**BAB I**

**PENDAHULUAN**

1. Latar Belakang

Perkembangan teknologi informasi dewasa ini telah berpengaruh pada hampir semua aspek kehidupan manusia. Saat ini internet seolah-olah menghiraukan batas-batas geografis suatu negara, bukan hal yang sulit bagi seseorang untuk berkomunikasi jarak jauh, mengirimkan data, mencari informasi dan sebagainya. Semua hal tersebut dapat dilakukan dengan internet secara cepat, efisien dan relatif murah. Namun di sisi lain, ternyata internet merupakan jalur yang tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan secara bebas oleh siapapun sehingga sangat rawan penyadapan informasi oleh pihak-pihak yang tidak absah. Oleh karena itu masalah keamanan, kenyamanan dan otorisasi dalam berinternet menjadi masalah krusial yang sampai hari ini masih menjadi perbincangan hangat. Banyak pertanyaan yang muncul, Apakah transaksi via internet bisa terjamin keamanannya? Apakah data yang dikirimkan via internet sampai pada tujuan yang tepat tanpa diketahui pihak yang tidak diinginkan? Bagaimana mencegah penyadapan informasi? Bagaimana mengantisipasi seseorang mencuri data?

Banyak metode yang dapat dilakukan untuk menjawab pertanyaan-pertanyaan diatas. Salah satunya dengan metode penyandian atau yang lebih dikenal dengan metode kriptografi. Banyak sekali metode penyandian atau metode kriptografi yang dikembangkan oleh pakar-pakar kriptografi hingga saat ini. Hal ini dilakukan dikarenakan penyadap dan pencuri informasi atau yang lebih dikenal dengan sebutan cracker semakin handal dalam mempenetrasi suatu sistem untuk menggali berbagai macam informasi. Oleh karena itu dalam rangka melawan tindakan keji tersebut, pakar-pakar kriptografi terus mengembangkan metode ini secara berkesinambungan. Banyak sekali metode penyandian yang telah diciptakan oleh pakar-pakar kriptografi dunia, sebut saja Algoritma DES, Algoritma Triple DES, Algotitma RSA, Algotitma MD5, Algoritma SHA-1 dan sebagainya. Algoritma-algoritma diatas telah diuji kemampuannya oleh pakar-pakar kriptografi, namun tidak semua metode kriptografi diatas bertahan dari serangan para penyadap informasi atau dalam istilah kriptografi sering disebut dengan cryptanalist. Sebut saja algoritma DES, sempat bertahan cukup lama yakni selama 20 tahun akhirnya harus rela di-crack hanya dalam tempo 3,5jam dengan biaya 1 juta US Dollar pada tahun 1993. Namun para pakar kriptografi tidak berdiam diri, karena setelah kejadian itu para pakar kriptografi mengembangkan varian baru dari algoritma DES seperti Algoritma TripleDES dan sebagainya.

Makalah ini akan membahas salah satu diantara banyak kriptografi handal yang hingga saat ini masih cukup kuat membendung serangan-serangan dari para cryptanalist, yaitu metode kriptografi dengan algoritma Data Encryption Standard atau DES.

1. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah di uraikan, dapat dirumuskan masalah-

masalah yang akan dibahas pada penulisan kali ini. Masalah yang dimaksud adalah

sebagai berikut :

1. Bagaimana sejarah kriptografi.
2. Apakah tujuan kriptografi.
3. Jenis – jenis kriptografi.
4. Bagaimana sejarah DES.
5. Fungi DES
6. Kekurangan dan Kelebihan DES
7. Bagaimana cara kerja DES.
8. Implementasi DES
9. Tujuan Pembuatan Makalah

Pembuatan makalah bermaksud untuk menganalisa proses penyandian pesan dan proses membuka kembali penyandian dalam kriptografi, khususnya kriptografi algoritma DES. Diharapkan dengan adanya makalah ini para pengguna jalur internet lebih ekstra hati-hati dalam penggunaan jalur publik ini. Untuk metode pengamanan dapat menggunakan metode kriptografi algoritma DES yang dibahas secara detail pada makalah ini.

**BAB II**

**LANDASAN TEORI**

1. Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul The Codebreakers. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa hieroglyph yang terdapat pada piramid) hingga penggunaan kriptografi pada abad ke-20 (Menezes et al, 1996).

