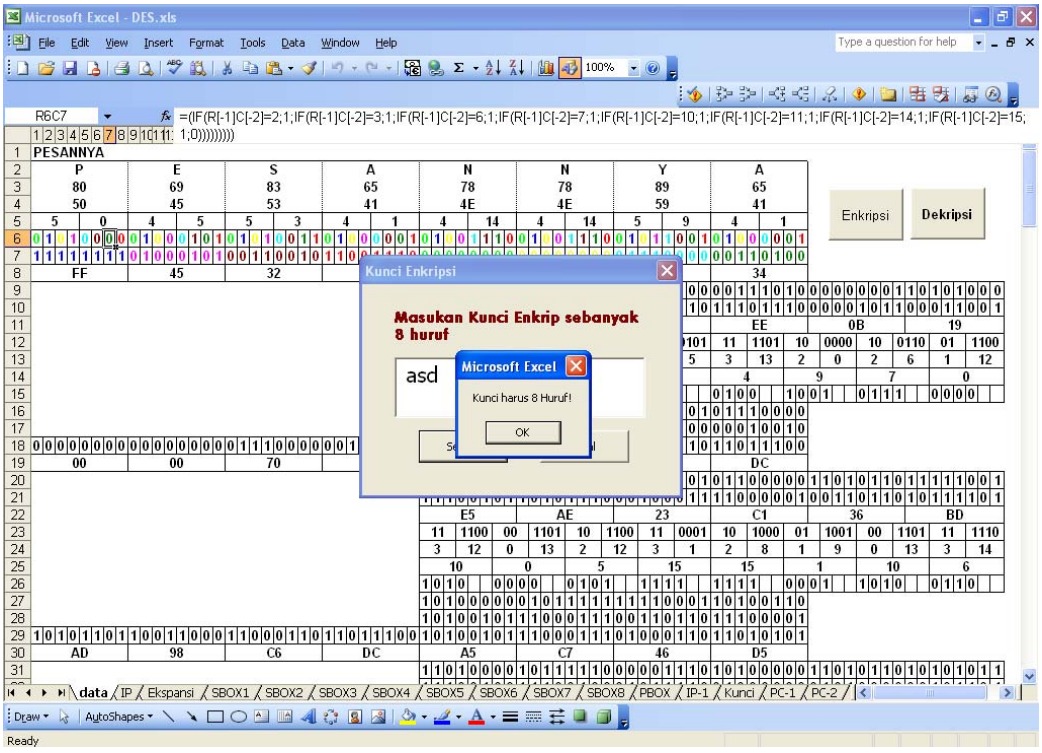
Penggunaan aplikasi ini sudah disederhanakan agar tidak terlalu rumit dipahami sesuai dengan delapan aturan emas perancangan IMK. Langkah pertama adalah menekan tombol enkripsi pada Sheet data (Gambar 4). Pada langkah ini akan diminta pesan yang akan di-enkripsi. Akan ada pesan yang menyatakan bahwa pesan hanya akan dienkripsi sebanyak delapan huruf karena ini adalah enkripsi per blok. Jika pesan yang dimasukkan kurang, akan ditambah padding ”A”. Ini hanya untuk melengkapi delapan huruf sebelum di-enkripsi. Untuk data yang sebenarnya, hal ini tidak perlu dilakukan karena spasipun bisa diproses. Hanya agar perubahan perubahan hasil enkripsi bisa terlihat, maka aplikasi ini tetap mensyaratkan delapan huruf untuk memulai proses enkripsi. Hasilnya dapat dilihat pada Gambar 5. Sedangkan untuk kunci, pengguna harus memasukkan sebanyak delapan huruf. Aplikasi tidak akan memberi toleransi dengan menambah padding atau mengambil hanya sebanyak delapan huruf saja karena pada akhirnya pengguna memang harus mengingat kunci sebanyak delapan huruf. Tidak boleh lebih atau kurang. Jika terjadi kesalahan dalam memasukkan jumlah kunci, aplikasi akan memunculkan pesan seperti yang terlihat pada Gambar 6.



Gambar 4. Screen capture untuk memulai proses enkripsi.

