WEK 3

Arkadiusz Ostrzyżek

1.

a)

128)

TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 2D A1 B5 77 8C B2 E7 44 A3 62 C8 B4 FF 6D 93 7B

KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

192)

TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25 55 17 5D CC
UZYSKANY SZYFROGRAM: 20 85 80 C1 90 EA E2 1E 36 C8 5E 8F 8D DD B4 41 1E 77 14 4C 33 07 42 F3 42 DB AC 91 41 94 05 D7

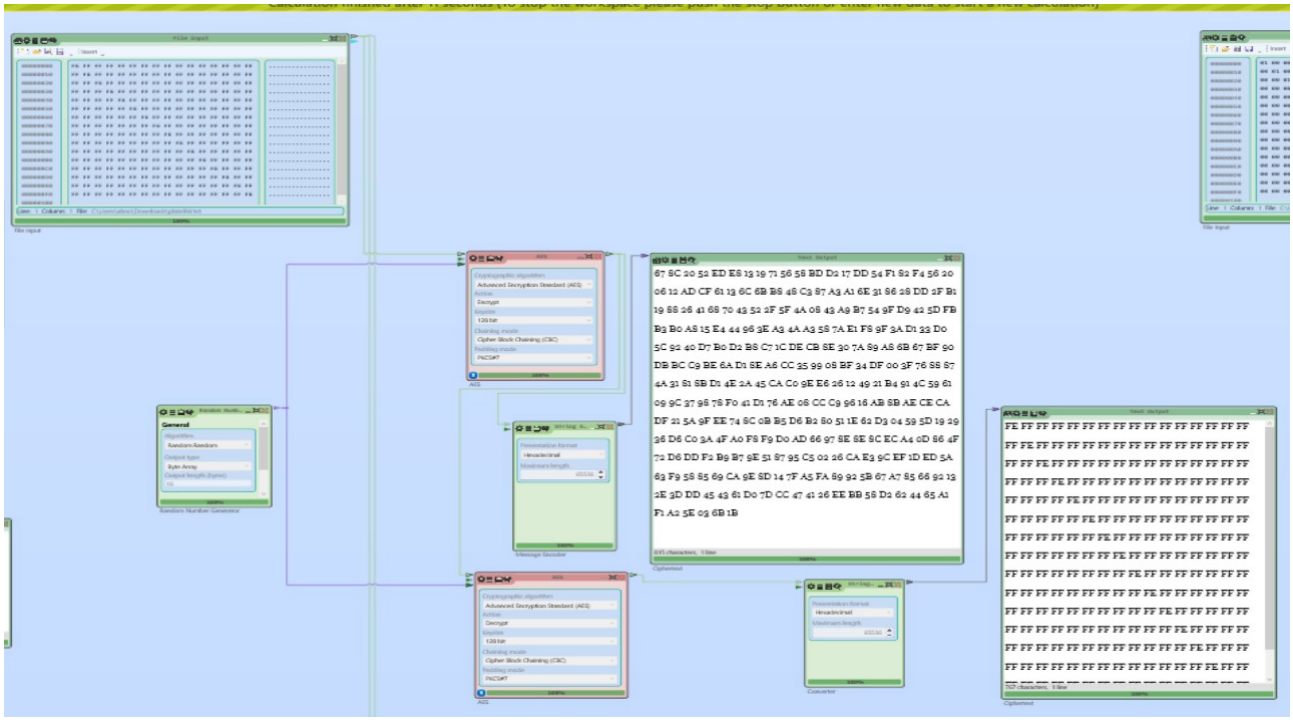
KLUCZ:  3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25 55 17 5D CC
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

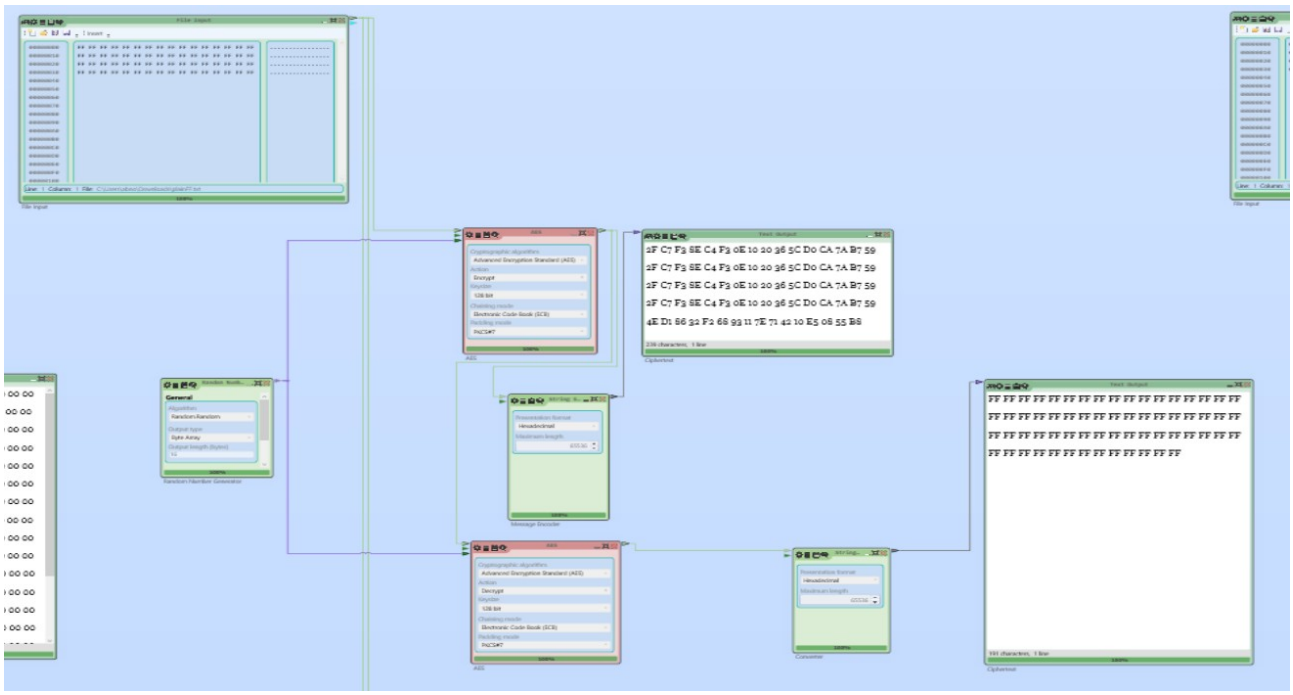
256)

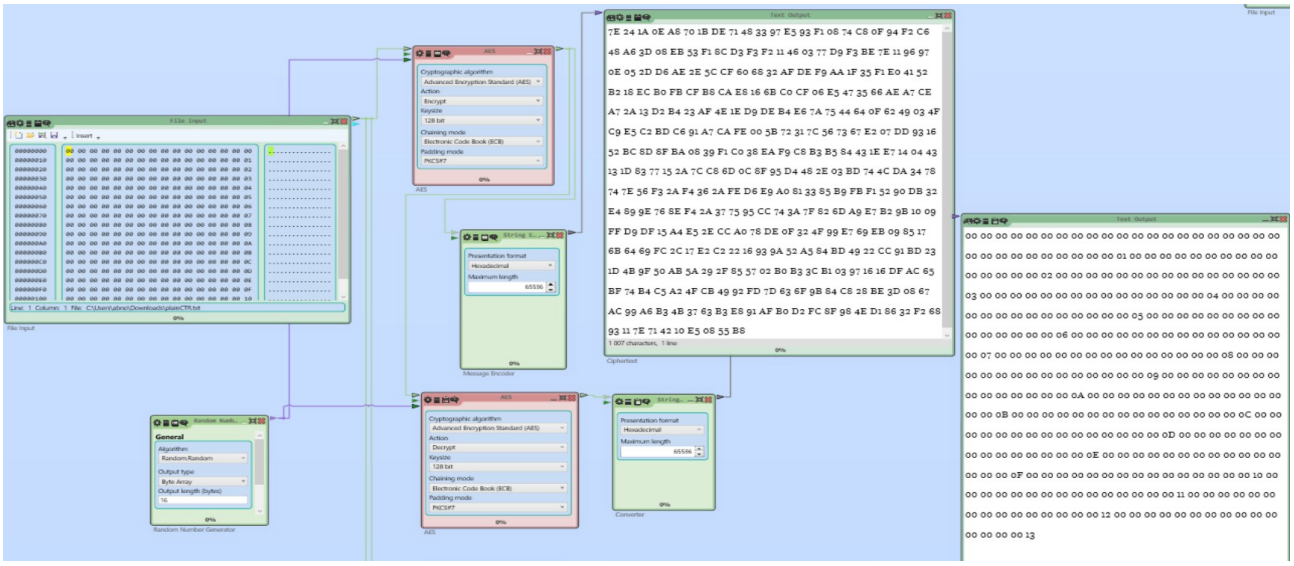
TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25 55 17 5D CC 6E 8B 09 14 57 9A B0 36
UZYSKANY SZYFROGRAM: 2F 6E 53 76 1A 1E EB 7B 6C E6 FA 10 C1 8B 89 10 57 32 2A 07 A3 D2 BF 05 8A AA B5 76 90 21 DA 55