Secara historis ada empat kelompok yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (lovers). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit. Kriptografi juga digunakan untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan relijius dari gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah “Angka si Buruk Rupa (Number of the Beast) di dalam Kitab Perjanjian Baru. Angka “666” menyatakan cara kriptografik (yaitu dienkripsi) untuk menyembunyikan pesan berbahaya, para ahli percaya bahwa pesan tersebut mengacu pada Kerajaan Romawi.

Di India, kriptografi digunakan oleh pencinta (lovers) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku Kama Sutra yang merekomendasikan wanita seharusnya mempelajari seni memahami tulisan dengan cipher. Pada Abad ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkrpsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode (Munir, 2006).

Seperti yang telah disebutkan di atas bahwa kriptografi umum digunakan di kalangan militer. Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan Enigma. Mesin yang menggunakan beberapa buah rotor (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun Enigma cipher berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memecahkan Enigma sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2 (Churchhouse, 2004). Dimulai dari usaha Feistel dari IBM di awal tahun 70-an dan mencapai puncaknya pada 1977 dengan pengangkatan DES (Data Encryption Standard) sebagai standar pemrosesan informasi federal Amerika Serikat untuk mengenkripsi informasi yang tidak belum diklasifikasi. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah.

Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada 1976 saat Diffie dan Hellman mempublikasikan ”New Directions in Cryptography”. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret. Meskipun Diffie dan Hellman tidak memiliki realisasi praktis pada ide enkripsi kunci publik saat itu, idenya sangat jelas dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi.

Pada 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik yang sekarang disebut RSA. Rancangan RSA berdasar pada masalah faktorisasi bilangan yang sulit, dan menggiatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran. Tahun 80-an terjadi peningkatan luas di area ini, sistem RSA masih aman. Sistem lain yang merupakan rancangan kunci publik ditemukan oleh Taher ElGamal pada tahun 1984. Rancangan ini berdasar pada masalah logaritma diskret.

Salah satu kontribusi penting dari kriptografi kunci publik adalah tanda tangan digital. Pada 1991 standar internasional pertama untuk tanda tangan digital diadopsi. Standar ini berdasar pada rancangan kunci publik RSA. Pada 1994 pemerintah Universitas Sumatera Utara. Amerika Serikat mengadopsi Digital Signature Standard, sebuah mekanisme kriptografi yang berdasar pada algoritma ElGamal (Menezes et al, 1996).

1. Tujuan Kriptografi

Secara umum tujuan ilmu kriptografi diciptakan adalah untuk merahasiakan suatu pesan agar tidak bisa dibaca oleh pihak yang tidak absah. berpedoman dari tujuan umum tersebut, terdapat empat tujuan mendasar ilmu kriptografi digunakan dalam bidang keamanan informasi yaitu :

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

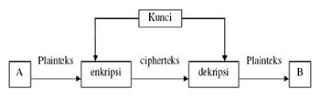
2.3 Jenis – jenis kriptografi

Algoritma kriptografi dibagi menjadi dua bagian berdasarkan kunci yang dipakainya :

1. Kriptografi Simetris

Kriptografi Simetris adalah : Kode Hill atau lebih dikenal dengan Hill cipher merupakan salah satu algoritma kriptografi kunci simetris dan merupakan salah satu kripto polyalphabetic. Hill cipher diciptakan oleh Lester S. Hill pada tahun 1929 .Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher yang tidak dapat dipecahkan menggunakanteknik analisis frekuensi. Berbeda dengan caesar cipher, hill cipher tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

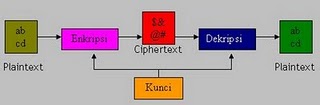
Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini enggunakan sebuah matriks persegi sebagai kunci berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks karena menggunakan matriks sebagai kunci, Hill cipher merupakan algoritma kriptografi kunci simetris yang sulit dipecahkan, karena teknik kriptanalisis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini. Hill cipher sangat sulit dipecahkan jika kriptanalis hanya memiliki ciphertext saja (chipertext-only), namun dapat dipecahkan dengan mudah jika kriptanalis memiliki ciphertext dan potongan dari plaintext-nya (known-plaintext).



Gambaran kriptografi simetris

2. Kriptografi Asimetris

Algoritma asimetris, sering juga disebut dengan algoritma kunci publik atausandi kunci publik, menggunakan dua jenis kunci, yaitu kunci publik (public key) dan kunci rahasia (secret key). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan.   
Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.



