Triple DES

در رمزنگاری،Triple DES نام متداولی است برای بلاک رمز، الگوریتم بین‌المللی رمزگذاری داده‌ها سه‌گانه (TDEAیا 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.

DESسه‌گانه یک «مجموعه کلید رمزکلید» که شامل سه کلید(K1،K2، DES (K1۳، Kکه هر کدام شامل ۵۶ بیت (به جز بیت‌های پریتی) هستند را به کار می‌برد.

الگوریتم رمزنگاری اینچنین است:

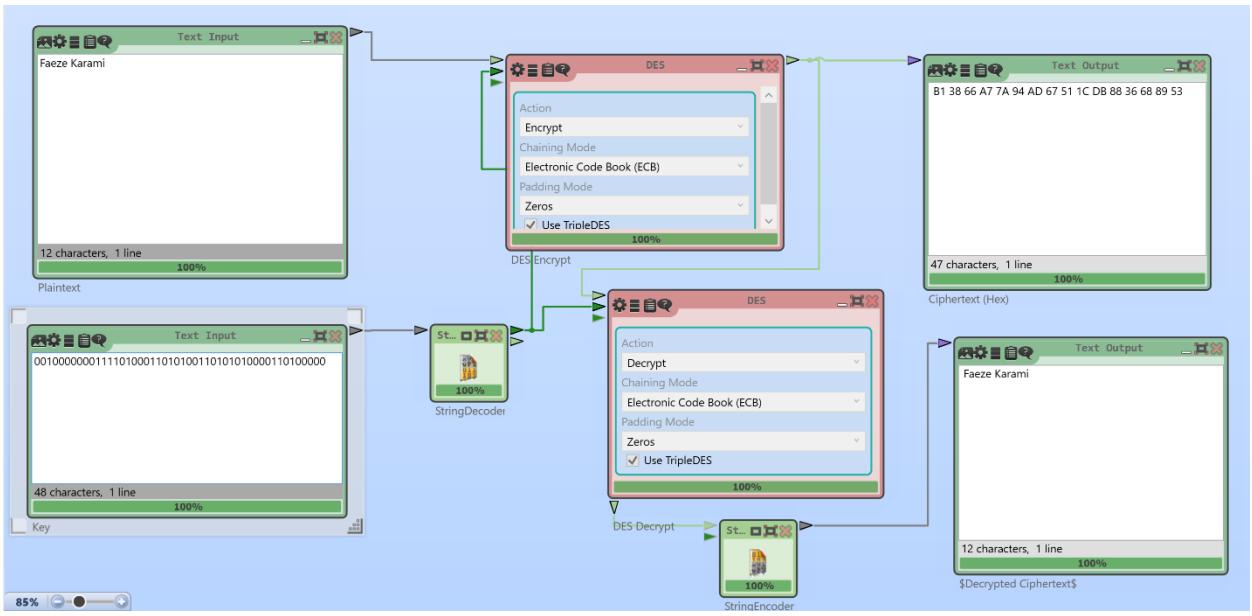
متن رمز شده=Enc_{K1}(Dec_{K2}(Enc_{K3}((متن اصلی)

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

پیاده سازی در cryptool:

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

در قسمت Plaintext متن اصلی Faeze Karami را وارد می کنیم. در قسمت Key کلید را ۰۰۱۰۰۰۰۰۰۰۱۱۱۱۰۱۰۰۰۱۱۰۱۰۱۰۰۱۱۰۱۰۱۰۱۰۰۰۰۱۱۰۱۰۰۰۰۰ نظر میگیریم. با زدن کلید start متن رمز شده B1 38 66 A7 7A 94 AD 67 51 1C DB 88 36 68 89 53F خواهد بود.


Text Input
Faeze Karami
12 characters, 1 line
100%
Plaintext
DES
Action
Encrypt
Chaining Mode
Electronic Code Book (ECB)
Padding Mode
Zeros
Use TrioleDES
100%
DES Encrypt
Text Output
B1 38 66 A7 7A 94 AD 67 51 1C DB 88 36 68 89 53
47 characters, 1 line
100%
Ciphertext (Hex)
Text Input
00100000001111010001101010011010101000011010000 0
48 characters, 1 line
100%
Key
St...
100%
StringDecoder
DES
Action
Decrypt
Chaining Mode
Electronic Code Book (ECB)
Padding Mode
Zeros
Use TripleDES
100%
DES Decrypt
St...
100%
StringEncoder
Text Output
Faeze Karami
12 characters, 1 line
100%
$Decrypted Ciphertext$
85%