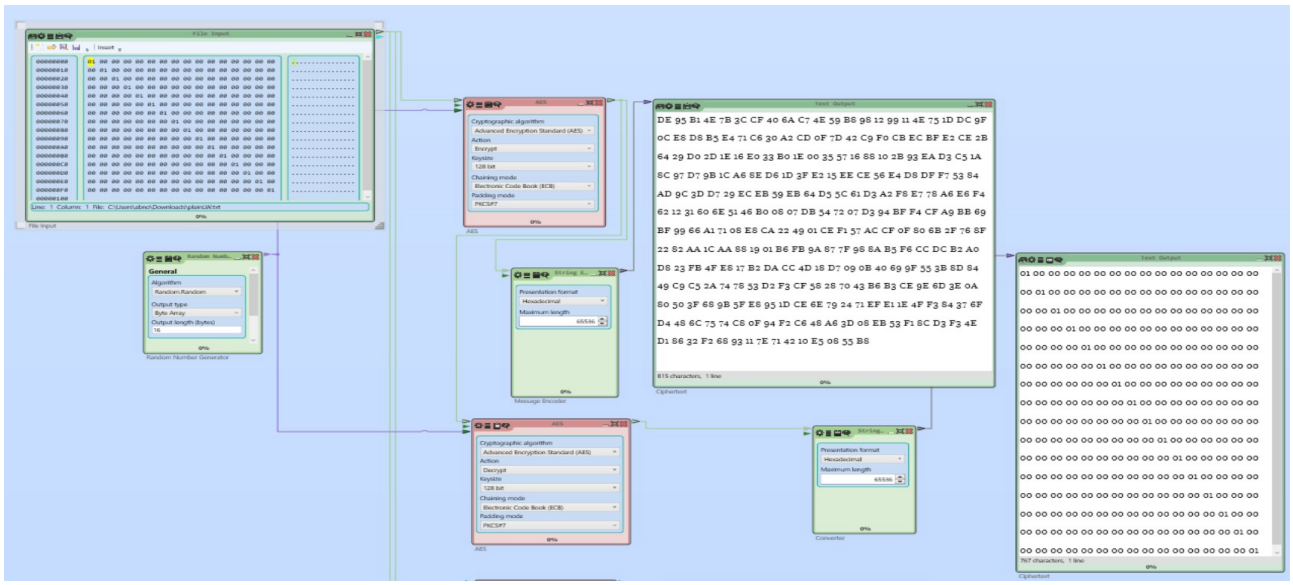
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A 6F B7 4D 25 55 17 5D CC 6E 8B 09 14 57 9A B0 36
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

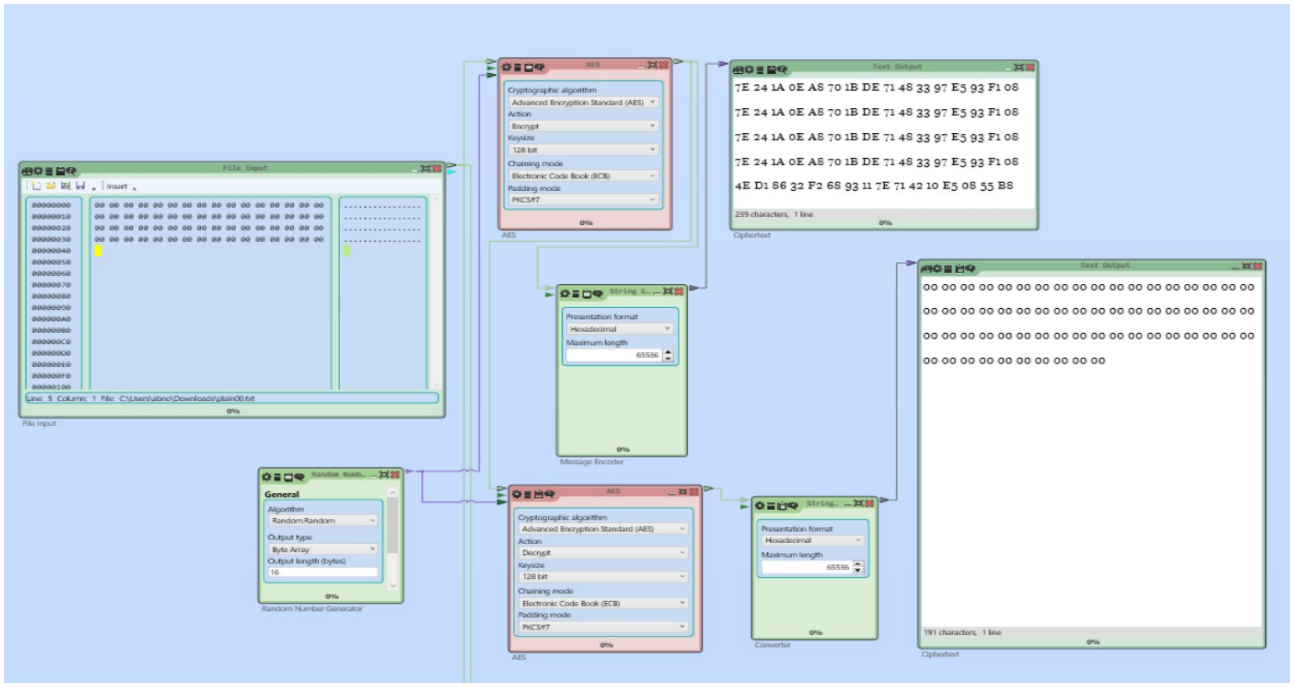

b)
Dla plików plain00.txt, plainFF.txt mają powtarzające się ciągi. Reszta plików takich nie ma.
Jest tak, ponieważ takie same dane są szyfrowane zawsze w ten sam sposób w trybie EBC.
Plik plain00.txt jest wypełniony zerami.
Plik plainFF.txt jest wypełniony FF.
Plik plainCRT.txt ma co 16 bajt równy ilości rzędów. Reszta jest wypełniona zerami.
Plik plainBW.txt ma “na ukos” FE, reszta bajtów wynosi FF.
Plik plainLW.txt ma “na ukos” 01, reszta bajtów wynosi 00.


67 8C 20 52 ED E8 13 19 71 56 58 BD D2 17 DD 54 F1 82 F4 56 20
06 12 AD CF 61 13 6C 6B B6 46 C3 87 A3 A1 6E 31 86 28 DD 2F B1
19 88 26 41 68 70 43 52 2F 5F 4A 08 43 A9 B7 54 9F D9 42 5D FB
B3 B0 A8 15 E4 44 96 3E A3 4A A3 58 7A E1 F8 9F 3A D1 33 D0
5C 92 40 D7 B0 D2 B8 C7 1C DE CB 8E 30 7A 89 A8 6B 67 BF 90
DB BC C9 BE 6A D1 8E A6 CC 25 99 08 BF 34 DF 00 3F 76 88 87
4A 31 81 8B D1 4E 2A 45 CA C0 9E E6 26 12 49 21 B4 91 4C 59 61
09 9C 37 98 78 F0 41 D1 76 AE 08 CC C9 96 16 AB 8B AE CE CA
DF 21 5A 9F EE 74 8C 0B B5 D6 B2 80 51 1E 62 D3 04 59 5D 19 29
36 D6 C0 3A 4F A0 F8 F9 D0 AD 66 97 8E 8E 8C EC A4 0D 86 4F
72 D6 DD F2 B9 B7 9E 51 87 95 C5 02 26 CA E3 9C EF 1D ED 5A
63 F9 58 85 69 CA 9E 8D 14 7F A5 FA 89 92 5B 67 A7 85 66 92 13
2E 3D DD 45 43 61 D0 7D CC 47 41 26 EE BB 58 D2 62 44 65 A1
F1 A2 5E 03 6B 1B