Gambaran Kriptografi Asimetris

**BAB III**

**PEMBAHASAN**

3.1 Sejarah DES

DES atau Singkatan dari Data Encryption Standard merupakan algoritma penyandian yang diadopsi dan dibakukan oleh NBS (National Bureau Standard) yang kini menjadi NIST (National Institute of Standards and Technology) pada tahun 1977 sebagai FIPS 46 (Federal Information Processing Standard).

DES bermula dari hasil riset Tuchman Meyer yang diajukan sebagai kandidat Sandi Standard Nasional yang diusulkan oleh NBS. Konon katanya, algoritma yang dikembangkan oleh Tuchman Meyer ini merupakan algoritma terbaik dari semua kandidat Sandi Standard Nasional. Pada mulanya, algoritma yang kini disebut DES, memiliki panjang kunci sandi 128 bit. Namun selama proses pengadopsian, NBS melibatkan NSA (National Security Agency), dan algoritma sandi ini mengalami pengurangan ukuran kunci sandi dari 128 bit menjadi 56 bit saja. Sebagian orang mungkin mengira bahwa pengurangan panjang kunci sandi ini merupakan usulan NSA untuk melemahkan algoritma Tuchman Meyer karena motif politik tertentu. Entah itu untuk mempermudah penyadapan atau untuk melemahkan pengamanan informasi lawan politik. Mungkin NSA menginginkan algoritma Tuchman Meyer ini “cukup aman” untuk digunakan warga sipil, tetapi mudah dipecahkan oleh organisasi besar semisal NSA dengan peralatan canggihnya. Bila dibandingkan dengan performa komputer personal pada saat itu, algoritma sandi dengan panjang kunci 56 bit dapat dikatakan cukup aman bila digunakan oleh orang-orang “biasa”, tapi dapat dengan mudah dipecahkan dengan peralatan canggih dan tentunya kepemilikan alat canggih ini hanya dapat dijangkau oleh organisasi elit seperti NSA. Dengan dukungan dana yang melimpah, pembuatan alat brute‐force DES bukanlah hal yang mustahil pada saat itu. Kini algoritma DES sudah usang dan keamanannya pun sudah tidak dapat dipertanggungjawabkan lagi. Kini komputer personal pun sudah cukup untuk membobol algoritma DES, apalagi dengan adanya teknologi parallel computing dan internet yang berkembang pesat. DES telah secara resmi digantikan fungsinya oleh AES (Advanced Encryption Standard) dengan panjang kunci sandi 128, 192 dan 256 bit.

Kendatipun kita telah mengetahui bahwa algoritma AES sudah kuno dan tidak aman, tidak ada salahnya jika kita mempelajari algoritma ini untuk tujuan hobi atau pendidikan. Perlahan tapi pasti, belajar dari algoritma yang sederhana dan perlahan‐lahan menuju algoritma lain yang lebih kompleks.

Algoritma DES merupakan algoritma enkripsi blok simetris. DES dikatakan enkripsi blok karena pemrosesan data baik enkripsi maupun dekripsi, diimplementasikan per blok (dalam hal ini 8 byte). DES dikatakan enkripsi simetris karena algoritma yang digunakan untuk enkripsi relatif atau bahkan sama persis dengan algoritma yang digunakan dalam proses dekripsi. Proses enkripsi dapat didefinisikan secara sederhana sebagai proses penterjemahan data “asli” yang “jelas” dan “kasat mata” yang dapat dipahami maknanya. secara langsung menjadi data lain yang terlihat “buram” atau “acak” sehingga tidak dapat dipahami secara langsung, sedemikian rupa sehingga makna informasi yang disembunyikan tidak lagi dapat diketahui secara langsung kecuali dengan mengembalikan informasi tersebut ke bentuk aslinya. Sedangkan proses dekripsi dapat didefinisikan secara sederhana sebagai proses pengembalian bentuk data, dari data “buram” atau “acak” menjadi data “asli” yang “jelas” dan “kasat mata” yang dapat dipahami maknanya. Algoritma enkripsi umumnya dilengkapi semacam kata sandi (password), untuk memvariasikan fungsi enkripsi tersebut. Data yang sama, kunci yang sama dan algoritma yang sama akan menghasilkan data enkripsi yang sama. Dalam algoritma penyandian DES, kunci yang digunakan dalam proses enkripsi dan dekripsi haruslah sama, supaya data dapat dikembalikan ke bentuk aslinya. Bisa jadi, karena “kesamaan” kunci inilah DES juga dinamakan algoritma enkripsi simetris. Inti dari proses enkripsi adalah penyembunyian data dengan mengaburkan data “asli” dan mengurangi keteraturan informasi, sehingga data tersebut tidak dapat “dibaca” kecuali oleh pihak yang berhak. Berbagai algoritma enkripsi sengaja dibuat untuk melindungi informasi dari penyadapan, karena ada kemungkinan terjadinya penyadapan saat data melewati media hantar (media hantar dapat berupa suara, surat, email, kabel, kertas, frekwensi radio atau apapun itu). Seandainya penyadap dapat menyadap semua informasi yang melalui media hantar, idealnya hasil sadapan tersebut hanya menghasilkan data “sampah” yang tidak berguna. Semua algoritma kriptografi diciptakan untuk mewujudkan kondisi ideal tersebut, tapi sayangya kondisi tersebut sangat sulit dicapai, karena selalu ada cara untuk membalikkan informasi sadapan ke bentuk aslinya.