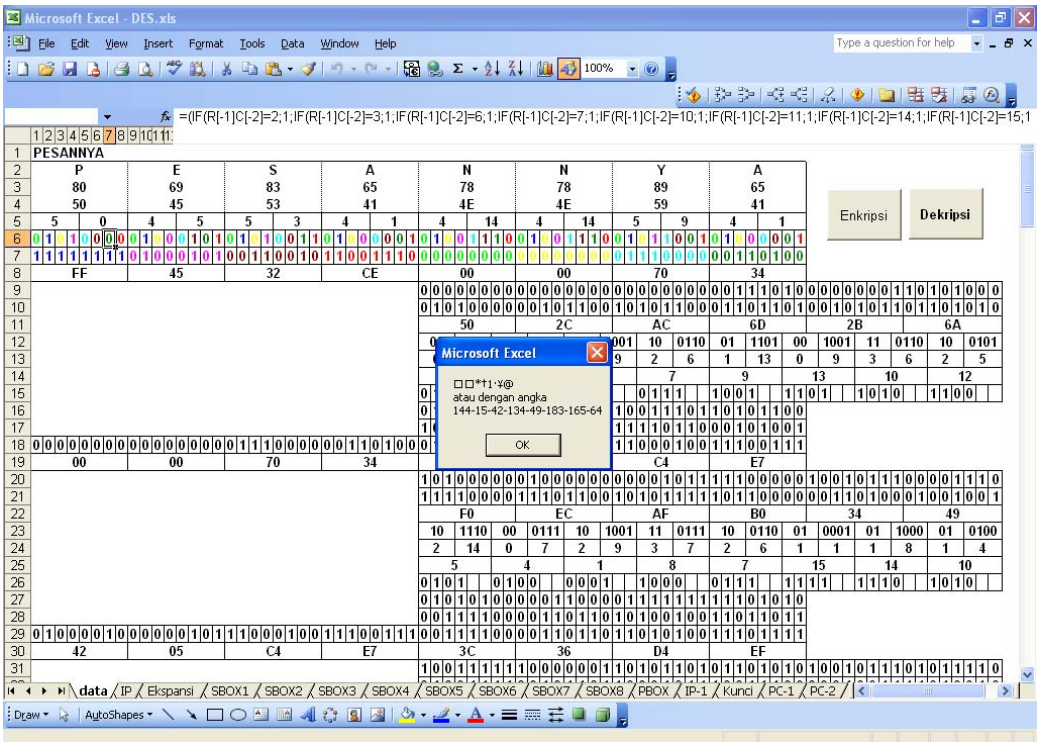


Gambar 5. Screen capture untuk memberitahu bahwa data yang dienkripsi hanya 8 huruf.



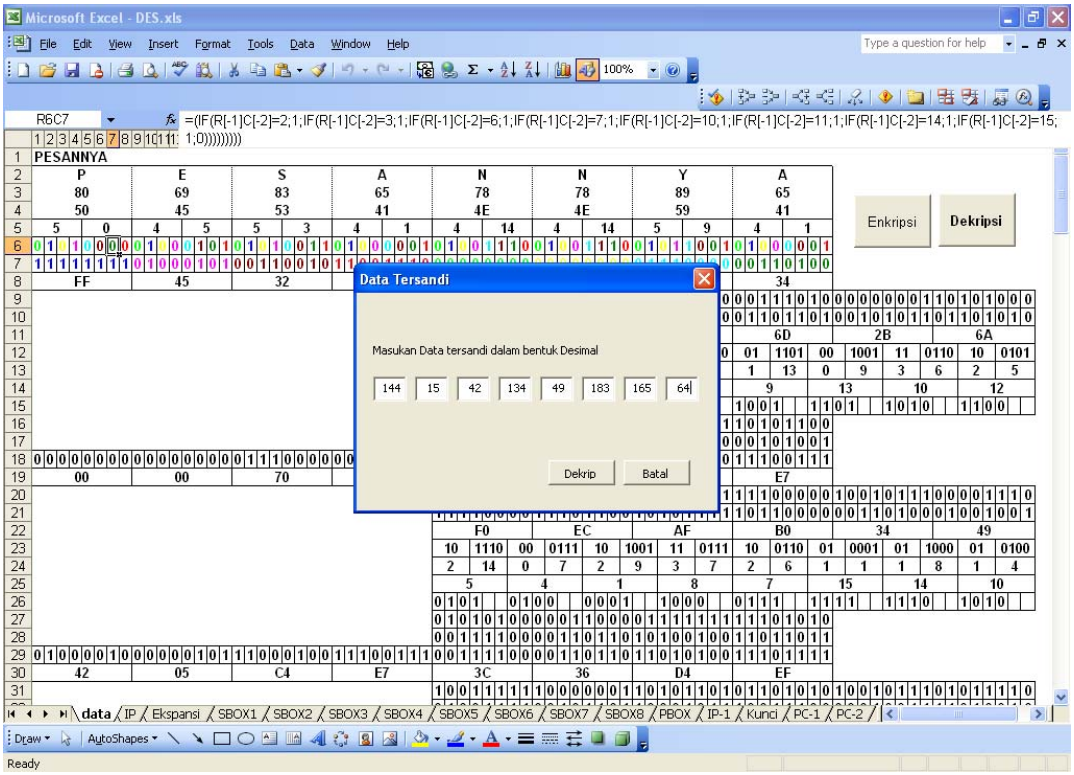
Gambar 6. Screen capture untuk pesan jika kunci bukan 8 huruf.