2F C7 F3 8E C4 F3 0E 10 20 36 5C D0 CA 7A B7 59
2F C7 F3 8E C4 F3 0E 10 20 36 5C D0 CA 7A B7 59
2F C7 F3 8E C4 F3 0E 10 20 36 5C D0 CA 7A B7 59
2F C7 F3 8E C4 F3 0E 10 20 36 5C D0 CA 7A B7 59
4E D1 86 32 F2 68 93 11 7E 71 42 10 E5 08 55 B8


7E 24 1A 0E A8 70 1B DE 71 48 33 97 E5 93 F1 08 74 C8 0F 94 F2 C6
48 A6 3D 08 EB 53 F1 8C D3 F3 F2 11 46 03 77 D9 F3 BE 7E 11 96 97
0E 05 2D D6 AE 2E 5C CF 60 68 32 AF DE F9 AA 1F 35 F1 E0 41 52
B2 18 EC B0 FB CF B8 CA E8 16 6B C0 CF 06 E5 47 35 66 AE A7 CE
A7 2A 13 D2 B4 23 AF 4E 1E D9 DE B4 E6 7A 75 44 64 0F 62 49 03 4F
C9 E5 C2 BD C6 91 A7 CA FE 00 5B 72 31 7C 56 73 67 E2 07 DD 93 16
52 BC 8D 8F BA 08 39 F1 C0 38 EA F9 C8 B3 B5 84 43 1E E7 14 04 43
13 1D 83 77 15 2A 7C C8 6D 0C 8F 95 D4 48 2E 03 BD 74 4C DA 34 78
74 7E 56 F3 2A F4 36 2A FE D6 E9 A0 81 33 85 B9 FB F1 52 90 DB 32
E4 89 9E 76 8E F4 2A 37 75 95 CC 74 3A 7F 82 6D A9 E7 B2 9B 10 09
FF D9 DF 15 A4 E5 2E CC A0 78 DE 0F 32 4F 99 E7 69 EB 09 85 17
6B 64 69 FC 2C 17 E2 C2 22 16 93 9A 52 A5 84 BD 49 22 CC 91 BD 23
1D 4B 9F 50 AB 5A 29 2F 85 57 02 B0 B3 3C B1 03 97 16 16 DF AC 65
BF 74 B4 C5 A2 4F CB 49 92 FD 7D 63 6F 9B 84 C8 28 BE 3D 08 67
AC 99 A6 B3 4B 37 63 B3 E8 91 AF B0 D2 FC 8F 98 4E D1 86 32 F2 68
93 11 7E 71 42 10 E5 08 55 B8


DE 95 B1 4E 7B 3C CF 40 6A C7 4E 59 B8 98 12 99 11 4E 75 1D DC 9F
0C E8 D8 B5 E4 71 C6 30 A2 CD 0F 7D 42 C9 F0 CB EC BF E2 CE 2B
64 29 D0 2D 1E 16 E0 33 B0 1E 00 35 57 16 88 10 2B 93 EA D3 C5 1A
8C 97 D7 9B 1C A6 8E D6 1D 3F E2 15 EE CE 56 E4 D8 DF F7 53 84
AD 9C 3D D7 29 EC EB 59 EB 64 D5 5C 61 D3 A2 F8 E7 78 A6 E6 F4
62 12 31 60 6E 51 46 B0 08 07 DB 54 72 07 D3 94 BF F4 CF A9 BB 69
BF 99 66 A1 71 08 E8 CA 22 49 01 CE F1 57 AC CF 0F 80 6B 2F 76 8F
22 82 AA 1C AA 88 19 01 B6 FB 9A 87 7F 98 8A B5 F6 CC DC B2 A0
D8 23 FB 4F E8 17 B2 DA CC 4D 18 D7 09 0B 40 69 9F 55 3B 8D 84
49 C9 C5 2A 74 78 53 D2 F3 CF 58 28 70 43 B6 B3 CE 9E 6D 3E 0A
80 50 3F 68 9B 5F E8 95 1D CE 6E 79 24 71 EF E1 1E 4F F3 84 37 6F
D4 48 6C 75 74 C8 0F 94 F2 C6 48 A6 3D 08 EB 53 F1 8C D3 F3 4E
D1 86 32 F2 68 93 11 7E 71 42 10 E5 08 55 B8


7E 24 1A 0E A8 70 1B DE 71 48 33 97 E5 93 F1 08
7E 24 1A 0E A8 70 1B DE 71 48 33 97 E5 93 F1 08
7E 24 1A 0E A8 70 1B DE 71 48 33 97 E5 93 F1 08
7E 24 1A 0E A8 70 1B DE 71 48 33 97 E5 93 F1 08
4E D1 86 32 F2 68 93 11 7E 71 42 10 E5 08 55 B8

2.
a)

1. PCKS#7 – dodawane jest x bajtów o wartości 0x.

TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 C7 1A 56 CF 57 95 7F 5C 7B 0E AB C6 35 00 20 6E
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

2. ANSI X9.23 – dodawane jest x-1 bajtów 00. Ostatni ma wartość 0x.

TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 1C C7 37 CC 4F D7 D5 DC 8E 06 3C 37 F6 65 17 A7
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

3. ISO 10126 – dodawane jest x-1 losowych bajtów. Ostatni ma wartość x.

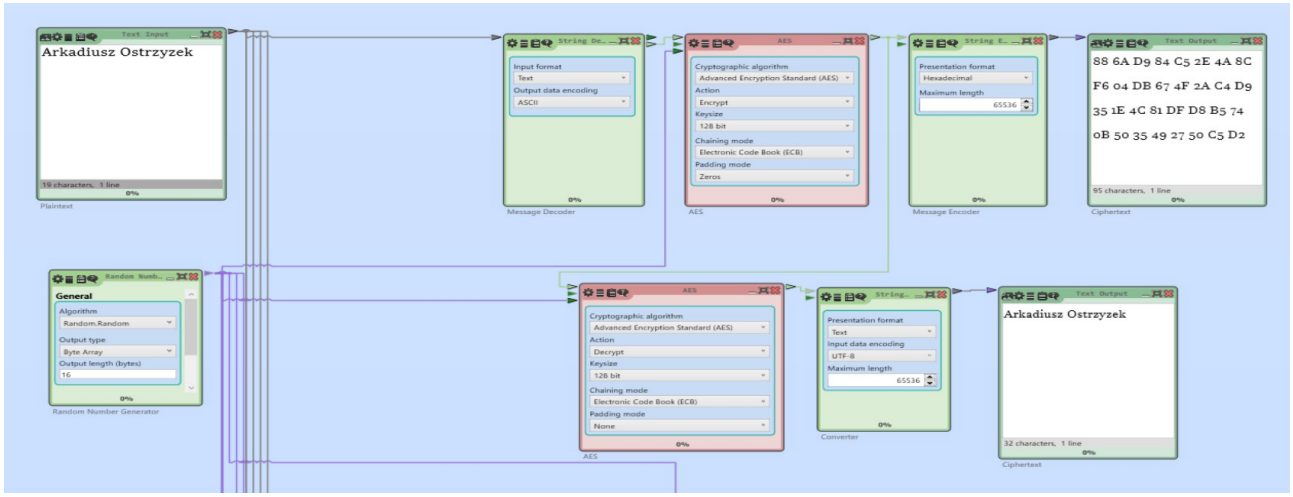
TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 7B C1 57 34 38 F3 68 3D 7B 23 DC 7C 63 27 67 B2
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

