|  |
| --- |
|  |
| Dasar-Dasar DES |
| Data Encryption Standard |
|  |
| **Edho Prima Arief (10104001)** |
| **10/17/2008** |

|  |
| --- |
| Tugas artikel kedua dari mata kuliah Kriptografi. |

Contents

[Sejarah Singkat 3](#_Toc212226116)

[Perkenalan 3](#_Toc212226117)

[Enkripsi 4](#_Toc212226118)

[Dekripsi 6](#_Toc212226119)

[Fungsi sandi 7](#_Toc212226120)

[Tabel yang Dianjurkan 9](#_Toc212226121)

[Fungsi kunci 10](#_Toc212226122)

[Kriptanalisis 12](#_Toc212226123)

[Referensi 12](#_Toc212226124)

# Sejarah Singkat

*Data Encryption Standard* merupakan salah satu sistem kripto yang dipilih oleh NBS (institut untuk standar dan teknologi nasional di Amerika Serikat) sebagai FIPS (standar pemrosesan informasi federal) pada tahun 1976 dan banyak digunakan di berbagai negara. Algoritma yang digunakan pada awalnya dipermasalahkan karena penggunaan elemen desain yang dirahasiakan, panjang kunci yang relatif pendek, dan kecurigaan terhadap kemungkinan penyadapan oleh NSA (agen keamanan nasional). DES kemudian dipelajari secara mendalam di berbagai universitas yang kemudian memotivasi pendalaman mengenai *block cipher* dan kriptanalisis secara modern.

Pada masa ini DES dianggap sudah tidak aman untuk berbagai aplikasi. Hal tersebut disebabkan terutama oleh penggunaan kunci sepanjang 56-bit yang dianggap terlalu kecil. Pada Januari 1999, *distributed.net* dan *Electronic Frontier Foundation* bekerja sama memecahkan sebuah kunci DES dan selesai dalam waktu 22 jam 15 menit. Terdapat juga sejumlah hasil analisis yang menunjukkan kelemahan dari sistem kripto ini meskipun tidak dapat diterapkan secara praktikal. Algoritma ini dianggap aman dalam bentuk 3DES (*Triple DES*) meskipun sudah ada teknik serangan secara teoretis. Setelah beberapa tahun, dibuat sebuah sistem kripto yang dianggap lebih baik dibanding DES yaitu AES (*Advanced Encryption Standard*).

# Perkenalan

Algoritma ini didesain untuk mengenkripsi dan mendekripsi blok data sepanjang 64 bit dengan kunci berukuran 64-bit (dimana 8 bit diantaranya merupakan *parity bits* sehingga ukuran kunci sebenarnya adalah 56-bit). Dekripsi dilakukan dengan menggunakan kunci yang sama dengan yang digunakan saat enkripsi dengan pengubahan pengalamat bit-bit kunci sehingga menghasilkan proses kebalikan dari proses enkripsi. Sebuah blok yang akan dienkripsi pertama-tama dipermutasikan dengan permutasi *IP*, kemudian di komputasi dengan algoritma kompleks yang dibentuk dari kunci dan akhirnya dikenakan permutasi balikan dari permutasi awal *IP-1*. Komputasi dengan kunci dapat didefinisikan dengan sebuah fungsi *f*, yang disebut fungsi *cipher*, dan sebuah fungsi *KS*, yang disebut *key schedule*.

Figure Gambaran dasar proses enkripsi dengan DES

# Enkripsi

Ilustrasi proses enkripsi:

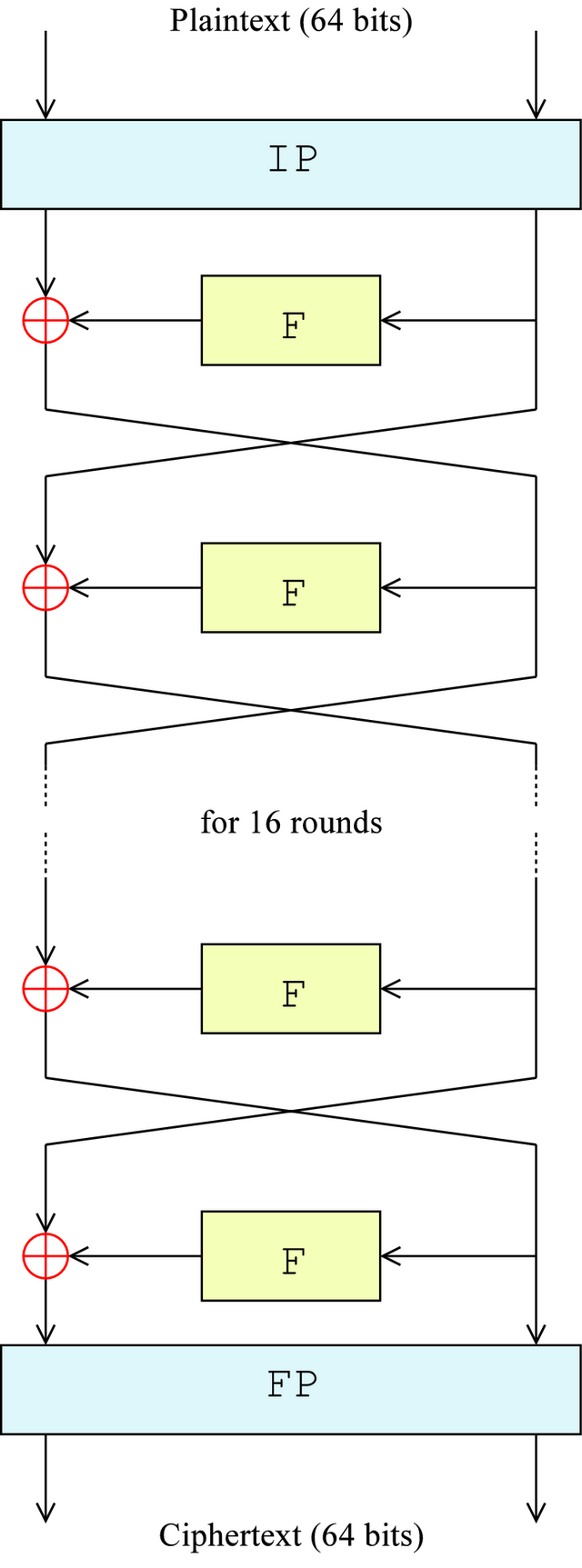


Figure Proses enkripsi DES

Pertama-tama, blok masukan sepanjang 64 bit yang akan dienkripsi dikenakan permutasi berikut yang disebut permutasi *IP*:

Dimana masukan yang sudah dipermutasi memiliki bit ke-58 dari masukan awal sebagai bit pertamanya, bit ke-50 sebagai bit kedua, dan seterusnya hingga bit ketujuh sebagai bit terakhir (bit ke-64). Blok masukan yang sudah dipermutasi kemudian menjadi masukan untuk komputasi bergantung-kunci yang dijelaskan dibawah. Hasil dari komputasi tersebut, disebut pra-keluaran, kemudian dikenakan permutasi yang merupakan balikan dari permutasi awal:

Dimana operasi yang dilakukan serupa dengan saat permutasi awal.

Komputasi yang menggunakan blok masukan yang sudah dipermutasi sebagai masukan untuk menghasilkan blok pra-keluaran terdiri dari, selain blok pertukaran akhir, sebanyak 16 kali iterasi perhitungan yang dijelaskan dibawah dengan funsi sandi yang mengoperasikan dua blok, 32 bit dan 48 bit yang kemudian menghasilkan blok sepanjang 32 bit.

Sebut 64 bit blok masukan terhadap iterasi terdiri dari 32 bit blok diikuti dengan 32 bit blok . Yang kemudian blok masukan dinyatakan dengan .

Sebut sebuah blok 48 bit yang dipilih dari kunci 64-bit. Kemudian keluaran dari sebuah iterasi dengan masukan didefinisikan dengan:

Persamaan (1)

Dimana menyatakan penjumlahan bit-demi-bit pada modulo 2.

Sebagaimana disebutkan sebelumnya, masukan dari iterasi pertama dari komputasi adalah blok masukan yang sudah dipermutasi. Jika adalah keluaran dari iterasi ke-16 maka adalah blok pra-keluaran. Pada setiap iterasi, kunci blok yang berbeda dipilih dari kunci 64-bit yang dinyatakan sebagai .

Dengan notasi tambahan dapat dijelaskan komputasi dari iterasi dengan lebih mendetil. Misal sebuah fungsi yang mengambil bilangan bulat dari 1 sampai 16 dan sebuah blok 64-bit sebagai masukan dan menghasilkan keluaran berupa blok 48-bit yang merupakan permutasi tertentu dari bit-bit di . Dimana

Persamaan (2)

Dengan ditentukan dari bit dalam 48 bit berbeda dari . disebut *key schedule* karena blok yang digunakan pada iterasi ke- dari persamaan (1) merupakan blok yang ditentukan dari persamaan (2).

Dari sebelumnya, sebut blok masukan yang sudah dipermutasi sebagai . Kemudian sebut dan sebagai dan serta sebut dan sebagai dan pada persamaan (1) dimana dan merupakan dan dan adalah dengan adalah bilangan bulat dari 1 sampai 16 yang menghasilkan

Persamaan (3)

Sehingga blok pra-keluaran adalah .