Jika semua proses pemasukan data dan kunci selesai dilaksanakan, maka aplikasi akan memproses semua data dengan megubah bit bit yang bersesuaian pada cell yang ada pada Excel. Hasilnya dapat dilihat pada Gambar 7. Akan diberikan dua bentuk *cipher*, yaitu bentuk ASCII dan bentuk desimalnya. Ini dilakukan karena keterbatasan Microsoft Excel, maka beberapa data yang sama tetap akan ditampilkan dalam bentuk seperti yang juga terlihat pada Gambar 8. Nilai 144 dan 15 mempunyai bentuk yang sama yaitu . Banyak lagi bilangan yang akan ditampilkan berbentuk tersebut.

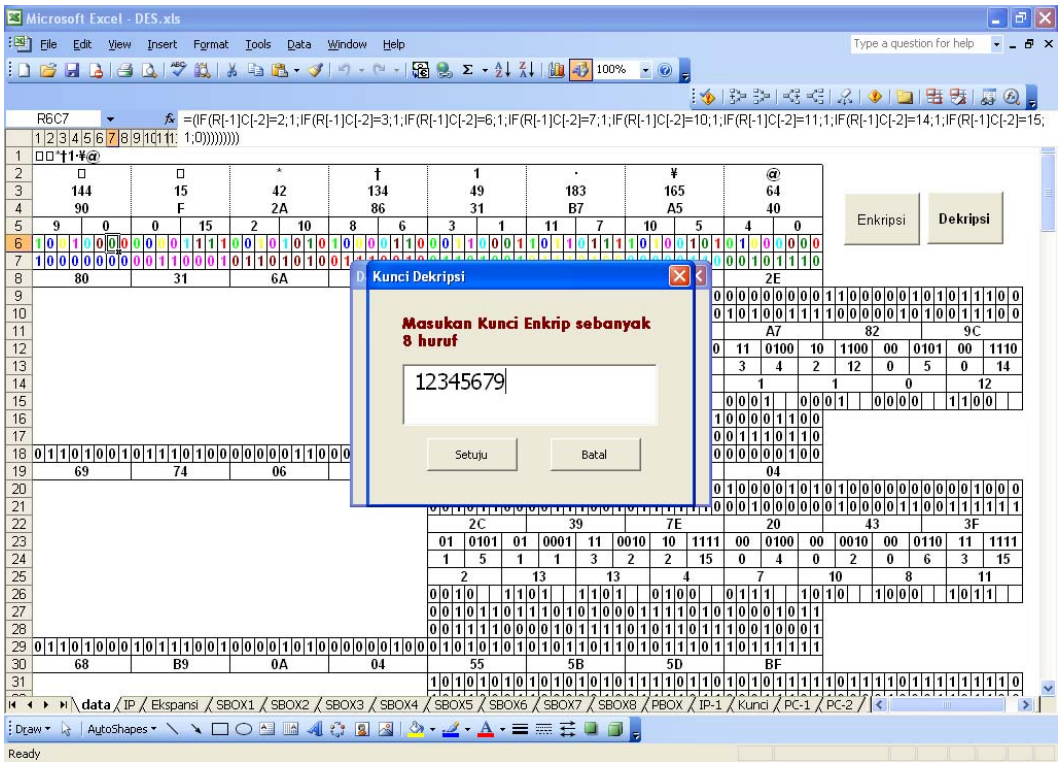


Gambar 8. Screen capture untuk hasil akhir proses enkripsi.

