Standard (DES) نوعی رمزنگاری رایانه ای است که الگوریتم های رمزنگاری بلوک سه بار به هر بلوک داده اعمال می شود. برای اطمینان از امنیت بیشتر از طریق قابلیت رمزگذاری ، اندازه کلید در Triple DES افزایش می یابد. هر بلوک شامل 64 بیت داده است. از سه کلید به عنوان کلیدهای بسته ای با 56 بیت در هر کلید استفاده می شود. در استانداردهای رمزگذاری داده سه گزینه کلید وجود دارد:

همه کلیدها مستقل هستند

کلید 1 و کلید 2 کلیدهای مستقلی هستند

هر سه کلید یکسان هستند

گزینه اصلی شماره 3 به عنوان triple DES شناخته می شود. طول کلید DES سه گانه شامل 168 بیت است اما امنیت کلید به 112 بیت می رسد.

Techopedia Triple DES را توضیح می دهد

Triple DES دارای مزیت است زیرا دارای طول کلید قابل توجهی است که از بیشتر طول کلیدهای وابسته به سایر حالت های رمزگذاری بیشتر است. با این حال ، الگوریتم DES با استاندارد رمزگذاری پیشرفته توسط انستیتوی استاندارد ملی و فناوری (NIST) جایگزین شد. بنابراین ، Triple DES اکنون منسوخ شده در نظر گرفته شده است. با این حال ، آن را اغلب همراه با Triple DES استفاده می شود. این روش از تک DES ناشی می شود اما این تکنیک در سه نسخه استفاده می شود و در صورت لزوم شامل سه کلید فرعی و کلید بالشتک است ، مانند مواردی که طول کلیدها باید به 64 بیت افزایش یابد. این نرم افزار به دلیل سازگاری و انعطاف پذیری مشهور است ، به راحتی می تواند برای Triple DES تبدیل شود. بنابراین ، ممکن است تقریباً به همان اندازه منسوخ شده باشد که توسط NIST در نظر گرفته شده است.

Triple DES سه بار داده ورودی را رمزگذاری می کند. به سه کلید k1 ، k2 و k3 گفته می شود. این فناوری در استاندارد ANSIX9.52 موجود است. Triple DES با DES معمولی سازگار است.