**3DES czyli Triple\_DES**

Ogólnie rzecz biorąc, Triple DES z trzema niezależnymi kluczami ma długość klucza 168 bitów (trzy 56-bitowe klucze DES), ale ze względu na atak typu „**meet-in-the-middle**” skuteczne bezpieczeństwo zapewnia tylko 112 bitów. Opcja kluczowania 2 zmniejsza efektywny rozmiar klucza do 112 bitów (ponieważ trzeci klucz jest taki sam jak pierwszy). Jednak ta opcja jest podatna na pewne ataki z wybranym tekstem jawnym lub znanym tekstem jawnym, i dlatego NIST określił, że ma tylko 80 bitów bezpieczeństwa. Można to uznać za niebezpieczne, w wyniku czego Triple DES został wycofany przez NIST w 2017 roku.

Krótki blok 64-bitowy sprawia, że ​​3DES jest podatny na blokowanie ataków **kolizyjnych**, jeśli jest używany do szyfrowania dużych ilości danych tym samym kluczem. Atak **Sweet32** pokazuje, jak można to wykorzystać w TLS i OpenVPN. Praktyczny atak **Sweet32** na zestawy szyfrów oparte na 3DES w TLS wymagane 2^36.6 bloki (785 GB) dla pełnego ataku, ale naukowcy mieli szczęście dostać tylko kolizję po około 2^20 blokach, co zajęło tylko 25 minut.

Czyli już mamy takie różne ataki:

* **Brute-force**

Technika łamania haseł lub kluczy kryptograficznych polegająca na sprawdzeniu wszystkich możliwych kombinacji. Jest to prosta metoda pozwalająca w teorii na odgadnięcie każdego klucza. Metoda ta ma jednak dużą złożoność obliczeniową, w związku z czym dla odpowiednio długich kluczy złamanie klucza tą metodą jest praktycznie niemożliwe