3.2 Fungsi DES

Secara umum tujuan DES diciptakan adalah untuk merahasiakan suatu pesan agar tidak bisa dibaca oleh pihak yang tidak absah. berpedoman dari tujuan umum tersebut, sehinga pesan yang dikirimkan aman dan tidak dapat dibajak

3.3 Kekurangan dan Kelebihan DES

Data Encryption Standard ( DES ) pun seperti sistem yang lainnya, memiliki kekurangan dan kelebihan. Salah satu kekurangan DES adalah proses yang lebih lama dalam melakukan proses dekripsi dan enkripsi.

Kelebihan DES yaitu, sistem sandi lebih kompleks sehingga membutuhkan waktu yang tidak cepat untuk menembus enkripsi DES dan sulit untuk diketahui dari pihak luar. Tetapi setelah berkembangannya jaman DES tidak digunakan karena ukuran kunci yang terlalu kecil, sehingga mudah untuk ditembus

3.4 Cara Kerja DES

Dalam DES, algoritma dekripsi tepatnya merupakan proses kebalikan (inverse) algoritma enkripsi. Dalam prakteknya proses pembalikan (proses dekripsi) ini diimplementasikan dengan membalikkan urutan sub kunci yang digunakan dalam proses enkripsi, selebihnya algoritma enkripsi dan dekripsi adalah sama. Algoritma enkripsi DES bekerja dengan mengolah blok data 8 byte (64 bit) dengan blok kunci 8 byte (64 bit). Proses penyandian dalam DES diawali dengan fungsi pengacakan bit yang dinamai IP (Initial Permutation) kemudian fungsi inti DES yang diulang sebanyak 16 kali dan terakhir ditutup dengan fungsi pengacakan bit lain yang dikenal denagn nama IP‐1 (Inverse Initial Permutation). Pada sisi lain algoritma penjadwalan sub kunci akan menghasilkan 16 sub kunci secara berurutan dari parameter kunci yang diberikan untuk digunakan pada setiap putaran fungsi inti DES. Sub kunci pertama untuk putaran pertama, sub kunci kedua untuk putaran kedua dan seterusnya hingga putaran ke 16.  
Perlu diingat, kendatipun slot kunci yang disediakan digunakan berukuran 8 byte (64 bit), ternyata pada faktanya ukuran kunci yang digunakan hanya sebanyak 56 bit saja, karena bit paling signifikan (MSB) dari setiap bit diabaikan. Jadi sebenarnya ukuran kunci DES adalah 56 bit. Adapun Ilustrasi penyandian DES dalam diagram blok dapat dilihat pada gambar di samping. Algoritma penjadwalan sub kunci dibentuk dari pengacakan bit dan pemutaran kiri ruas kanan dan kiri kunci. Pertama kali, bit-bit kunci diacak dengan Permutation Choice 1 dan dibagi dua menjadi ruas kiri dan ruas kanan. Kedua ruas tersebut kemudian diputar kiri dan diacak kembali dengan Permutation Choice 2 untuk menghasilkan sub kunci. Jumlah pemutaran ke kiri ditentukan secara spesifik untuk setiap sub kunci.  
Rinciannya adalah sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Untuk lebih lanjut, mari terlebih dahulu kita bahas detail algoritma penjadwalan sub kunci kemudian algoritma enkripsi dan terakhir algoritma dekripsi. Inti dari semua proses permutasi dalam DES adalah pengacakan bit. Sebagai contoh, jika masukan permutasi sebanyak n bit, maka akan ada sebanyak 2n kemungkinan masukan permutasi dan ada 2n kemungkinan hasil permutasi. Setiap satu kemungkinan masukan akan berpasangan dengan satu kemungkinan keluaran.  
Sebelum proses penjadwalan kunci dimulai, kunci terlebih dahulu dipetakan menjadi matriks 8x8 dan diberi indeks. Dalam setiap byte, indeks paling kecil melambangkan LSB dan indeks paling besar melambangkan MSB. Sebagai contoh, indeks ke 1 melambangkan LSB byte pertama, index ke 8 melambangkan MSB byte pertama, indeks ke 9 melambangkan LSB byte kedua, indeks ke 16 melambangkan MSB byte kedua dan seterusnya hingga indeks ke 64 yang melambangkan MSB byte ke 8. Mari kita perhatikan contoh dibawah ini. Kunci = 0x01, 0x23, 0x45, 0x67, 0x89, 0xab, 0xcd, 0xef

