**الگوریتم رمزنگاری DES:**

**در نرم افزار برای رمز نگاری قالب ورودی textمیباشد و قالب خروجی عدد در مبنای شانزده میباشد و گزینه ی encانتخاب میشود برای رمز گشایی قالب ورودی و خروجی عوض شده و گزینه ی dec انتخاب میشود.**  
1) ورودی رمز نگار یک رشته 64 بیتی است، بنابراین داده های ورودی بایست در گروه های هشت کاراکتری دسته بندی و به ورودی سخت افزار رمزنگار DES، اعمال شوند.  
  
2) اولین عملی که برروی رشته ورودی انجام می شود جابجا کردن محل رشته 64 بیتی طبق جدول است. به عنوان مثال طبق این جدول، بیت پنجاه وهشتم از ورودی به موقعیت یکم و بیت یکم به موقعیت چهلم منتقل می شود. به این عمل (جایگشت مقدماتی) گفته می شود و کلید رمز هیچ دخالت و تاثیری در این جابجایی ندارد. این عمل تنها وابستگی آماری بیت های مجاور را به هم می ریزد.  
جدول جايگشت مقدماتی IP:  
3) در گام بعد رشته 64 بیتی جایگشت شده از گام قبل، به دو نیمه 32 بیتی چپ و راست تقسیم بندی خواهد شد.  
4)در گام چهارم، فرآیند رمز نگاری مبتنی بر کلید آغاز می شود و تا شانزده «دور» (Round) ادامه می یابد. ماهیت پردازش در تمام دورها دقیقاً یکسان است با این تفاوت که پارامترهای ورودی در هر دور متفاوتند. این 16 دور به شانزده کلید 48 بیتی متفاوت نیاز دارد که همگی آنها به روشی غیر خطی و نسبتاً پیچیده از کلید 56 بیتی اصلی، استخراج می شوند.  
این 16 کلید درون یک آرایه در اختیار است. در هر دور، 32 بیت سمت راست مستقیماً به سمت چپ منتقل شده و 32 بیت سمت چپ طبق رابطه زیر به یک رشته 32 بیتی جدید تبدیل و به سمت راست منتقل خواهد شد.

Li-1 xor f(Ri-1,Ki)

f تابعی غیر خطی، خاص و مبهم است.  
  
Li-1 رشته 32 بیتی سمت چپ از مرحله قبل است.  
  
Ri-1 رشته 32 بیتی سمت راست از مرحله قبل است.  
  
Ki کلید فرعی هر دور است.  
  
5) پس از دور شانزدهم، جای نیمه 32 بیتی سمت چپ و راست عوض خواهد شد. سپس عکس عمل جایگشتی که در ابتدا انجام شده بود صورت می گیرد تا بیتها سرجای اصلی شان برگردند.   
  
6) حال خروجی 64 بیتی رمز شده، در خروجی آماده است.  
  
*جزئیات تابع f:*  
تابع f یک تابع غیر خطی مشتمل بر عملیات «توسیع» (Expansion)، «جانشینی»، " XOR " و «جایگشت» است؛ پیچیدگی و استحکام DES از همین تابع منشاء گرفته است.  
  
الف) در اولین گام رشته 32 بیتی ورودی (Ri-1) با تکرار برخی از بیتها، به یک رشته 48 بیتی توسعه داده می شود.  
  
ب) در گام بعد، کلید فرعی متناظر با شماره دور، با رشته توسعه یافته، بیت به بیت XOR می شود. بدین ترتیب یک رشته جدید 48 بیتی جدید پدید می آید.  
  
ج) در گام سوم، رشته 48 بیتی حاصل بایست به 32 بیت کاهش یابد، برای این کار رشته 48 بیتی در قالب 8 دسته شش بیتی به هشت S-Box متفاوت وارد می شود. هر یک از این S-Box ها، یک عدد شش بیتی را گرفته و آن را بر اساس جدولی به یک عدد 4بیتی می نگارد.  
  