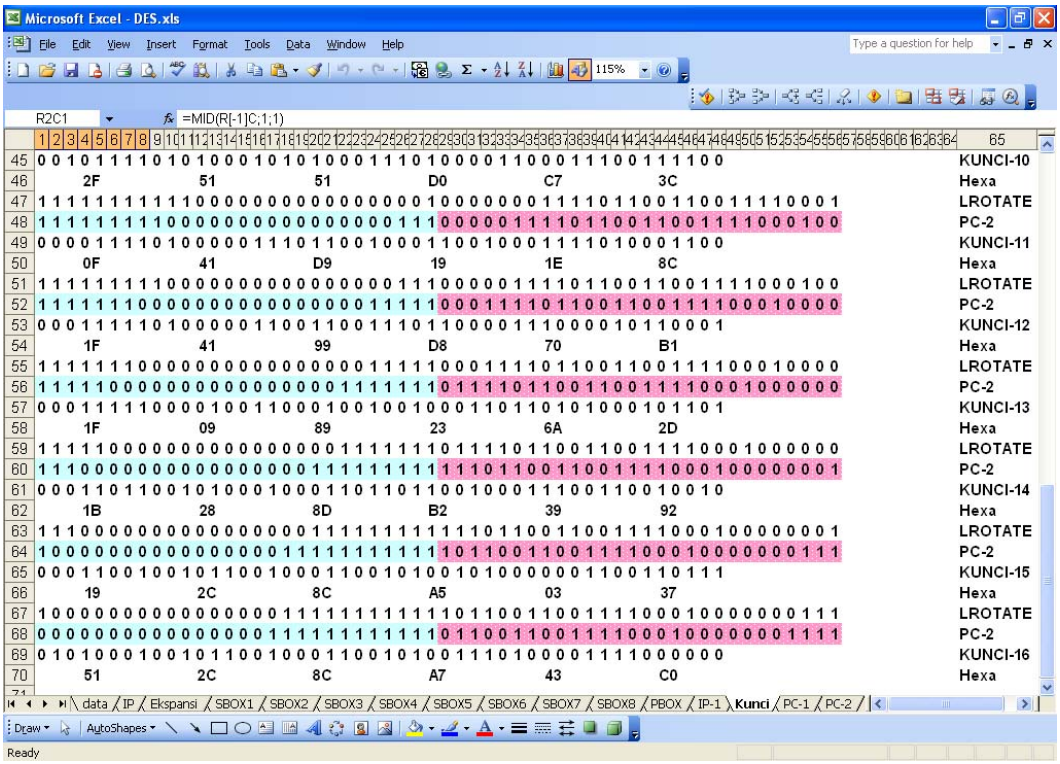
Aplikasi ini juga dilengkapi dengan proses Dekripsi untuk mengubah pesan tersandi Ciphertext ke bentuk normal (Plain text). Untuk itu, pengguna harus menekan tombol dekripsi. Penekanan tombol ini akan memunculkan pesan untuk memasukkan nilai cipher dalam bentuk desimal. Ini dilakukan karena timbul kesulitan untuk memasukkan bentuk bentuk huruf yang tidak ada pada keyboard. Ini bisa dilihat pada kotak pesan yang terlihat pada Gambar 9. Selanjutnya akan ditunjukkan kotak pesan yang akan meminta kunci untuk mendekrip pesan cipher text. Pesan ini dalam bentuk normal karena asumsi bahwa pengguna akan menggunakan huruf huruf yang ada pada keyboard. Bentuknya dapat dilihat pada Gambar 10. Sedangkan kunci yang dihasilkan pada ronde 10 sampai ronde 16 dapat dilihat pada Gambar 11 dan 12.