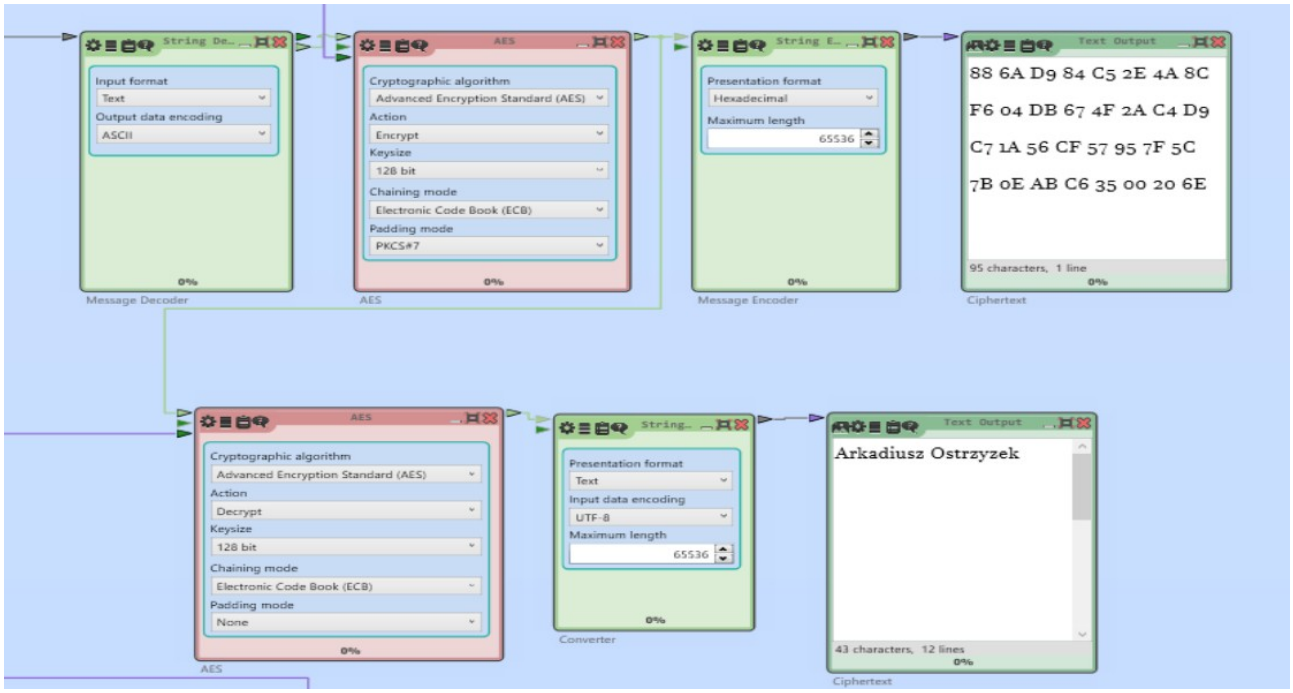
4. 1-0 – dodawane jest 1, a potem 0 do konca bloku.

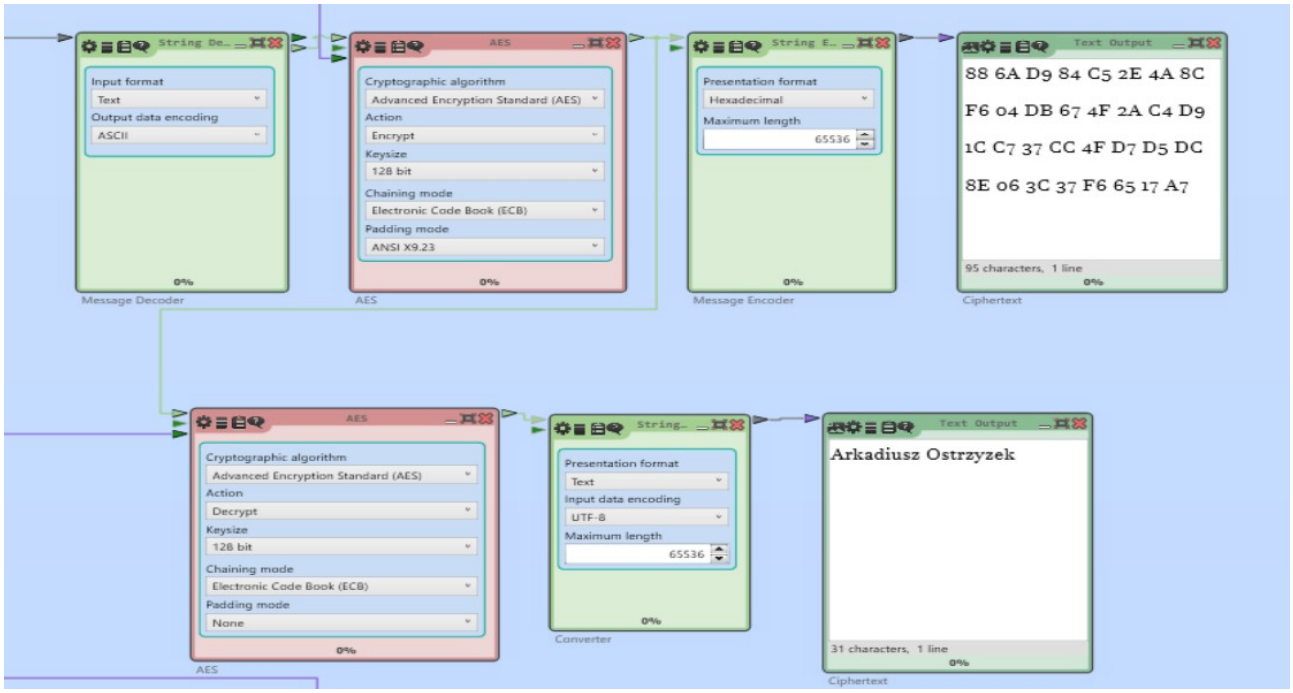
TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM:
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

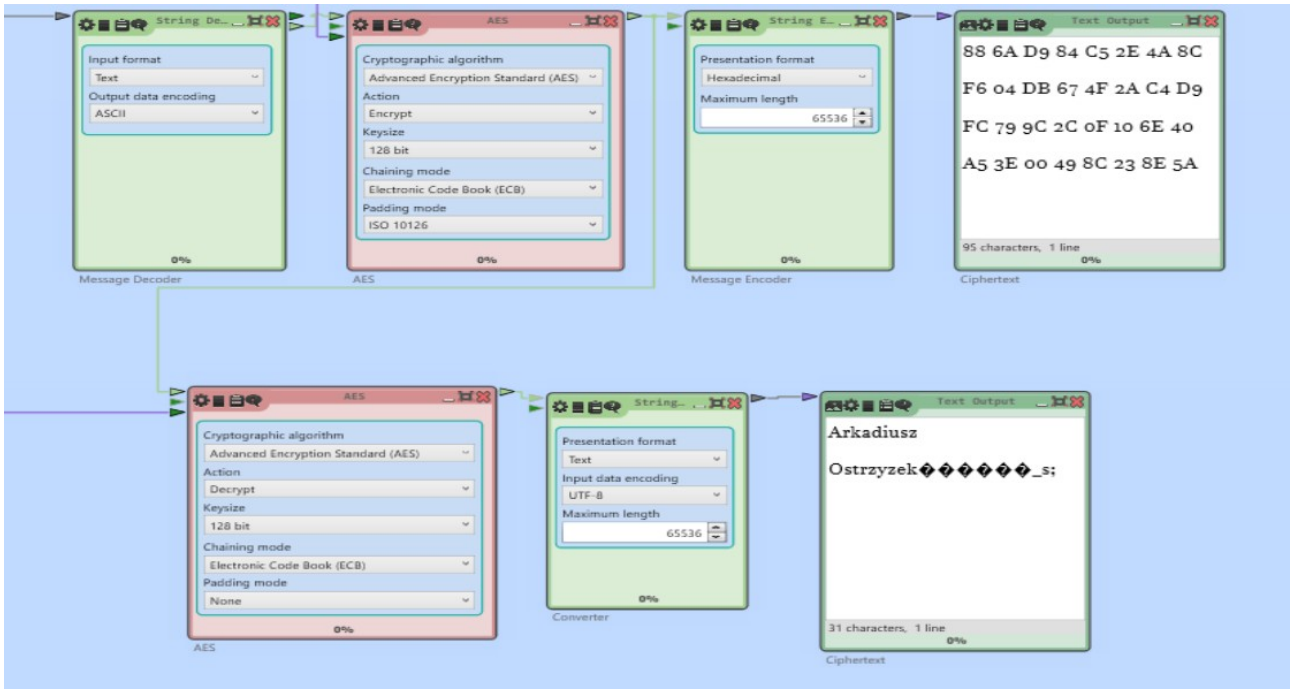
5. zeros – dodawane są same zera.