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Setelah pemetaan, hasilnya adalah sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Matriks Indeks Hasil Pemetaan  
Pengacakan bit Permutation Choice‐1 akan mengolah 8 byte blok kunci menjadi 56 bit sub kunci yang siap diproses lebih lanjut. Untuk lebih mudahnya, proses pengacakan bit dilambangkan dengan pengacakan indeks bit yang bersangkutan. Berikut ini adalah detail Permutation Choice 1.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)Setelah kunci diacak dengan Permutation Choice 1, hasil pengacakan bit tersebut kemudian dibagi 2, yakni ruas kiri dan ruas kanan, masing masing berukuran 28 bit (ditandai dengan garis tebal pada hasil Permutation Choice 1). Selanjutnya kedua ruas tersebut kemudian mengalami pemutaran kiri sebanyak jumlah yang tertera pada tabel penjadwalan jumlah pemutaran yang telah kita bahas sebelumnya. Berikut ini adalah ilustrasi pemutaran ke kiri sebanyak 1 kali (untuk ruas kiri atau ruas kanan kunci yang panjangnya 28 bit). Untuk pemutaran ke kiri dengan jumlah yang lebih besar, cukup mengulangi proses ini sebanyak yang diinginkan.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

 Setelah ruas kiri dan ruas kanan diputar kiri dengan jumlah tertentu, selanjutnya hasil pemutaran tersebut digabungkan kembali menjadi 56 bit dan diacak dengan Permutation Choice‐2 untuk menghasilkan sub kunci. Rincian Permutation Choice 2 adalah sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Karena jumlah keluaran Permutation Choice 48 bit sementara masukannya 56 bit, dengan demikian ada 8 bit yang “dihilangkan”. Bit-bit yang tidak muncul dalam keluaran Permutation Choice 2 diwarnai abuabu. Selanjutnya, mari kita perjelas algoritma enkripsinya. Setelah melihat diagram blok secara keseluruhan proses enkripsi, ada tiga hal yang perlu digarisbawahi dan dibahas lebih lanjut yaitu, pertama IP (Initial Permutation), kedua detail fungsi F dan IP 1 (Inverse Initial Permutation).  
Selama proses enkripsi, pertama data dipetakan dan diberi indeks dengan prosedur sama persis seperti pemberian indeks pada penjadwalan kunci yang telah didiskusikan sebelumnya. Selanjutnya hasil pemetaan diacak dengan menggunakan Initial Permutation dengan rincian sebagai berikut  
Masukan IP

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Setelah data melewati proses Initial Permutation, data yang akan disandikan kemudian dibagi menjadi dua ruas, yaitu ruas kiri dan ruas kanan yang masIng-masing lebarnya 4 byte (32 bit). Pada setiap putaran, ruas kanan dan sub kunci yang bersangkutan diproses dalam fungsi F dan hasilnya di XOR dengan ruas kiri ruas kanan dan kiri dipertukarkan. Proses ini diulang sebanyak 16 kali.  
Pada putaran terakhir ruas kiri dan ruas kanan dipertukarkan kembali untuk menghilangkan efek pertukaran pada putaran terakhir. Hasil ini kemudian diacak kembali dengan menggunakan IP 1 (Inverse Initial Permutation). XOR merupakan fungsi Boolean yang didefinisikan dengan table benaran berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Initial Permutatrion dan Inverse Initial Permutation memiliki karakter saling menetralkan. Dalam notasi matematika, IP−1(IP(A))= A. Inverse Initial Permutation didefinisikan sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