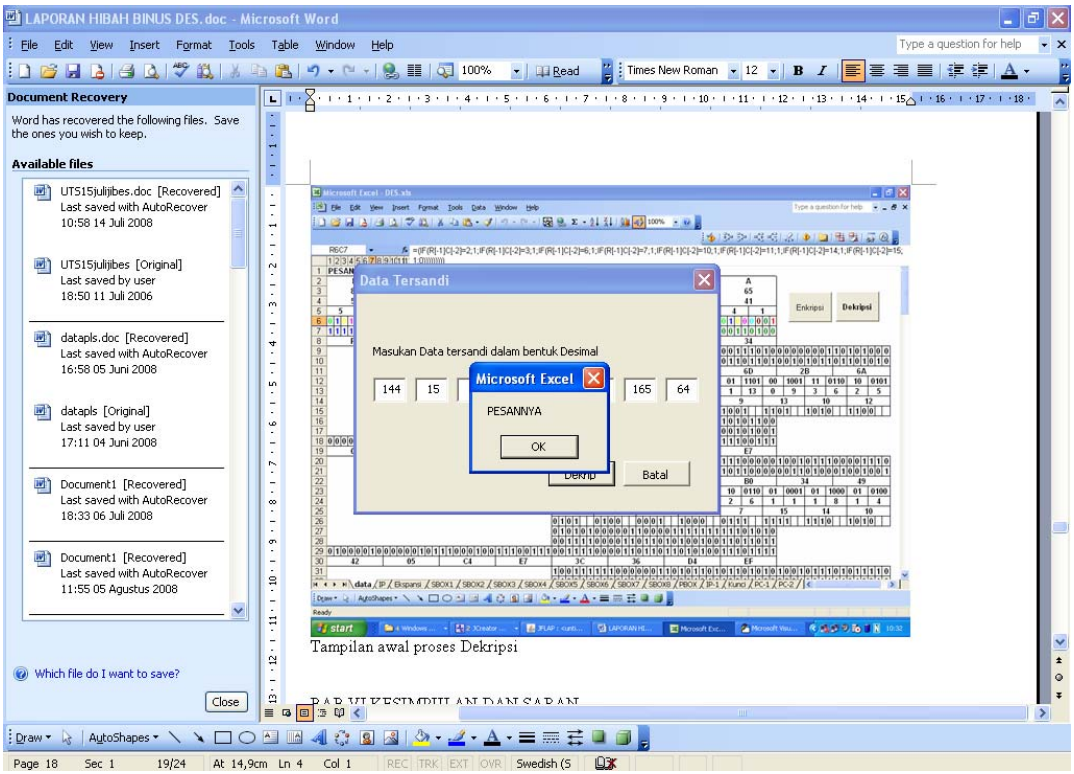
Gambar 9. Screen capture untuk tampilan awal proses dekripsi.



Gambar 10. Screen capture untuk memasukan kunci dekripsi.

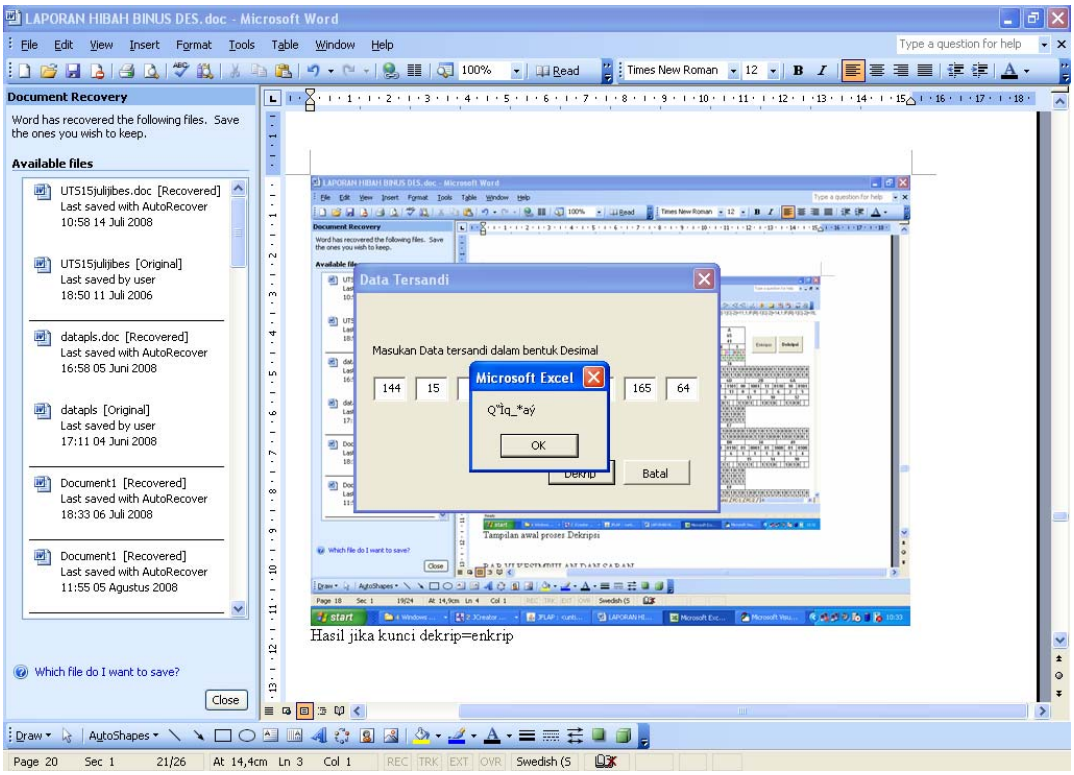


Gambar 11. Screen capture untuk kunci Dekrip 12345679 ronde 10-16



Gambar 12. Screen capture untuk hasil jika kunci dekrip sama dengan enkrip.