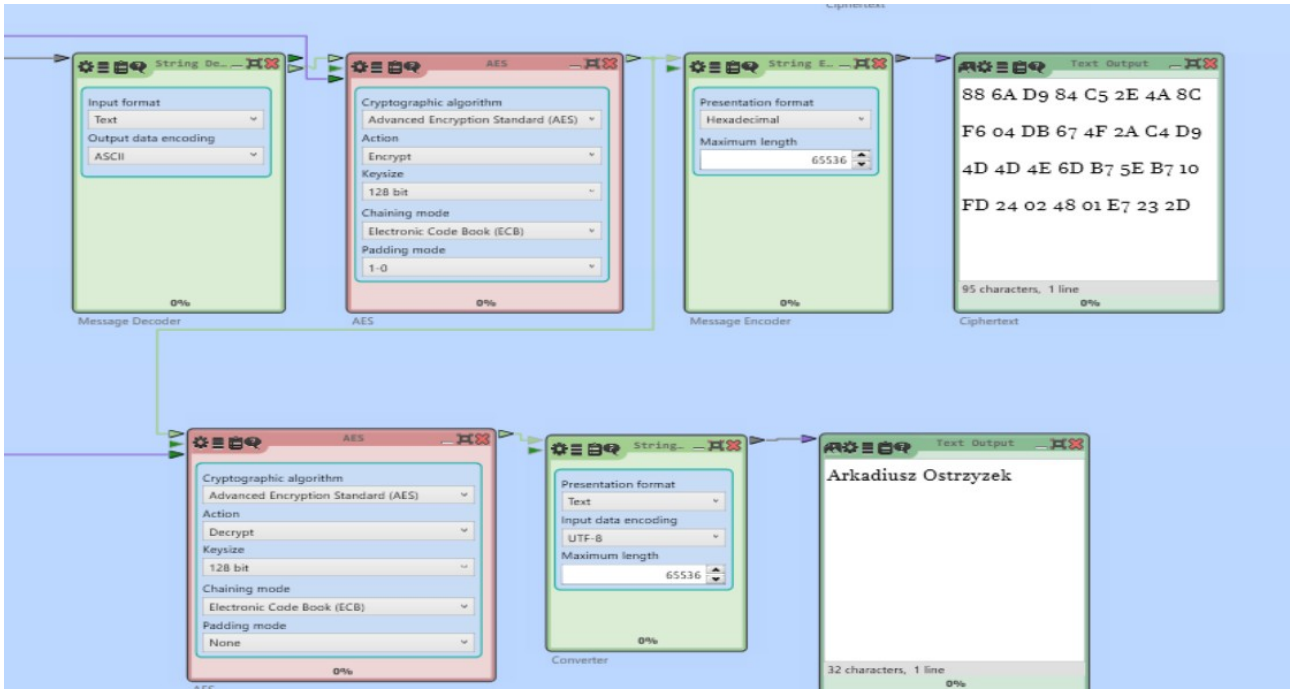
TEKST JAWNY: Arkadiusz Ostrzyżek
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 35 1E 4C 81 DF D8 B5 74 0B 50 35 49 27 50 C5 D2
ODZYSKANY TEKST JAWNY: Arkadiusz Ostrzyżek

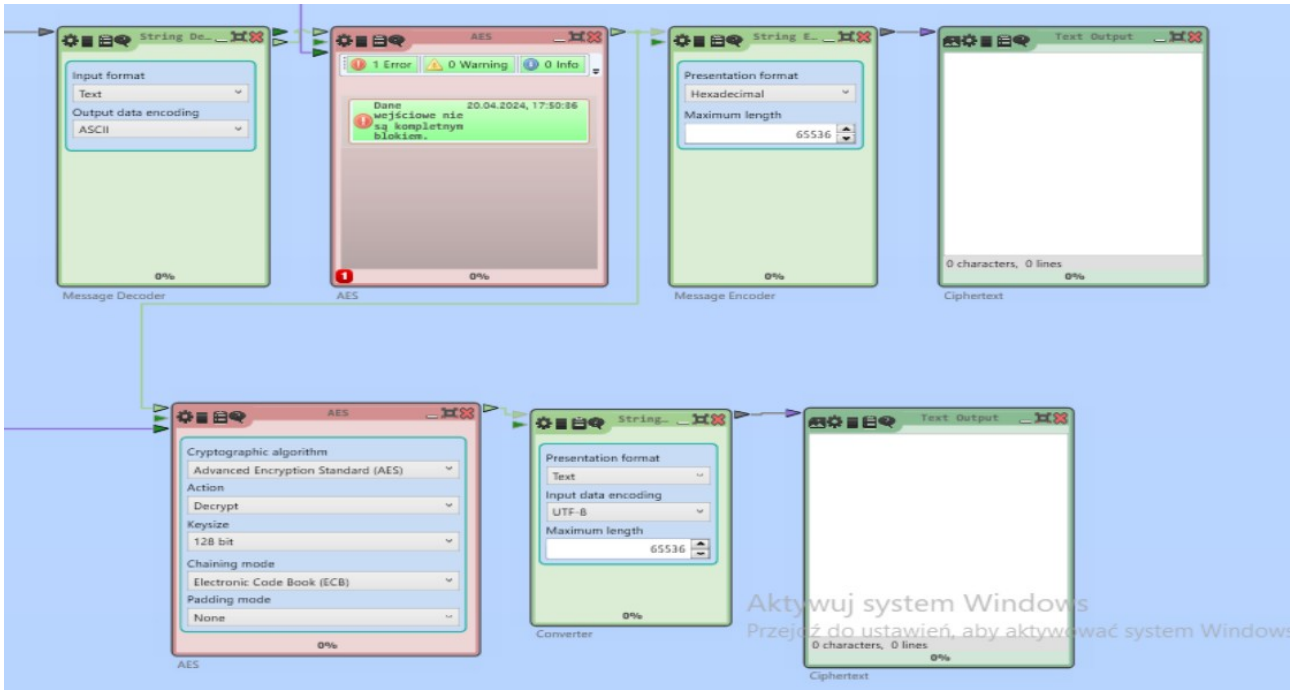

Text Input
Arkadiusz Ostrzyzek
19 characters, 1 line
0%
Plaintext
String De...
Input format
Text
Output data encoding
ASCII
0%
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
Zeros
0%
AES
String E...
Presentation format
Hexadecimal
Maximum length
65536
0%
Message Encoder
Text Output
88 6A D9 84 C5 2E 4A 8C
F6 04 DB 67 4F 2A C4 D9
35 1E 4C 81 DF D8 B5 74
0B 50 35 49 27 50 C5 D2
95 characters, 1 line
0%
Ciphertext
Random Numb...
General
Algorithm
Random.Random
Output type
Byte Array
Output length (bytes)
16
0%
Random Number Generator
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
0%
AES
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
0%
Converter
Text Output
Arkadiusz Ostrzyzek
32 characters, 1 line
0%
Ciphertext


String De...
Input format
Text
Output data encoding
ASCII
0%
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
PKCS#7
0%
AES
String E...
Presentation format
Hexadecimal
Maximum length
65536
0%
Message Encoder
Text Output
88 6A D9 84 C5 2E 4A 8C
F6 04 DB 67 4F 2A C4 D9
C7 1A 56 CF 57 95 7F 5C
7B 0E AB C6 35 00 20 6E
95 characters, 1 line
0%
Ciphertext
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
0%
AES
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
0%
Converter
Text Output
Arkadiusz Ostrzyzek
43 characters, 12 lines
0%
Ciphertext


Input format
Text
Output data encoding
ASCII
Message Decoder
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
ANSI X9.23
AES
Presentation format
Hexadecimal
Maximum length
65536
Message Encoder
88 6A D9 84 C5 2E 4A 8C
F6 04 DB 67 4F 2A C4 D9
1C C7 37 CC 4F D7 D5 DC
8E 06 3C 37 F6 65 17 A7
95 characters, 1 line
Ciphertext
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
AES
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
Converter
Arkadiusz Ostrzyzek
31 characters, 1 line
Ciphertext


Input format
Text
Output data encoding
ASCII
Message Decoder
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
ISO 10126
AES
Presentation format
Hexadecimal
Maximum length
65536
Message Encoder
88 6A D9 84 C5 2E 4A 8C
F6 04 DB 67 4F 2A C4 D9
FC 79 9C 2C 0F 10 6E 40
A5 3E 00 49 8C 23 8E 5A
95 characters, 1 line
Ciphertext
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
AES
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
Converter
Arkadiusz
Ostrzyzek
31 characters, 1 line
Ciphertext


String De...
Input format
Text
Output data encoding
ASCII
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
1-0
AES
String E...
Presentation format
Hexadecimal
Maximum length
65536
Message Encoder
Text Output
88 6A D9 84 C5 2E 4A 8C
F6 04 DB 67 4F 2A C4 D9
4D 4D 4E 6D B7 5E B7 10
FD 24 02 48 01 E7 23 2D
95 characters, 1 line
Ciphertext
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
Converter
Text Output
Arkadiusz Ostrzyzek
32 characters, 1 line


String De...
Input format
Text
Output data encoding
ASCII
Message Decoder
AES
1 Error
0 Warning
0 Info
Dane wejściowe nie są kompletnym blokiem.
20.04.2024, 17:50:86
String E...
Presentation format
Hexadecimal
Maximum length
65536
Message Encoder
Text Output
0 characters, 0 lines
Ciphertext
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Electronic Code Book (ECB)
Padding mode
None
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
Converter
Text Output
0 characters, 0 lines
Ciphertext
Aktywuj system Windows
Przejdź do ustawień, aby aktywować system Windows

3.
a)

Electronic Codebook – wszystkie bloki są szyforwane oddzielnie. Wprowadzenie zmian wpływa tylko na pojedyńczy blok.

