

Triple DES

در رمزنگاری، Triple DES نام متداولی است برای بلاک رمز، الگوریتم بین‌المللی رمزگذاری داده‌ها سه‌گانه (TDEA یا TRIPLE DEA)، که الگوریتم استاندارد رمزنگاری داده را سه بار بر روی هر بلاک داده اعمال می‌نماید.

سایز اصلی کلید کد DES 168 بیتی است که زمانیکه این الگوریتم طراحی شد کارا بود اما با افزایش توان محاسباتی امکان حملات Brute-Force وجود دارد. DES سه‌گانه یک شیوه نسبتاً ساده از افزایش سایز کلید DES به منظور حفاظت در مقابل حملات، بدون نیاز به طراحی یک الگوریتم با کد جدید فراهم می‌سازد.

DES سه گانه یک «مجموعه کلید رمز کلید» که شامل سه کلید (K1، K2، K3) که هر کدام شامل ۵۶ بیت (به جز بیت‌های پر تیر) هستند را به کار می‌برد.

الگوریتم رمزنگاری اینجنین است:

متن رمز شده = $Enc_{K1}(Dec_{K2}(Enc_{K3}(\text{متن اصلی})))$

یعنی DES با K1 رمزگذاری می‌نماید با کلید K2 رمزگشایی می‌نماید و سپس با K3 رمزگذاری می‌نماید، رمزگشایی به صورت معکوس صورت می‌گیرد.

پایاده سازی در cryptool:

ابتدا در قسمت `templates>>Cryptography>>Modern>>Triple DES Cipher` را باز می کنیم.

در قسمت Plaintext متن اصلی Sepide Omidvar را وارد می کنیم. در قسمت Key کلید را
۱۱.....۱۱ نظر میگیریم. با زدن کلید start متن رمز شده 08 07 9A 60 D3 6C 55 8B AF 29 65 53 45 0C 76 5F خواهد بود.