Jika pengguna memasukan kunci yang berbeda dengan kunci saat mendekripsi pesan, maka aplkasi akan menghasilkan plain Text yang berbeda. Ini terlihat pada Gambar 13.



Gambar 13. Screen capture untuk hasil jika kunci dekrip tidak sama dengan enkrip.

Untuk mengetahui kebenaran logika dari aplikasi ini maka telah dilakukan pencarian pada Google untuk mendapakan contoh contoh enkripsi dan dekripsi menggunakan DES. Hasil perbandingan proses pengujian dapat dilihat pada penjelasan berikut ini.

Contoh DES dari Katzan (1977):
Kunci : 5B5A57676A56676E (Tabel 1)
Plaintext : 675A69675E5A6B5A (Tabel 2)
Ciphertext : 974AFFBF86022D1F (Tabel 3)

Untuk menguji data diatas menggunakan aplikasi yang sudah dibuat, bentuk heksa dari kunci tersebut harus dirubah dulu ke bentuk ASCII sehingga bentuk kunci berubah menjadi bentuk berikut, dimana baris pertama adalah huruf atau karakternya, sedangkan baris kedua adalah ASCII dari karakter diatasnya dalam bentuk desimal. Baris terakhir adalah bentuk heksa dari baris kedua atau bentuk heksa dari ASCII untuk karakter yang ada pada baris pertama.

Tabel 1
Kunci: 585A57676A56676E

[	**Z**	**W**	**g**	**J**	**V**	**g**	**n**
91	**90**	**87**	**103**	**106**	**86**	**103**	**110**
5B	**5A**	**57**	**67**	**6A**	**56**	**67**	**6E**

Sedangkan Pesan, atau yang lebih sering disebut sebagai *Plain Text* yang akan dirahasiakan dan akan dikirim menggunakan media transmisi yang tidak aman berubah menjadi bentuk berikut.

Tabel 2
Plaintext: 675A69675E5A6B5A

G	**Z**	**i**	**g**	**^**	**Z**	**k**	**Z**
103	**90**	**105**	**103**	**94**	**90**	**107**	**90**
67	**5A**	**69**	**67**	**5E**	**5A**	**6B**	**5A**

Setelah mengalami proses penyandian sebanyak 16 ronde, *Plain Text* akan berubah menjadi bentuk berikut, dimana baris pertama adalah bentuk heksa, sebagai hasil dari proses penyandian huruf-huruf atau karakter-karakter dari Pesannya, sedangkan baris kedua adalah bentuk desimal dari bilangan heksa diatasnya. Baris terakhir adalah bentuk huruf dari ASCII untuk bilangan heksa yang ada pada baris pertama.

Tabel 3
Ciphertext: 974AFFBF86022D1F

97	**4A**	**FF**	**BF**	**86**	**02**	**2D**	**1F**
151	**74**	**255**	**191**	**134**	**2**	**45**	**31**
—Jÿ¿† -							

Jika menggunakan aplikasi yang banyak tersedia di internet yang juga telah diuji silang dengan data-data yang lain, akan diperoleh hasil pengujian sebagai berikut ini.

Hasil pertama untuk kunci: PASSWORD dan data: PESANAKU
setKey(50415353574f5244) atau bentuk hurufnya PASSWORD
encryptDES(504553414e414b55) atau bentuk hurufnya PESANAKU