*Key schedule* dari algoritma diatas akan dijelaskan kemudian.

# Dekripsi

Permutasi *IP-1* yang dikenakan pada blok pra-keluaran adalah balikan dari permutasi awal *IP* yang dikenakan pada masukan. Lebih jauh, dari persamaan (1) didapat

Persamaan (4)

Sehingga untuk melakukan dekripsi cukup menerapkan algoritma yang sama terhadap blok sandi pesan dengan memperhatikan penggunaan blok bit kun yang digunakan sama dengan yang digunakan saat melakukan enkripsi. Dengan notasi bagian sebelumnya, persamaan diatas dapat dinyatakan dengan

Persamaan (5)

Dimana sekarang merupakan blok masukan yang sudah dipermutasi untuk perhitungan dekripsi dan merupakan blok pra-keluaran.

# Fungsi sandi

Gambaran dari fungsi sebagai berikut

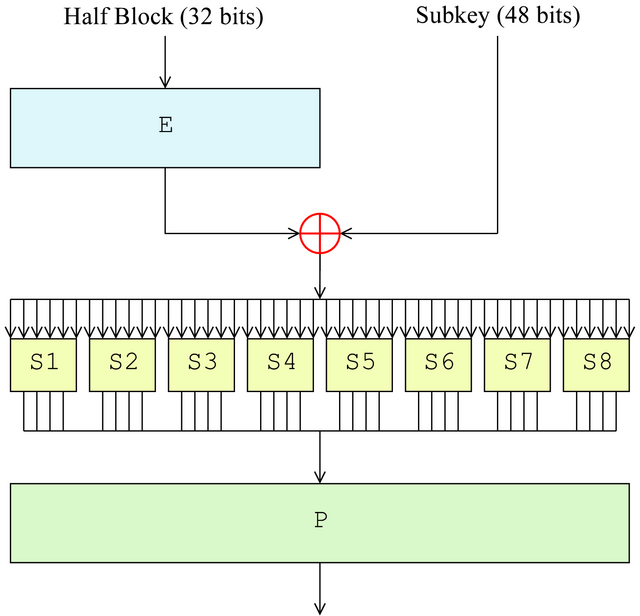


Figure Fungsi untuk menghitung

Misalkan menyatakan fungsi yang mengambil blok sepanjang 32 bit sebagai masukan dan menghasilkan blok sepanjang 48 bit sebagai keluaran. Misalkan sehingga 48 bit dari output tersebut ditulis sebagai 8 blok dengan masing-masing sepanjang 6 bit didapat dengan memilih bit dari masukan dengan urutan berdasarkan tabel berikut

Sehingga tiga bit pertama dari adalah bit-bit dari posisi 32, 1 dan 2 dari serta dua bit terakhir dari adalah bit-bit pada posisi 32 dan 1 dari .

Masing-masing fungsi pemilih unik , mengambil blok sepanjang 6 bit sebagai masukan dan menghasilkan blok sepanjang 4 bit sebagai keluaran. Tabel berikut merupakan nilai yang dianjurkan:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No. Baris | No. Kolom | | | | | | | | | | | | | | | |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 0 | 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 1 | 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 2 | 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 3 | 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

Jika adalah fungsi yang didefinisikan dengan tabel ini dan adalah blok 6-bit, maka ditentukan sebagai berikut: bit pertama dan terakhir dari menyatakan dalam basis 2 sebuah angka dari 0 sampai 3 (yaitu ). Misalkan angka tersebut . 4 bit di tengah-tengah menyatakan dalam basis 2 sebuah angka dari 0 sampai 15. Misalkan angka tersebut . Kemudian lihat di tabel baris ke- dan kolom ke-. Angka tersebut yang dinyatakan dalam 0 sampai 15 direpresentasikan secara unik dalam blok 4-bit. Blok tersebut merupakan keluaran dari untuk masukan . Misal masukan 011011, dimana barisnya adalah baris 01, yaitu baris 1, dan untuk kolomnya ditentukan oleh 1101, yaitu kolom 13 ( pada basis 2). Pada baris 1 dan kolom 13 adalah 5 sehingga keluarannya adalah 0101 ( pada basis 2).

Tabel untuk yang lain dari yang dianjurkan ditulis pada bagian setelah ini.

Kemudian terdapat fungsi permutasi yang menghasilkan keluaran 32-bit dari masukan 32-bit dengan melakukan permutasi dari blok masukan. Fungsi tersebut didefinisikan sebagai berikut

Kemudian misalkan merupakan delapan fungsi pemilih yang berbeda dan fungsi permutasi serta fungsi yang sudah didefinisikan sebelumnya.