د)در گام آخر، بیتهای رشته 32 بیتی بدست آمده از مرحله قبل، جایگشت داده می شوند. به عبارتی جای هر بیت بر اساس جدول تغییر می کند.

ساختار کلی فرایند رمزنگاری در روش DES را میتوان با استفاده از شکل زیر بیان نمود:

|  |
| --- |
| des |
| فلوچارت رمزنگاری به روش DES - مرجع FIPS46-3 |

رمز نگاری در این روش براساس تغیر در قطعه ای از اطلاعات ورودی صورت میگیرد برای رمزنگاری مراحل زیر انجام میشود.   
1 - پیام اولیه به صورت قطعات 64 بیتی از ورودی اخذ میشود. درصورتی که پیام ورودی کمتر از 64 بیت باشد باقیمانده پیام تاسقف 64 بیت با بیت های تصادفی پرخواهد شد.   
2 - با استفاده از [جدول جایگزینی اولیه](https://ircrypt.com/des.php#initialpermutation) (Initial Permutation) مکان بیت های رشته ورودی جابجا خواهد شد.   
3 - در جایگشت اول, پیام به دو بخش L0,R0 تقسیم میشود   
4 - مقدار R0 به بخش L1 در مرحله بعد انتقال می یابد L1 = R0   
5 - مقدار R1 بر اساس ترکیب R1=L0 XOR F(R0,K1) تولید میشود . وظیفه تابع F در این بخش انجام عملیات اصلی رمزنگاری می باشد.   
6 - مراحل چهارم و پنجم تا 15 مرحله تکرار خواهد شد.   
7 - در مرحله شانزدهم از فرمول زیر برای محاسبه استفاده می شود:   
L16=R15   
R16=L15 XOR F(R15,K16)   
7 - در مرحله نهایی رشته بدست امده از مرحله شانزدهم, با استفاده از [جدول جایگزینی معکوس](https://ircrypt.com/des.php#inverseinitialpermutation)(Inverse Initial Permutation) مکان بیت های رشته خروجی جابجا خواهد شد   
8 - مراحل اول تا هفتم تا اتمام رشته ورودی ادامه خواهد یافت   
وظیفه تابع F در این بخش انجام عملیات اصلی رمزنگاری می باشد که که در بخش جداگانه ای توضیح داده شده است.   
کلید مورد استفاده در بخش پنجم به ازای هر چرخه به طور مستقل تولید می شود وظیفه تولید کلید مورد نیاز بر عهده تابع تولید کلید می باشد.   
  
  
**جدول جایگزینی اولیه**   
براساس استاندارد الگوریتم DES بیتهای رشته ورودی می باید جابجا شوند. جابجائی مورد نظر بر اساس جدول جایگزینی اولیه (Initial Permutation) انجام می شود. این جابجایی در ابتدای فرایند رمزنگاری انجام شده و بیتهای ورودی براساس جدول زیر مرتب خواهند شد:

|  |
| --- |
| initial permutation |
| جدول جایگزینی اولیه Initial Permutation |

**جدول جایگزینی معکوس**   
براساس استاندارد الگوریتم DES بیتهای رشته خروجی در انتهای فرایند می باید جابجا شوند. جابجائی مورد نظر بر اساس جدول جایگزینی معکوس (Inverse Initial Permutation) انجام می شود. این جابجایی در انتهای فرایند رمزنگاری انجام شده و بیتهای خروجی براساس جدول زیر مرتب خواهند شد:

|  |
| --- |
| inverse initial permutation |
| جدول جایگزینی معکوس Inverse Initial Permutation |

تابع کلید

در رمزنگاری به روش DES می بایست از یک کلید ورودی به عنوان کلید مبنا استفاده شود. هریک از مراحل شانزده گانه روش DES نیازمند کلیدهای منجصر به فرد می باشند که بر اساس فرمول زیر تولید می شود:  
KS=(n,KEY)   
کلیدهای تولید شده در این مرحله مستقل بوده و توالی کلید ها دارای اهمیت می باشند این توالی در فرایند رمزگشایی مورد استفاده قرار میگیرد و در صورت عدم رعایت توالی مورد نظر رمزگشایی به درستی انجام نمی پذیرد. 