 Fungsi F merupakan fungsi inti kompleks yang terdiri dari beberapa proses. Fungsi F menerima dua parameter, yaitu sub kunci dan ruas kanan data yang akan dienkripsi. Berikut ini adalah diagram blok detail fungsi F. Pada fungsi F, ruas kanan (32 bit) diacak sekaligus diperluas dengan permutasi E menjadi 48 bit. Hasil pengacakan tersebut kemudian di XOR dengan sub kunci yang telah ditetapkan dengan putaran yang bersangkutan. Hasil XOR kemudian dipecah menjadi 8 unit yang masing‐masing lebarnya 6 bit. Setiap unit tersebut kemudian disubstitusikan dalam SBOX S1 hingga S8. 6 bit paling kiri disubstitusikan ke dalam S1 dan 6 bit paling kanan disubstitusikan ke dalam S8. Hasil setiap substitusi kemudian digabungkan menjadi data selebar 48 bit yang kemudian diacak dan diperpendek dengan permutasi P menjadi 32 bit. Hasil permutasi P kemudian dinyatakan sebagai keluaran fungsi F yang nantinya akan di XOR kan dengan ruas kiri data yang akan dienkripsi.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Sekarang mari kita bahas detail fungsi F satu per satu. Pertama, permutasi E memetakan 32 bit masukan menjadi 48 bit keluaran. Karena lebar keluaran lebih besar dari lebar masukan, maka ada beberapa bit masukan yang digandakan untuk mengisi kekosongan. Permutasi E didefinisikan sebagai berikut

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Kedua, DES memiliki 8 buah SBOX (S1 hingga S8) yang memiliki masukan selebar 6 bit dan keluaran selebar 4 bit. Karena lebar keluaran SBOX lebih kecil daripada lebar masukannya, maka adakemungkinan beberapa kombinasi masukan yang berbeda akan menghasilkan keluaran yang sama. Seandainya masukan setiap SBOX adalah 1 2 3 4 5 6 x x x x x x maka S1 hingga hingga S8 didefinisikan sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Ketiga, hasil substitusi SBOX kemudian digabungkan menjadi 32 bit dan diacak dengan permutasi P dan hasil permutasi P merupakan keluaran fungsi F yang nantinya di XOR dengan ruas kiri. Permutasi P didefinisikan sebagai berikut.

[](https://link.safelinkconverter.com/?id=aHR0cDovL3B1c2F0LW1ha2FsYWhrdS5ibG9nc3BvdC5jb20v&c=0&user=61204)

Dalam DES, algoritma yang digunakan dalam proses enkripsi sama persis dengan algoritma yang digunakan dalam proses dekripsi, hanya saja penggunaan sub kuncinya saja yang berbeda. Dalam proses dekripsi, urutan sub kunci yang digunakan merupakan kebalikan urutan sub kunci yang digunakan dalam proses enkripsi.

3.3 Implementasi DES

Operasi yang digunakan dalam algoritma DES merupakan operasi‐operasi sederhana semisal move, bit copy, XOR, lookup, shift dan rotate. Semua operasi tersebut tersedia dalam mikroprosesor/mikrokontroler 8 bit. Dengan demikian dapat kita simpulkan bahwa DES dapat diterapkan dalam platform 8 bit.

Semua operasi permutasi dalam DES, baik IP, IP 1, PC 1, PC 2, E dan P, pada intinya hanyalah operasi penyalinan bit. Jika instruksi penyalinan bit tidak tersedia, maka permutasi juga dapat diimplementasikan dengan operasi shift, dengan memanfaatkan carry yang timbul dari setiap instruksi shift. Selain itu, operasi substitusi dengan SBOX juga dapat dengan mudah diimplementasikan menggunakan table lookup dengan ukuran yang masih dapat dijangkau. Dalam platform 32 atau 64 bit, DES dapat diimplementasikan lebih effektif lagi, tapi sayangnya operasi bit per bit seperti permutasi mungkin sedikit menyita performa prosesor dan memperlambat laju enkripsi per detik.