الگوریتم 3DES

الگوریتم DES سه گانه (Triple DES – 3DES) اولین بار در سال ۱۹۸۵ برای استفاده در کاربردهای مالی، با نام X9.17 در استانداردهای ANSI ثبت گردید. **روش ۳DES** با انتشار FIPS PUB 46.3 در سال ۱۹۹۹ به عنوان بخشی از استاندارد رمزنگاری دیتا (DES) بکار گرفته شد. **الگوریتم ۳DES** از سه کلید و سه بار اجرای الگوریتم DES استفاده می کند. تابع از یک دنباله رمزنگاری – رمزگشائی – رمزنگاری (EDE) تبعیت می کند

C = E(K3 , D(K3 , E(K1 , P)))

که در آن

متن رمز شده C = (ciphertext)

متن ساده P = (plaintext)

رمزنگاری X با استفاده از کلید E [K,X] = K

رمزگشائی Y با استفاده از کلید D [K,X] = K

رمزگشائی بسادگی همان عملیات قبل است که ترتیب کلیدها در آن عوض شده است.

P = D(K1 , E(K2  , D(K3 , C)))

از نظر رمزنگاری، هیچ ویژگی خاصی در استفاده از رمز گشائی مرحله دوم **رمزنگاری ۳DES** وجود ندارد. تنها حسن آن این است که به کاربران ۳DES اجازه میدهد تا داده هائی را که توسط فرم قدیمی DES رمزنگاری شده بودند، رمز گشائی نمایند:

C = E(K1 , D(K1 , E(K1 , P))) = E[K , P]

با سه کلید متمایز، ۳DES دارای کلیدی با طول مؤثر ۱۶۸ بیت است. FIPS 46.3 همچنین استفاده از دو کلید، K1 = K3 را اجازه میدهد که در این مورد طول کلید ۱۱۲ بیت خواهد بود. FIPS 46.3 شامل سه دستورالعمل زیر برای ۳DES است:

* الگوریتم ۳DES روش رمزنگاری متقارن منتخب و تأئید شده توسط FIPS است.
* الگوریتم DES اولیه که از یک کلید ۵۶ بیتی استفاده می کند و تنها در استاندارد سیستم هائی که وارث آن هستیم مجاز می باشد. ساختار های جدید بایستی از ۳DES حمایت نمایند.
* توصیه می شود که سازمان های دولتی، سیستم های موروثی DES را با ۳DES تعویض نمایند.
* پیش بینی می شود که ۳DES و AES در کنار هم، به عنوان الگوریتم های پذیرفته شده FIPS همزیستی داشته و در طول زمان بتدریج ۳DES حذف و AES استاندارد غالب شود.

به سهولت می توان دریافت که ۳DES یک الگوریتم نیرومند است. چون الگوریتم رمزنگاری بستر آن DEA (Data Encryption Algorithm) است، ۳DES می تواند در مقابل تلاش های مربوط به کشف رمز، همان ادعاهای DEA را داشته باشد. علاوه بر آن با یک کلید ۱۶۸ بیتی، حمله همه جانبه به آن عملا غیرممکن است. بالاخره و در نهایت قرار است AES جایگزین ۳DES شود، ولی این تحول سال ها طول خواهد کشید (این نوشته برای ۲۰۰۷ است). NIST پیش بینی می کند که ۳DES برای آینده ای قابل پیش بینی، الگوریتم موفقی باشد.