### **تشریح تابع کلید**

همانطور که گفته شد هر چرخه از فرایند رمزنگاری DES دارای کلید های منحصر به فرد خود می باشد. وظیفه تابع کلید, ایجاد کلید های مورد نیاز بر اساس شماره چرخه می باشد. تابع کلید بر اساس فلوچارت زیر اجرا میشود .

|  |
| --- |
|  |
| جدول محاسبه کلید - مرجع |

فلوچارت محاسبه کلید را میتوان به صورت زیر تشریح نمود:   
1 - در ابتدا یک رشته 64 بیتی به عنوان ورودی تعین میشود.   
2 - در مرحله دوم یک جایگشت بر روی رشته ورودی انجام میشود این جایگشت از آخرین بیتهای موجود در هر بایت صرفنظر کرده و از رشته 64 بیتی موجود 56 بیت را برای کلید استخراج میکند. جدول pc1 نحوه این جایگشت را مشخص میکند. با مشاهده جدول pc1 مشاهده میکنیم بیتها به ترتیب خاصی از هم جدا شده و بیتهای آخر هر بایت در این جدول وجود ندارند.از بیتهای اخر برای کنترل توازن بر مبنای زوج بودن اعداد استفاده میشود.

|  |
| --- |
| des premuted choice |
| جدول جایگشت انتخابی اول |

3 - خروجی مرحله قبل به دو دسته C,D تفکیک می شوند که این دسته بندی برای تمامی مراحل شانزده گانه انجام میشود.  
4 - هر بلاک C و D می بایست به سمت چپ شیفت داده شوند که بر بر اساس جدول شیفت تعداد دفعات شیفت به چپ برای هر کدام از چرخه ها مشخص می شود

|  |
| --- |
| des shift table |
| جدول شیفت |

5 - خروجی مرحله چهارم که با نام C1,D2 مشخص شده است پس از اعمال جایگشت دوم به عنوان کلید K1 استخراج میشود.

|  |
| --- |
| des premuted choice |
| جدول جایگشت انتخابی دوم |

این فرایند تا شانزده مرحله تکرار می شود. خروجی های بدست امده به عنوان کلید برای فرایند رمزنگاری و رمزگشایی مورد استفاده قرار میگیرد.

تابع اصلی

برای تولید کلید در این روش در چند مرحله صورت می گیرد. شکل زیر این مساله را به درستی روشن می کند:

|  |
| --- |
| DES f KEY Refrence |
| نمودار تولید کلید در روش DES - |

این نمودار شامل تابع کسترش E فرایند جمع کلید و خروجی تابع E, توابع S و تابع فشرده ساز P میباشد که هرکام در جای خود تشریح می شود.

### **تابع P**

قبل ازهر اقدامی طول رشته سمت راست که معادل 32 بیت است می باید افزایش یافته و به 48 بیت برسد. تابع P این کا را با استفاده از جدول زیر انجام میدهد:

|  |
| --- |
| DES E Table |
| جدول انتخاب بیت در تابع E |

تابع E برای گسترش ورودی بر اساس جدول بالا ترکیبی از بیتها را بر اساس توالی موجود در جدول در کنار هم قرارمی دهد. به عنوان مثال برای تولید 6 بیت اول بیتهای 32,1,2,3,4,5 در کنار هم قرار میگیرند و 6 بیت اول را تولید میکنند. برای تولید شش بیت دوم اعداد 4,5,6,7,8,9 در کنار هم قرار میگیرد و شش بیت دوم تولید می شود. این فرایند تا مرحله هشتم ادامه یافته و هشت مجموعه شش بیتی معادل 48 بیت در کنار هم قرار گرفته و خروجی تابع E را تولید میکنند. با بررسی جدول E مشاهده میکنیم تکرار در استفاده از بیتها مشکلی را در اجرا بوجود نخواهد اورد.

