**AES**

**توضیح الگوریتم :**

پیاده سازی الگوریتم AES را میتوان به گونه ای مشابه الگوریتم رمزنگاری DES دانست. در این الگوریتم ترکیبی از رشته های مورد نیاز برای رمزنگاری به عنوان ارایه ورودی درنظر گرفته شده و پس از انتقال آن بر روی یک آرایه میانی عملیات رمزنگاری مورد نیاز انجام می شود. خروجی این مرحله به عنوان متن رمزشده قابل انتقال می باشد. تعاریف زیر میتواند فرایند رمزنگاری در AES را مشخص نماید:   
  
بلاک ورودی و خروجی   
هر مجموله از فرایند های رمزنگاری می بایست برروی رشته هایی از متن ورودی انجام گیرد. در روش AES رشته های ورودی متوانند دارای طولهای 128 بیتی, 192 بیتی و یا 256 بیتی باشند. بر اساس طول بلاک انتخاب شده طول کلید , دفعات اجرای فرایند رمزنگاری متفاوت خواهد بود.   
  
رابطه طول کلید, طول بلاک و تعداد چرخه در روش AES رابطه طول کلید, طول بلاک و تعداد چرخه از جدول زیر تبعیت میکند.

|  |  |  |  |
| --- | --- | --- | --- |
| **تعداد چرخه** | **طول بلاک** | **طول کلید** | **نوع الگوریتم** |
| 10 | 4 | 4 | AES-128 |
| 12 | 4 | 6 | AES-192 |
| 14 | 4 | 8 | AES-256 |

1-برای عملیات رمزنگاری رشته ورودی از آرایه Input برداشته شده و در آرایه State درج می شود. پس از اجرای فرایند که در ادامه شرح داده خواهد شد محتوی ارایه State به آرایه Output انتقال می یابد که به عنوان خروجی به حساب می آید. با توجه به این توضیحات عملیات رمزنگاری بر روی آرایه State انجام شده و بر اساس اجرای چهار روتین نرم افزاری به شرح زیر خواهد بود.   
  
1- SubBytes   
این روتین وظیفه دگرگونی آرایه State را برعهده دارد که نوعی جایگزینی غیر خطی بر روی اعضای آرایه را انجام میدهد.   
  
2 – Row Shift   
این روتین ردیف اول ارایه را به اخر منتقل نموده و سایر ردیف ها را به مقدار یک واحد به بالا انتقال میدهد.   
  
3- MixColumne   
این روتین وظیفه ضرب ستون های آرایه در یک مقدار ثابت و یک پیمانه ریاضی خواهد داشت.   
  
4- AddRoundKey   
این روتین وظیفه XOR نمودن کلید مورد استفاده را بر عهده خواهد داشت. دفعات اعمال کلید بر اساس نوع الگوریتم انتخاب می شود.   
  
تا این مرحله عملیات رمزنگاری انجام پذیرفته و خروجی به آرایه Output منتقل خواهد شد.