TEKST JAWNY: Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 5F 3F AD 70 3C CC 4C 72 74 2E 08 B9 0C EF 6A 3F 2D 30 D0 5C E9 7E FB C0 FF 51 F3 3A 6D C4 D6 D6 44 3B 4B 78 DA 79 FD A4 5C 7B E9 56 9D 56 E6 4F 4E D1 86 32 F2 68 93 11 7E 71 42 10 E5 08 55 B8
ODZYSKANY TEKST JAWNY:
Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909

Cipher Block Chaining – tekst bloku jest xorowany z poprzednim zaszyfrowanym blokiem przed zaszyfrowaniem, a więc pojedyńcza zmiana zmienia wszystkie następne bloki.

TEKST JAWNY: Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 88 6A D9 84 C5 2E 4A 8C F6 04 DB 67 4F 2A C4 D9 82 8F B4 49 92 D5 8F 45 97 A7 A4 E9 FE 22 F5 FD 07 D8 85 FD 7C C8 8D C7 7F F5 57 C3 94 2B F5 C9 38 9D BA 45 78 14 F1 E2 9C 21 95 9D 6B C6 25 79 17 E4 9D 28 5C 0C 51 CB 3E 6D 57 E4 24 87 33 88
ODZYSKANY TEKST JAWNY:
Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909

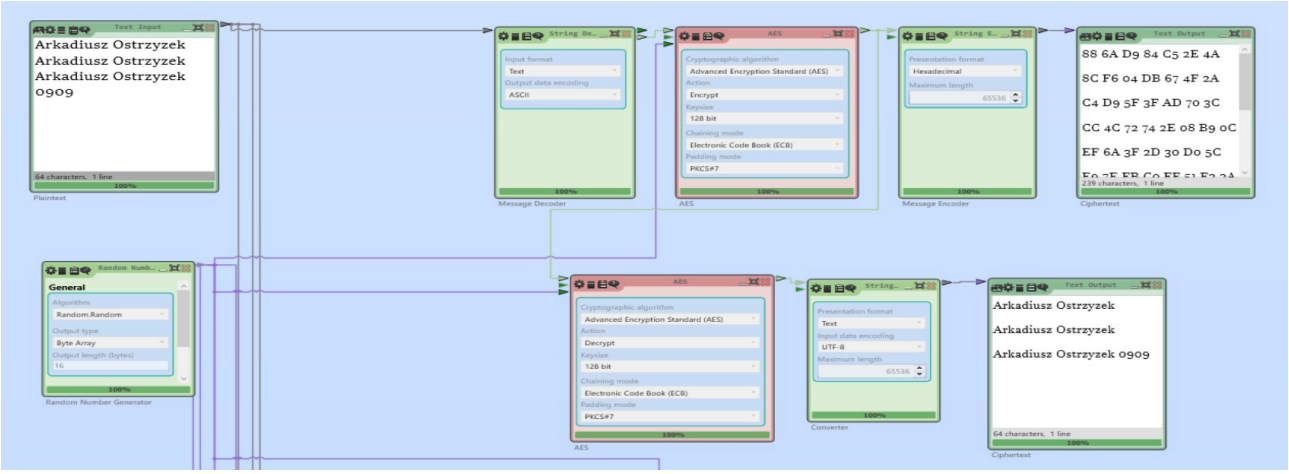
Cipher Feedback – używany jest początkowy wektor, który jest szyfrowany przy użyciu klucza. Następnie jest on xorowany z tekstem przed zaszyfrowaniem. Każdy następny tekst jest xorowany z poprzednim wynikiem szyfrowania. Oznacza to, że wszystkie następne bloki od momentu wprowadzenia zmiany będą inne.

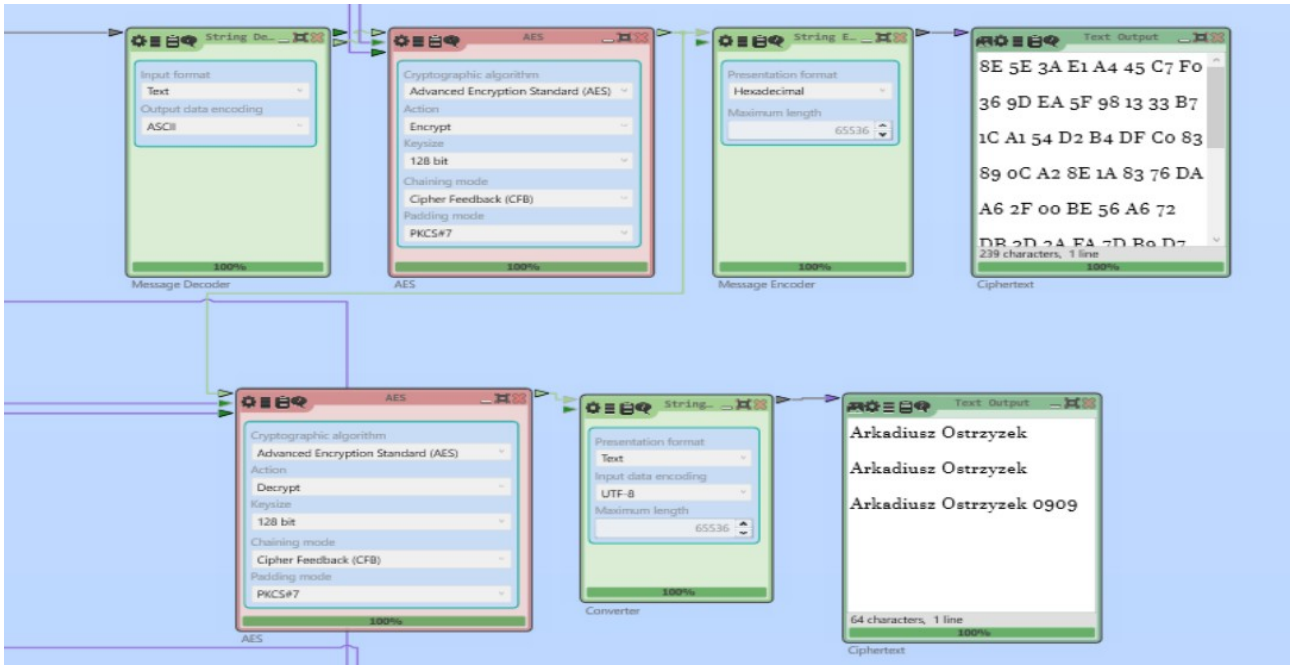
TEKST JAWNY: Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 8E 5E 3A E1 A4 45 C7 F0 36 9D EA 5F 98 13 33 B7 1C A1 54 D2 B4 DF C0 83 89 0C A2 8E 1A 83 76 DA A6 2F 00 BE 56 A6 72 DB 3D 2A FA 7D B9 D7 BF 53 60 BB 86 B2 12 56 2E B3 F5 C5 91 13 D0 6C 66 30 87 C1 FE B4 93 77 26 CB AE 20 CC 2B CA 16 75 51
ODZYSKANY TEKST JAWNY:
Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909

Output Feedback - używany jest początkowy wektor, który jest szyfrowany przy użyciu klucza. Następnie jest on xorowany z tekstem. Zaszyfrowany wektor początkowy jest szyfrowany ponownie, przed xorowaniem z każdą kolejną wiadomością. Oznacza to, że wprowadzenie zmiany w tekście jawnym zmodyfikuje tylko jeden blok.