IP: L0=ff8592ee, R0=00005054
Rnd1 f(R0=00005054, SK1=28 09 09 0a 19 22 09 27) = 44c8f036
Rnd2 f(R1=bb4d62d8, SK2=2c 01 0b 12 1c 2c 04 03) = 311f24b4
Rnd3 f(R2=311f74e0, SK3=0d 05 09 10 11 22 14 0e) = b6115fcd
Rnd4 f(R3=0d5c3d15, SK4=01 25 05 14 3b 03 07 08) = 8a7ad809
Rnd5 f(R4=bb65ace9, SK5=03 24 05 15 18 0d 09 2b) = cae378f7
Rnd6 f(R5=c7bf45e2, SK6=03 34 04 29 15 29 30 2a) = 3c25d97f
Rnd7 f(R6=87407596, SK7=22 30 06 29 23 01 35 38) = 52dac4f0
Rnd8 f(R7=95658112, SK8=26 10 2a 09 02 1f 29 30) = e3a37167
Rnd9 f(R8=64e304f1, SK9=0e 10 22 0a 32 04 29 29) = f6172c57
Rnd10 f(R9=6372ad45, SK10=0c 02 22 0c 24 2d 28 1c) = 0c7fa1ec
Rnd11 f(R10=689ca51d, SK11=04 02 30 14 24 11 1e 30) = bb26bde4
Rnd12 f(R11=d85410a1, SK12=11 02 30 34 26 12 28 21) = 3a2a9b0d
Rnd13 f(R12=52b63e10, SK13=31 2a 10 24 1c 26 28 14) = 6b2b251c
Rnd14 f(R13=b37f35bd, SK14=32 28 18 22 0c 12 06 1e) = 2fa6903f
Rnd15 f(R14=7d10ae2f, SK15=3a 09 08 2a 29 13 02 03) = ced1bd5c

Rnd16 f(R15=7dae88e1, SK16=28 19 0a 22 0e 32 0f 01) = 4a6fbdf0
FP: L=d775f1b9, R=d5f2932b
returns d775f1b9d5f2932b

Sedangkan hasil enkripsi terhadap data contoh yang diberikan menggunakan Aplikasi Excel yang sudah dibuat terlihat pada Tabel 4.

Tabel 4
Hasil Enkripsi Pertama

D7	**75**	**F1**	**B9**	**D5**	**F2**	**93**	**2B**
215	**117**	**241**	**185**	**213**	**242**	**147**	**43**
×uñ¹Õò“+							

Hasil kedua untuk kunci: PENGUNCI dan data: PESANAKU
setKey(50454e47554e4349) atau bentuk hurufnya PENGUNCI
encryptDES(504553414e444941) atau bentuk hurufnya PESANAKU

IP: L0=ff0532ce, R0=00005014
Rnd1 f(R0=00005014, SK1=28 09 09 0a 21 32 38 33) = 5fdef0be
Rnd2 f(R1=a0dbc270, SK2=28 01 0b 12 2c 15 0c 03) = 6e2acc9b
Rnd3 f(R2=6e2a9c8f, SK3=0d 05 09 10 35 20 08 26) = ed438df4
Rnd4 f(R3=4d984f84, SK4=01 25 05 10 35 02 2f 0c) = 48796750
Rnd5 f(R4=2653fbdf, SK5=03 24 05 15 0c 0b 0b 19) = f12e2fa5
Rnd6 f(R5=bcb66021, SK6=03 34 04 09 1c 3b 10 23) = 078b0923
Rnd7 f(R6=21d8f2fc, SK7=02 30 06 29 0b 22 34 2a) = e97408d6
Rnd8 f(R7=55c268f7, SK8=26 10 22 09 0b 07 25 16) = 28834e3a
Rnd9 f(R8=095bbcc6, SK9=06 10 22 0a 33 20 25 21) = 0e44c404
Rnd10 f(R9=5b86acf3, SK10=0c 02 22 0c 30 2e 2d 18) = cf357358
Rnd11 f(R10=c66ecf9e, SK11=04 02 30 04 1c 19 1c 18) = 9a3224bc
Rnd12 f(R11=c1b4884f, SK12=10 02 30 34 36 11 10 2a) = 78e5ddc6
Rnd13 f(R12=be8b1258, SK13=31 0a 10 24 13 07 28 2c) = 8ead2d91
Rnd14 f(R13=4f19a5de, SK14=30 28 18 22 0c 07 23 3c) = 4eb51ab8
Rnd15 f(R14=f03e08e0, SK15=3a 09 08 22 28 19 22 33) = f0c2f764
Rnd16 f(R15=bfdb52ba, SK16=28 19 08 22 2a 36 0e 18) = 4c89e5c6
FP: L=b4bbd5e6, R=fad72cf6
returns b4bbd5e6fad72cf6

Sedangkan hasil enkripsi terhadap data contoh yang diberikan menggunakan Aplikasi Excel yang sudah dibuat terlihat pada Tabel 5.

