**DES АЛГОРИТМЫ**

**DES (Data Encryption Standard) –** блоктық шифрлау алгоритмі, 64 биттік блоктарды 56 биттік кілт арқылы шифрлайды. Бұл алгоритм симметриялық болып табылады, яғни дешифрлау сол кілтті қолдану арқылы орындалады.Бұл жерде біз  **DES алгоритмын** пайдаланып, мәтінді шифрлау процесін қарастырамыз.

**1. Жаңа жобаны бастау**

**Home → Жаңа (New)** таңдаңыз. Жаңа жұмыс кеңістігі (Workspace) ашылады.

Қажетті блоктарды жобаға қосамыз:

* Text Input(2 дана, біреуі шифрланатын мәтін , кілт)
* Text Output(Шифрланған мәтінді алу)
* DES Visualization (DES блогы)
* String Decoder (Жолды кодтау)

**Text Input (Мәтін енгізу)**

**Мақсаты:**Бұл блок арқылы ашық мәтінді және кілтті енгіземіз. DES 64 биттік блоктармен жұмыс істейтіндіктен, мәтін ұзындығы 64 биттен кем болмауы керек.

**Екі Text Input блогы қажет:**

* Біріншісі шифрланатын мәтін үшін.
* Екіншісі кілт үшін.

**DES Visualization (DES блогы)**

**Мақсаты:** Бұл блок DES алгоритмінің қалай жұмыс істейтінін визуалды түрде көрсетеді. Шифрлау немесе дешифрлау операциясын орындау үшін қолданылады.

**Параметрлері:**

* ECB (Electronic Codebook) немесе CBC (Cipher Block Chaining).
* Encrypt (Шифрлау) немесе Decrypt (Дешифрлау).

**String Decoder (Жолды кодтау)**

**Мақсаты:**

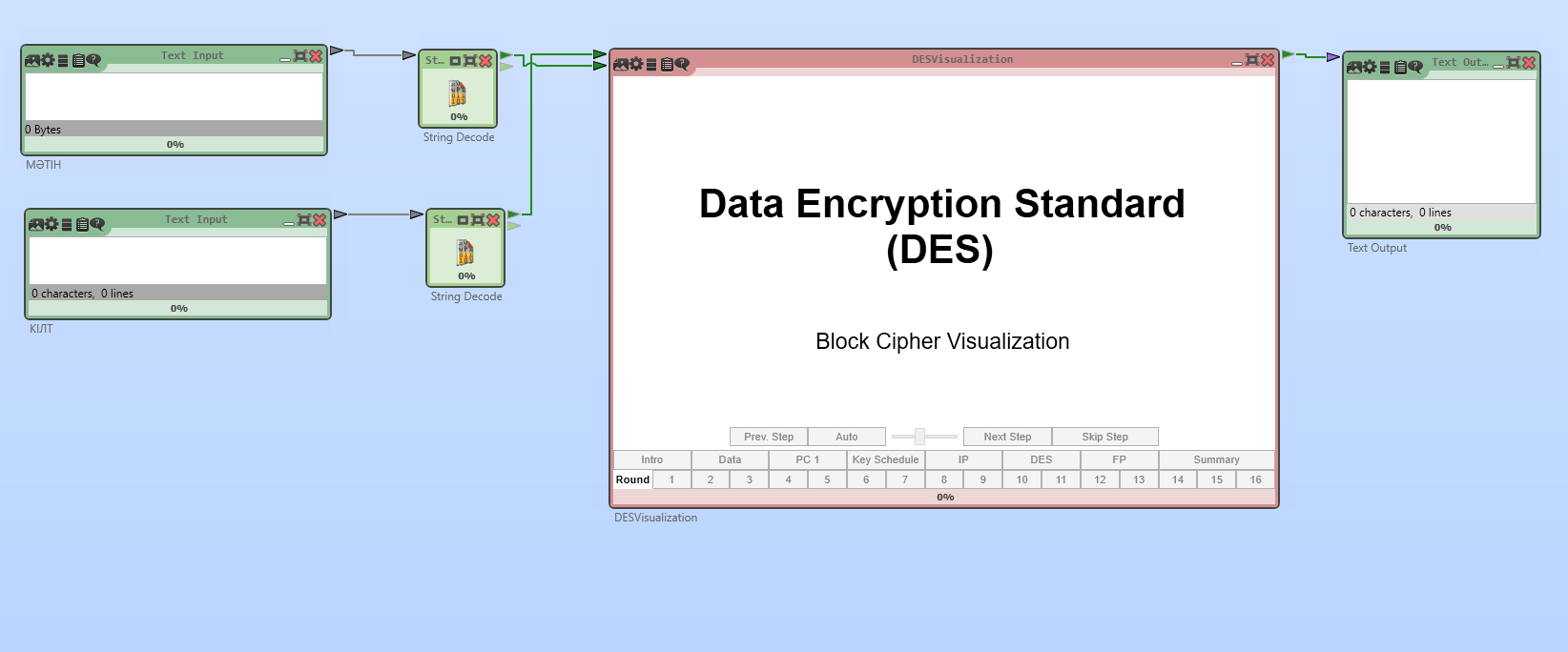
* DES шифрланған мәтін бинарлық немесе HEX кодта болуы мүмкін, оны оқылатын мәтінге түрлендіру үшін String Decoder қолданылады.