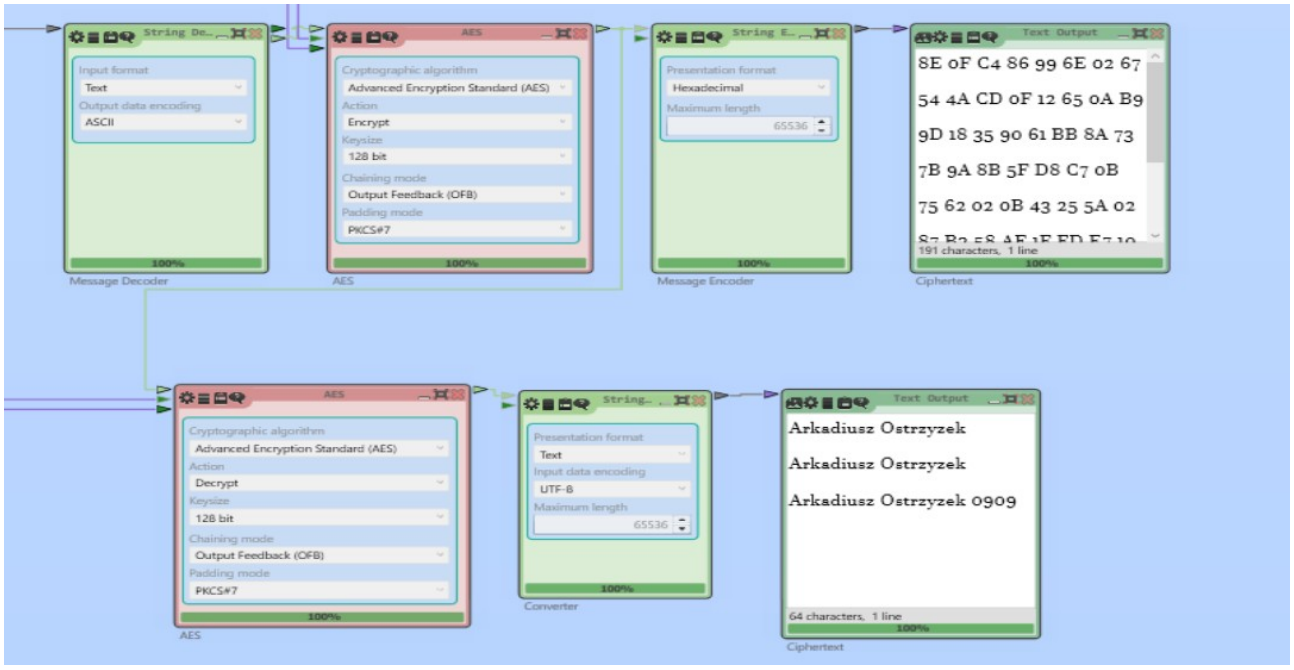
TEKST JAWNY: Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909
KLUCZ: 3E 17 BA 96 AE 04 CD 3B 99 86 9E 56 F0 AD BF 3A
UZYSKANY SZYFROGRAM: 8E 0F C4 86 99 6E 02 67 54 4A CD 0F 12 65 0A B9 9D 18 35 90 61 BB 8A 73 7B 9A 8B 5F D8 C7 0B 75 62 02 0B 43 25 5A 02 87 B3 58 AF 1F FD E7 10 04 E7 9F DC 77 8A 7B 87 12 14 69 E9 22 FB A4 FF E8
ODZYSKANY TEKST JAWNY:
Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek Arkadiusz Ostrzyzek 0909

b)
W obu przypadkach zmniana wektora początkowego wpłynie na zmodyfikowanie wszystkich zaszyfrowanych bloków.

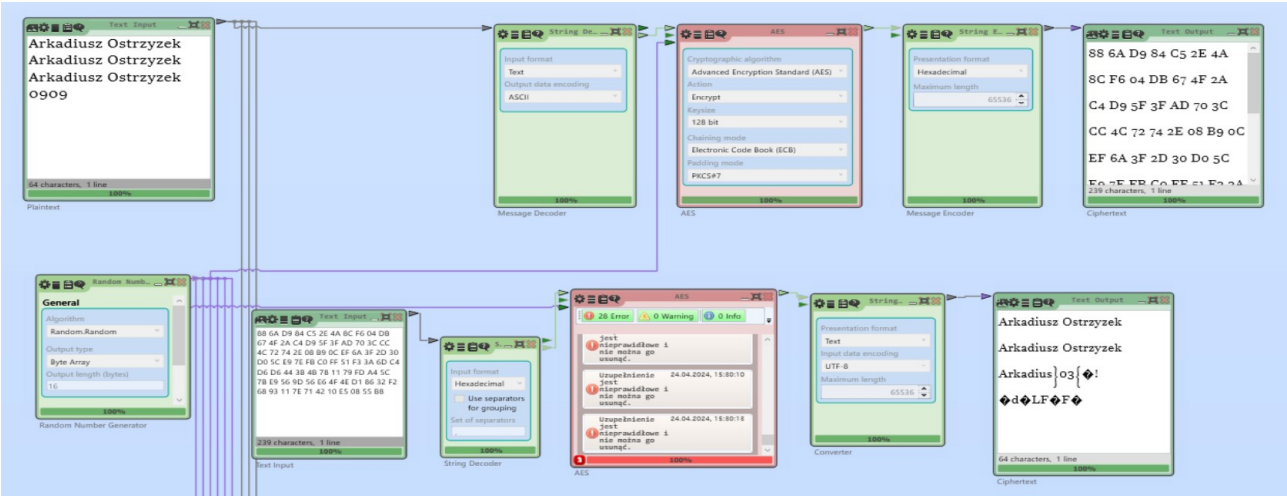


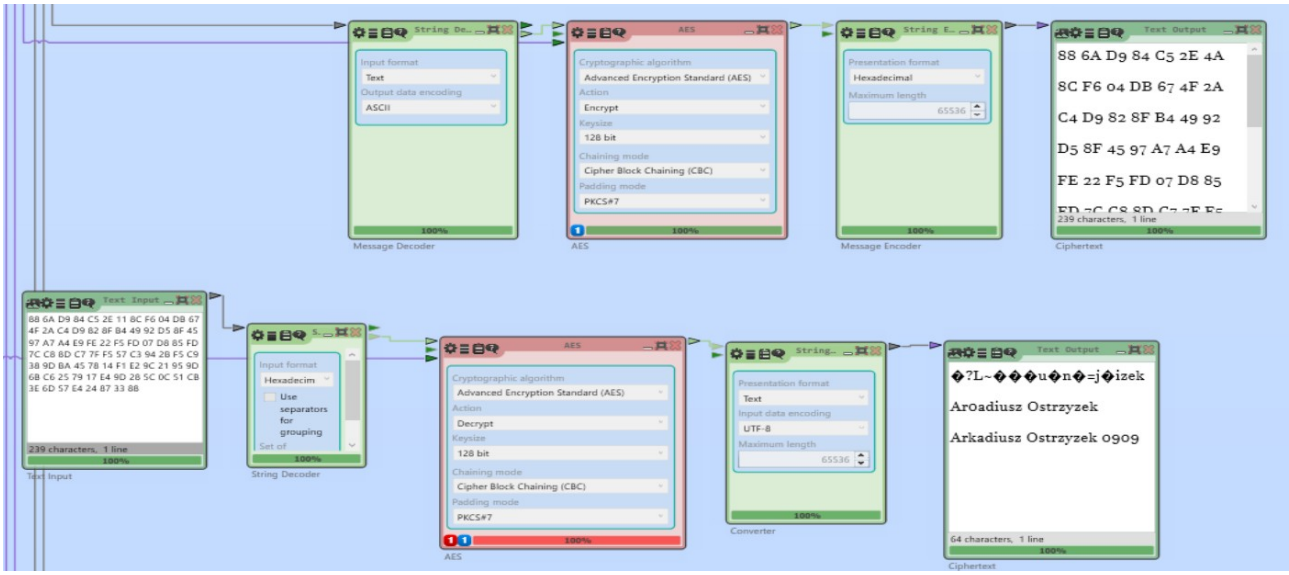

String De...
Input format
Text
Output data encoding
ASCII
100%
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Cipher Block Chaining (CBC)
Padding mode
PKCS#7
100%
AES
String E...
Presentation format
Hexadecimal
Maximum length
65536
100%
Message Encoder
Text Output
88 6A D9 84 C5 2E 4A
8C F6 04 DB 67 4F 2A
C4 D9 82 8F B4 49 92
D5 8F 45 97 A7 A4 E9
FE 22 F5 FD 07 D8 85
239 characters, 1 line
100%
Ciphertext
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Cipher Block Chaining (CBC)
Padding mode
PKCS#7
100%
AES
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
100%
Converter
Text Output
Arkadiusz Ostrzyzek
Arkadiusz Ostrzyzek
Arkadiusz Ostrzyzek 0909
64 characters, 1 line
100%
Ciphertext


String De...
Input format
Text
Output data encoding
ASCII
100%
Message Decoder
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Encrypt
Keysize
128 bit
Chaining mode
Output Feedback (OFB)
Padding mode
PKCS#7
100%
AES
String E...
Presentation format
Hexadecimal
Maximum length
65536
100%
Message Encoder
Text Output
8E 0F C4 86 99 6E 02 67
54 4A CD 0F 12 65 0A B9
9D 18 35 90 61 BB 8A 73
7B 9A 8B 5F D8 C7 0B
75 62 02 0B 43 25 5A 02
191 characters, 1 line
100%
Ciphertext
AES
Cryptographic algorithm
Advanced Encryption Standard (AES)
Action
Decrypt
Keysize
128 bit
Chaining mode
Output Feedback (OFB)
Padding mode
PKCS#7
100%
AES
String...
Presentation format
Text
Input data encoding
UTF-8
Maximum length
65536
100%
Converter
Text Output
Arkadiusz Ostrzyzek
Arkadiusz Ostrzyzek
Arkadiusz Ostrzyzek 0909
64 characters, 1 line
100%
Ciphertext

