**الگوریتم رمزنگاری متقارن 3DES**

با توجه به نقاط ضعف الگوریتم DES و لزوم تقویت ان الگوریتم 3DES معرفی شد. الگوریتم 3DES بر مبنای الگوریتم DES طراحی شده است. وجه تمایز الگوریتم 3DES در اجرای سه مرحله ای آن می باشد. این الگوریتم از سه کلید مجزا برای رمزنگاری استفاده میکند. فرایند های رمزنگاری و رمزگشایی در این روش به شرح زیر می باشد.

**فرایند رمزنگاری:**

O=Ek3(Dk2(Ek1(I)))

1- متن مورد نظر بوسیه الگوریتم DES و کلید k1 رمزنگاری می شود.

2 - خروجی مرحله اول توسط کلید k2 رمزگشایی می شود

3 - خروجی مرحله دوم توسط کلید k3 مجددا رمزنگاری میشود.

**فرایند رمزگشایی:**

I=Dk1(Ek2(Dk3(O)))

1 - متن رمزشده توسط کلید k3 رمزگشایی میشود.

2 - خروجی مرحله اول توسط کلید k2 رمزنگاری می شود.

3 - خروجی مرحله دوم توسط کلید k1 رمزنگاری می شود.

خروجی مرحله سوم به عنوان متن اولیه قابل استفاده خواهد بود. با کمی بررسی مشاهده می شود فرایند رمزگشایی قرینه فرایند رمزنگاری می باشد.

مستند FIPS46-3 ترکیب پیشنهادی زیر را برای انتخاب کلیدهای K1, K2, K3 ارائه می دهد:

1 - K1, K2, K3 مستقل از همدیگر انتخاب شوند.

2 - K1, K2 بطور مستقل از هم انتخاب شده و K1=K3 باشد.

3- K1=K2=K3