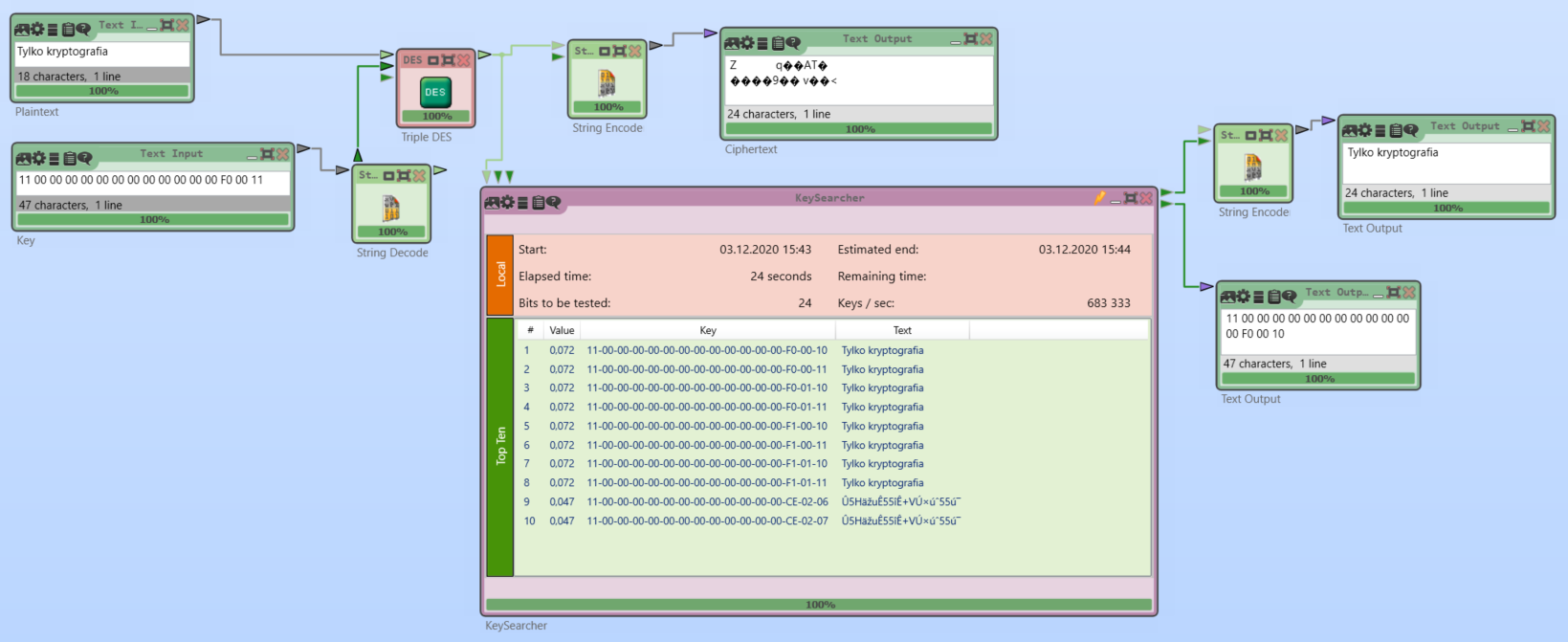
* **Known-plaintext**

Jedna z najpopularniejszych metod łamania szyfrów, która zakłada, że kryptoanalityk dysponuje zarówno szyfrogramami, jak i ich tekstami jawnymi, dzięki którym ma możliwość uzyskania klucza szyfrującego. Istnieje wiele sposobów zdobycia szyfrogramu danego tekstu jawnego: może zostać przechwycony lub przekupiona osoba może zaszyfrować konkretny tekst jawny. W przypadku algorytmów z kluczem publicznym uzyskanie szyfrogramu z tekstu jawnego nie jest żadnym problemem

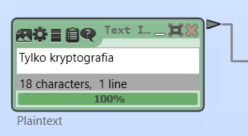
* **Atak ze spodziewanym tekstem jawnym**
* **Meet in the middle**

Jest rodzajem ataku kryptograficznego z jawnym tekstem. Do jego przeprowadzenia konieczna jest znajomość zarówno tekstu jawnego, jak i zaszyfrowanego (atak ze znanym tekstem jawnym). Algorytmami podatnymi na tego rodzaju ataki są algorytmy używające 2 lub więcej kluczy do wielokrotnego szyfrowania tym samym algorytmem np. 3DES.

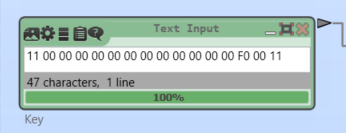
**Przykład ataku Brute-force**



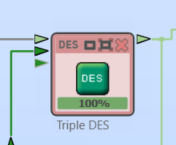
Na początku mamy tekst jawny do szyfrowania



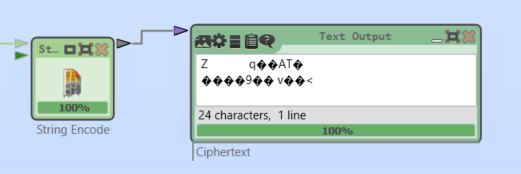
Mamy wygenerowany losowy klucz



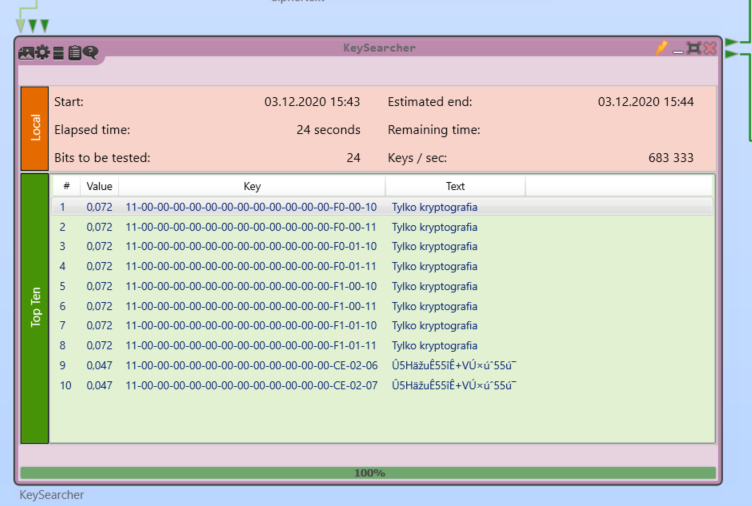
Szyfrujemy przez 3DES uważając, że tych danych mu nie znamy



Po szyfrowaniu otrzymujemy szyfrogram



Do generatora kluczów podłączamy szyfrogram

  
Po skończeniu generowania różnych kluczów otrzymujemy takie wyniki. Dla wygodniejszego wyglądu możemy te wyniki pobrać w bloki Textoutput. Ale to jest nie konicznie, tak jak w KeySearcheru już mamy wszystko potrzebne. Generowanie kluczów nie jest szybkim algorytmem, dlatego dla gużych tektów jawnych zajęło by to znacznie więcej czasu.