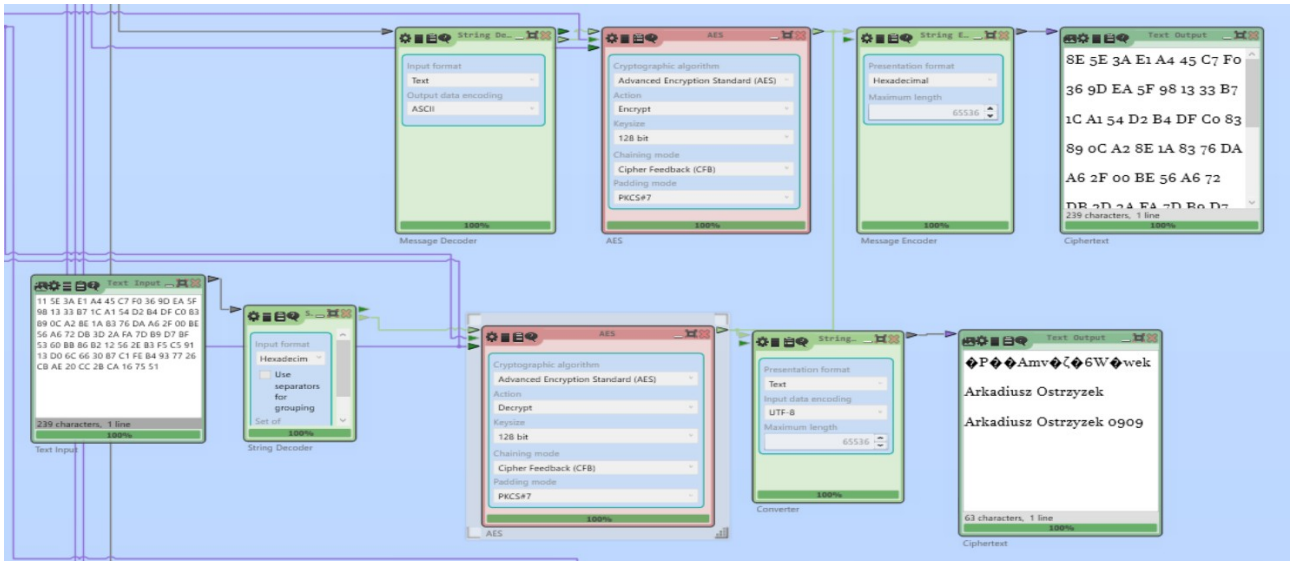
4.
Electronic Codebook – wszystkie bloki są szyforwane oddzielnie. Wprowadzenie zmian wpływa tylko na pojedyńczy blok.



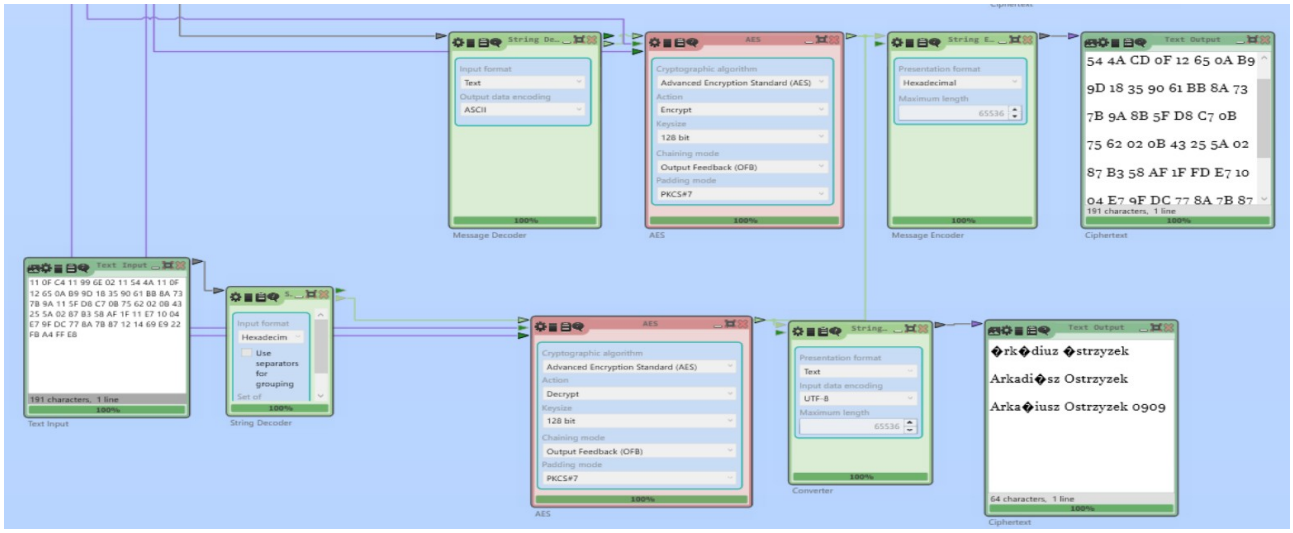

Cipher Block Chaining – Zmiana w zaszyfrowanym tekście wpływa tylko na odczyt pojedyńczego bloku.



Cipher Feedback – Zmiana w zaszyfrowanym tekście wpływa tylko na odczyt pojedyńczego bloku.




Output Feedback – zmiany wpływają tylko na pojedyńcze znaki.

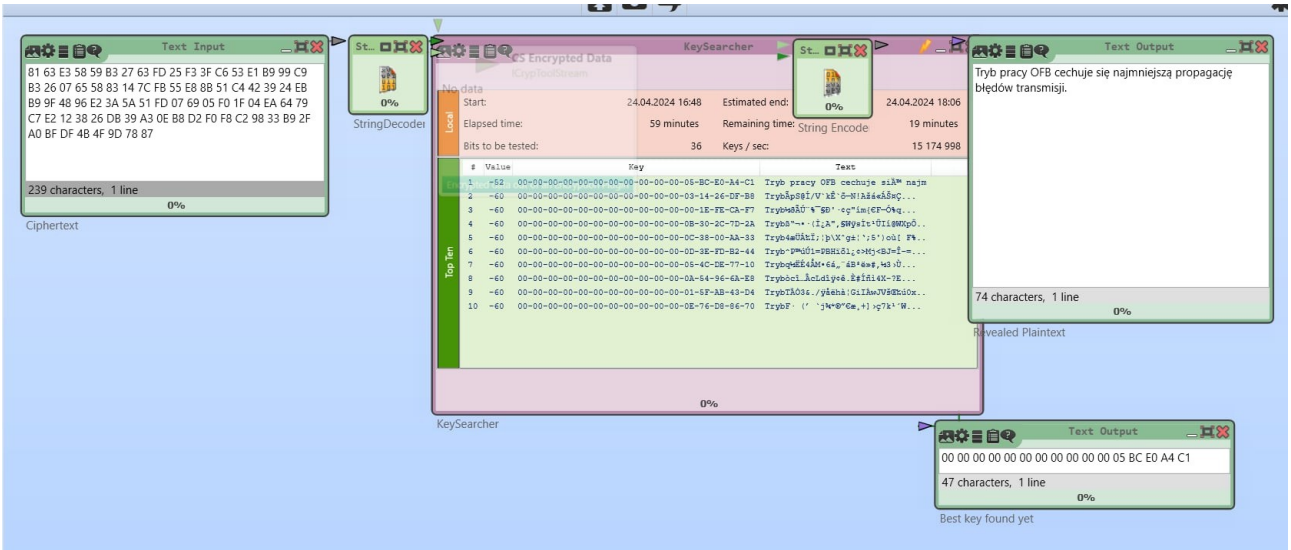


5.

KLUCZ: 00-00-00-00-00-00-00-00-00-00-00-00-00-00-9C-4C-DA
ODZYSKANY TEKST JAWNY: Szyfr blokowy wykorzystuje iterowane proste rundy.


KLUCZ: 00-00-00-00-00-00-00-00-00-00-00-00-00-65-59-BD-BA
ODZYSKANY TEKST JAWNY: AES wykorzytuje w rundzie: podstawianie, transpozycję i liniową dyfuzję.


KLUCZ: 00-00-00-00-00-00-00-00-00-00-00-00-05-BC-E0-A4-C1
ODZYSKANY TEKST JAWNY: Tryb pracy OFB cechuje się najmniejszą propagację błędów transmisji.



6.

DES
Blowfish
rc2
rc4