### **جمع کردن خروجی تابع E و کلید ورودی**

در این مرحله خروجی تابع E و کلید ورودی با هم جمع میشوند. بیتهای متناظر باهم در این مرحله با استفادر از اپراتور OR جمع خواهند شد.

### **توابع S**

خروجی مرحله قبل 48 بیتی میباشد و می باید به قالب 32 بیتی تبدیل شود. تبدیلات مورد نظر در این مرحله با استفاده از توابع S انجام میشود . این توابع که 8 عدد میباشند ورودی را به صورت 6 بیتی دریافت کرده و خروجی را به صورت 4 بیتی ایجاد میکنند حاصل خروجی این مرحله رشته ای به طول 32 بیت خواهد بود. توابع S برای انجام تبدیلات خود از جداولی مستقل استفاده میکند. این جداول با حرف S و شماره تابع مربوطه تعریف میشود. جدول تابع S1 به صورت زیر است:

|  |
| --- |
| DES S1 Table |
| جدول انتخاب بیت در تابع S1 - مرجع |

براساس ورودی به تابع S1 که یک مقدار 6 بیتی ست, حروف اول و اخر رشته را جدا می کنیم. عدد بدست آمده که عددی دو بیتی است مقادیری بین 0 الی 3 را اتولید نموده که مقدار بدست آمده سطر انتخابی را تعیین میکند. حال به چهار بیت میانی توجه میکنیم عدد بدست امده در مبنای باینری عددی دو رقمی در مبنای 10 را در بازه 0 الی 15 اختیار میکند. بر اساس عدد بدست امده ستون مورد نظر را را تعین میکنم . بر اساس سطر و ستون تعین شده عدد موجود را انتخاب کرده و عدد را به مبنای 2 تبدیل میکنیم عدد تولید شده خروجی تابع S1 می باشد. بعنوان مثال عدد ورودی 101101 را در نظر بگیرید. با انتخاب عدد اول و آخر رشته دو بیتی 11 استخراج می ود این عدد معرف عدد 3 در مبنای 10 است که سطر سوم را تعین میکند. حال چهار بیت میانی را تعین میکنیم که برابر 0110 است این عدد در مبنای 10 برابر عدد 6 خواهد بود که معرف ستون مورد نظر است با انتخاب سطر سوم و ستون ششم به عدد 1 خواهیم رسید که مبنای دوی این عدد برابر 0001 می باشد . این رشته به عنوان خروجی تابع S1 برگردانده خواهد شود.   
توابع S2 الی S8 دارای جداول جداگانه بوده و از همین قانون برای تولید خروجی استفاده میکنند. برای بررسی توابع فوق میتوانید به مستند FIPS46-3 مراجعه نمائید.

### **تابع P**

خروجی توابع S در انتهای فرایند به تابع P وارد میشوند. تابع P وظیفه جایگشت بیتهای ورودی را بر عهده دارد . جایگشت مورد نظر به شرح جدول زیر انجام میشود:

|  |
| --- |
| DES P Table |
| جدول انتخاب بیت در تابع P - مرجع |

خروجی تابع P دارای هیچ تکراری نبوده و به عنوان خروجی تابع اصلی قلمداد می شود.

**رمزگشایی:**

برای رمزگشایی از یک متن رمزشده مانند فرایند رمزنگاری شانزده چرخه محاسباتی خواهیم داشت. چرخه های مورد استفاده به ترتیب عکس فرایند رمزنگاری اجرا خواهند شد مراحل اجرایی به شرح زیر است   
:برای تولید چرخه پانزدهم از چرخه شانزدهم به شرح زیر استفاده میکنیم   
R15=L16   
L15=R16 xor F(L16, K16)   
این فرایند به همین ترتیب تا تولید خروجی مرحله اول ادامه خواهد یافت.