Untuk mendifinisikan pertama-tama didefinisikan merupakan blok 6-bit dimana

Persamaan (6)

Dimana kemudian blok didefinisikan sebagai

Persamaan (7)

pertama-tama dibagi menjadi 8 sebagaimana terlihat di persamaan (6). Kemudian masing-masing diambil sebagai masukan untuk dan 8 blok dari masing-masing dengan panjang 4 bit disambung menjadi sebuah blok 32-bit yang digunakan untuk masukan dari . Keluaran dari persamaan (7) adalah keluaran dari fungsi terhadap masukan dan .

# Tabel yang Dianjurkan

Berikut ini tabel yang dianjurkan. Untuk sesuai yang disebutkan sebelumnya. Pengoperasian tabel berikut sama dengan pengoperasian tabel yang dijelaskan sebelumnya.

# Fungsi kunci

Gambaran perhitungan (*subkey*) yang digunakan adalah sebagai berikut:

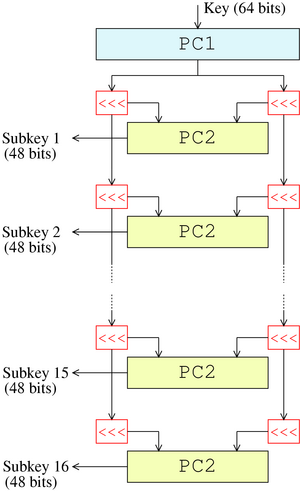


Figure Proses *Key Schedule*

Untuk melengkapi definisi cukup dijelaskan dua pilihan permutasi (PC1 dan PC2) serta *schedule* dari pergeseran kiri (<<<). Satu bit pada masing-masing 8-bit kunci dapat digunakan untuk pendeteksian kesalahan dari pembangkitan, pendistribusian dan penyimpanan kunci. Bit-bit 8, 16, ..., 64 digunakan untuk memastikan bahwa setiap *byte* (8-bit) tidak memiliki kesalahan.

Pilihan permutasi 1 (PC1) dinyatakan dengan tabel berikut

Tabel tersebut dibagi dua bagian dimana bagian pertama menentukan bagaimana bit-bit (bagian kiri gambar 4) dipilih, dan bagian kedua untuk bit-bit (bagian kanan gambar 4). Bit-bit dari diberi angka 1 sampai 64. Bit-bit adalah bit-bit 57, 49, 41, 33, ..., 44 dan 46 dari , dan bit-bit dari adalah bit-bit 63, 55, 47, ..., 12 dan 4 dari .

Dengan dan terdefinisi, lalu ditentukan bagaimana blok dan didapat dari blok-blok dan untuk . Hal tersebut didapat dengan mengikuti schedule pergeseran kiri dari blok individu:

|  |  |
| --- | --- |
| Iterasi ke- | Jumlah pergeseran kiri |
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |
| 5 | 2 |
| 6 | 2 |
| 7 | 2 |
| 8 | 2 |
| 9 | 1 |
| 10 | 2 |
| 11 | 2 |
| 12 | 2 |
| 13 | 2 |
| 14 | 2 |
| 15 | 2 |
| 16 | 1 |

Kemudian pilihan permutasi 2 dinyatakan dengan tabel berikut

Sehingga bit pertama dari adalah bit ke-14 dari , bit kedua adalah bit ke-17, dan seterusnya hingga bit ke-47 adalah bit ke-29 dan bit ke-48 adalah bit ke-32.

# Kriptanalisis

Hingga kini serangan pada DES yang secara praktik dapat digunakan hanya berupa *brute force*, yaitu dengan mencoba semua kemungkinan kunci yang ada. Kriptanalisis yang diketahui sampai sejauh ini serta teori-teori serangan yang memungkinkan, meskipun memiliki tingkat kompleksitas yang lebih rendah dibanding *brute force*, memerlukan jumlah known/chosen plaintext yang tidak realistis sehingga dianggap tidak mungkin digunakan. Untuk serangan secara *brute force* pernah dibuat beberapa mekanisme serangan baik dengan mesin/chip yang didesain khusus untuk menyerang DES ataupun dengan *software* yang memanfaatkan *distributed computing*.

# Referensi

* Algoritma DES: *FIPS 46-3: The official document describing the DES standard*. <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf> .
* Sejarah Singkat, kriptanalisis dan Ilustrasi: *Data Encryption Standard - Wikipedia, the free encyclopedia*. <http://en.wikipedia.org/wiki/Data_Encryption_Standard> .