Tabel 5
Hasil Enkripsi Kedua

B4	**BB**	**D5**	**E6**	**FA**	**D7**	**2C**	**F6**
180	**187**	**213**	**230**	**250**	**215**	**44**	**246**
´»Õæú×,ö							

Hasil ketiga untuk kunci: PENYAMAR dan data: PESANNYA
setKey(50454e59414d4152) atau bentuk hurufnya PENYAMAR
encryptDES(504553414e4e5941) atau bentuk hurufnya PESANNYA

```
 IP:          L0=ff4532ce, R0=00007034
 Rnd1  f(R0=00007034, SK1=2c 09 09 02 31 03 14 30 ) = e4387af5
 Rnd2  f(R1=1b7d483b, SK2=28 01 29 12 27 1d 00 01 ) = 121d37d4
 Rnd3  f(R2=121d47e0, SK3=09 07 09 10 10 24 19 20 ) = 865e2aed
 Rnd4  f(R3=9d2362d6, SK4=01 25 15 10 26 0a 24 0c ) = 81837698
 Rnd5  f(R4=939e3178, SK5=13 24 05 11 28 05 1a 10 ) = 910b5158
 Rnd6  f(R5=0c28338e, SK6=03 3c 04 09 16 12 08 23 ) = cd13ed11
 Rnd7  f(R6=5e8ddc69, SK7=02 30 06 0b 2d 24 20 08 ) = a10da58d
 Rnd8  f(R7=ad259603, SK8=0e 10 22 09 00 03 0d 16 ) = fb295164
 Rnd9  f(R8=a5a48d0d, SK9=06 11 22 08 33 00 06 11 ) = 8ca3b8ed
 Rnd10 f(R9=21862eee, SK10=04 02 23 0c 00 36 09 0d ) = cac0f3a9
 Rnd11 f(R10=6f647ea4, SK11=04 06 30 04 1c 29 06 00 ) = 80baa275
 Rnd12 f(R11=a13c8c9b, SK12=10 02 34 24 20 00 14 2f ) = 42dcdff0
 Rnd13 f(R12=2db8a154, SK13=30 0a 10 25 13 23 2a 00 ) = 091c0a5a
 Rnd14 f(R13=a82086c1, SK14=30 18 18 22 1c 04 05 39 ) = e162badf
 Rnd15 f(R14=ccda1b8b, SK15=38 09 0a 22 00 39 20 0a ) = b9185c85
 Rnd16 f(R15=1138da44, SK16=28 09 08 22 02 00 1f 1a ) = ec59da9d
 FP:          L=94190328, R=a9600e1c
returns  94190328a9600e1c
```

Sedangkan hasil enkripsi terhadap data contoh yang diberikan menggunakan Aplikasi Excel yang sudah dibuat terlihat pada Tabel 6.

Tabel 6
Hasil Data Ketiga

94	**19**	**03**	**28**	**A9**	**60**	**0E**	**1C**
148	**25**	**3**	**40**	**169**	**96**	**14**	**28**

” (©`

PENUTUP

Dengan selesainya penelitian ini dapat ditarik beberapa kesimpulan, yaitu (1) usaha untuk mempermudah pemahaman algoritma enkripsi moderen ini perlu dilakukan; (2) Excel membantu mempermudah dalam menyandikan pesan pesan sebanyak 64 bit (8 huruf) dengan baik; (3) aplikasi yang dibuat mampu menunjukkan bentuk-bentuk biner dan heksadesimal dari enkripsi dan dekripsi; dan (4) aplikasi dibuat sederhana agar mudah digunakan oleh semua pihak yang berminat mengetahui konsep dan cara kerja enkripsi dan dekripsi DES.

Untuk penyempurnaan hasil penelitian ini maka disarankan untuk: (1) mengembangkan aplikasi untuk algoritma enkripsi lain, misalnya AES karena kelebihan yang dimiliki Excel akan mampu melakukannya; (2) mengembangkan fungsi yang akan mengubah hasil enkripsi jika data dimasukkan dipertengahan ronde sehingga nilai nilai yang ada diatas dan dibawahnya menjadi berubah sesuai aturan DES; dan menempatkan tombol enkripsi dan Dekripsi pada toolbar dengan cara mengkustomisasi icon dengan mengisi macro yang sudah dibuat sehingga lebih variatif.

DAFTAR PUSTAKA

Katzan, H. (1977). *The Standard Data Encryption Algorithm*. New York: Petrocelli Books.

Kurniawan, Y. (2004) *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.