**Text Output (Мәтін шығару)**

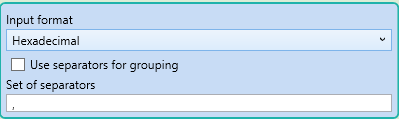
**Мақсаты:**

* Бұл блок DES шифрланған немесе дешифрланған мәтінді көрсетеді.
* Егер шифрланған мәтін бинарлы түрінде болса, қажет онда алдымен String Encoder қолданылады.

**2. Блоктарды суреттегідей байланыстыру**

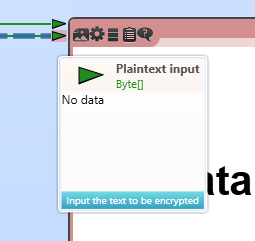
****

**String Decoder (Жолды кодтау)** блогының параметрін келесідей өзгертеміз.

****

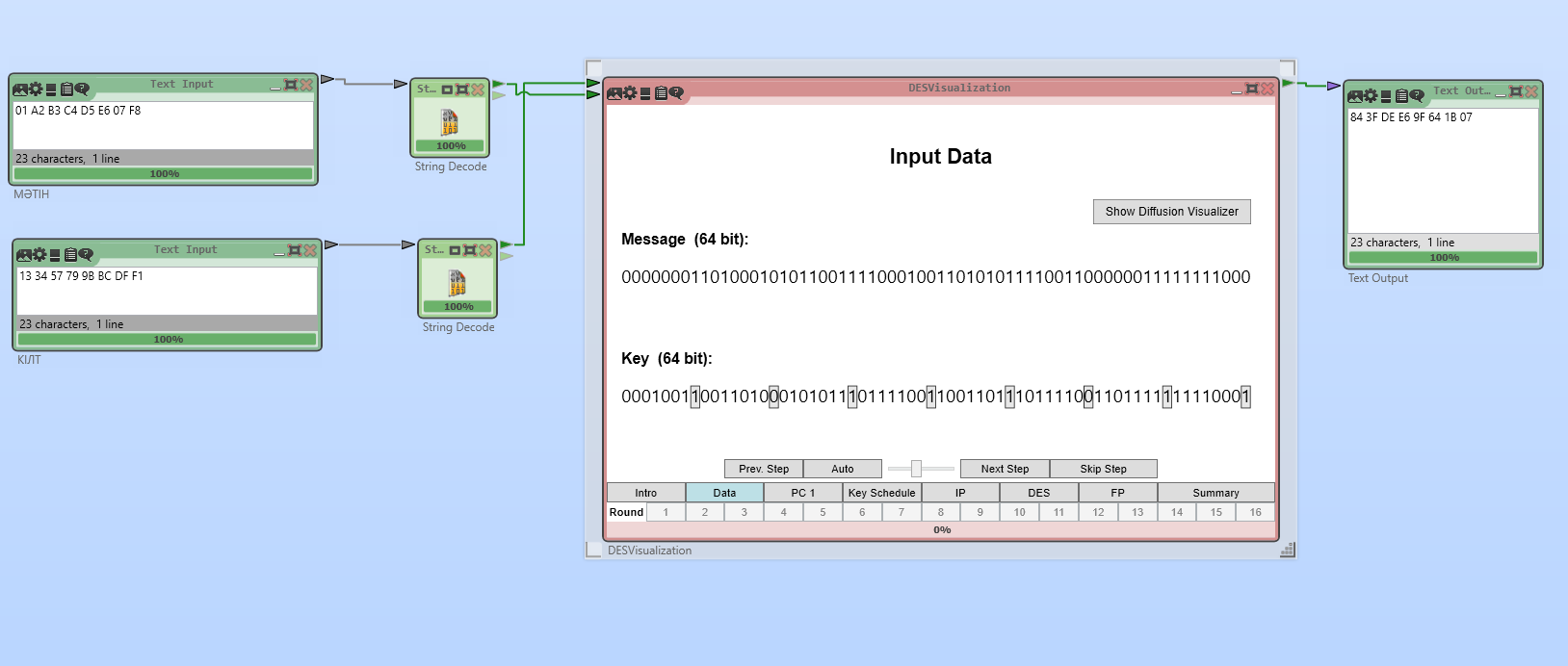
**ЕСКЕРТУ**

*БЛОГТАРДЫ ӨЗАРА БАЙЛАНЫСТЫРҒАН КЕЗДЕ , БАЙЛАНЫС НҮКТЕЛЕРІНІҢ АНЫҚТАМАСЫНА МӘН БЕРІҢІЗ. АНЫҚТАМАСЫН БАЙЛАНЫС НҮКТЕСІНЕ ТІНТУІРДІ АПАРСАНЫЗ ЖЕТКІЛІКТІ. БАЙЛАНЫС НҮКТЕЛЕРІ БІР-БІРІМЕН ДҰРЫС БАЙЛАНЫСҚАНЫ ЖӨН.*

**

**3. Мәндерді енгізіп нәтижені көру**

"Play" (▶) түймесін басып, шифрлау нәтижесін қараңыз.



01 A2 B3 C4 D5 E6 07 F8 мәтінің 13 34 57 79 9B BC DF F1 кілті арқылы шифрлап, **"** **84 3F DE E6 9F 64 1B 07"**  шифрланған мәтінін алдық. Бұл HEX түріндегі шифрланған мәлімет**.**

**Қорытынды**

* DES – 64 биттік блоктармен жұмыс істейтін симметриялық шифрлау алгоритмі.
* Cryptool 2-де бұл алгоритмді оңай қолданып, шифрлау және дешифрлау процесін көрнекі түрде тексеруге болады.
* DES Visualization блогы арқылы алгоритмнің әр қадамын мәтінді толықтай шифрлағанға дейін көре аламыз.

**ПРАКТИКАЛЫҚ ТАПСЫРМА**

**1-тапсырма: Шифрлау**

Теориялық бөлімде талданған мысалдың дұрыс екендігіне көз жеткізіңіз.

**2-тапсырма: Дешифрлау**

Мысалдағы "**84 3F DE E6 9F 64 1B 07** " шифрланған мәтінін  дефирлаңыз(Ол үшін DES блогын қолданыңыз).