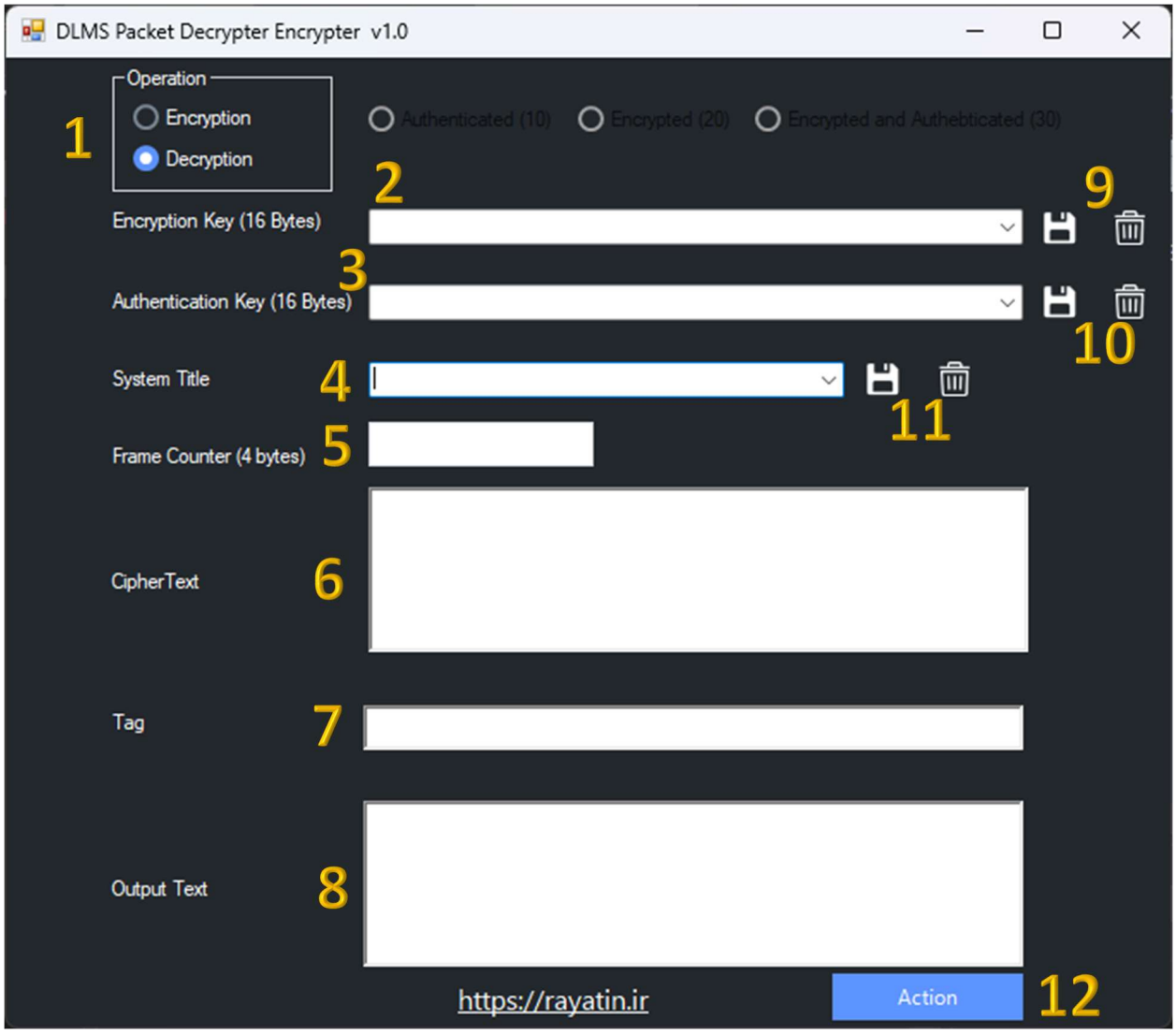
DLMS Packet Decrypter/Encrypter User Guide

This document describes how to use DLMS Packet Decrypter/Encrypter tool.

This tool written with C# language. In below picture you can see the window of this software. All part of that will be described.



1- Operation Section: you can choose what you want to do, Encryption or Decryption
2- Encryption Key combo box: it can be used from default value or can write user value. the value of this combo box must be 16 bytes
3- Authentication Key combo box: it can be used from default value or can write user value. the value of this combo box must be 16 bytes
4- System Title combo box: : it can be used from default value or can write user value
5- Frame Counter text box: this value is 4 bytes

6- Input text: if user choose Decryption from Operation Section this value must be Ciphered text that we want Decrypt that
7- Tag: this test box is used in Decryption and is 12 bytes and produced in Encryption mode.
8- Output Text: if user choose Decryption the output is final Plain text and if user choose Encryption this value produce cipher text.
9- EK save and delete buttons that used for save new default keys for Encryption or delete those
10- AK save and delete buttons that used for save new default keys for Authentication or delete those
11- System Title save and delete buttons that used for save new default keys for System Titles or delete those
12- Action Button: use for run the process

Example:

In the below there is a ciphered packet and we show how to decrypt that.

7E A0 4B 00 02 FE FF 03 32 0E 7E E6 E6 00 DB 08 43 54 54 30 30 30 30 30 31 30 80 3F 37 FF F1 B7 1E A7 4A 00 E8 A0 36 4E 46 FC 2B 0B E5 60 88 0B 6F 23 40 66 4E 87 2F 8A FE DB 57 9C 2F C2 AE 4E B5 E2 75 88 1F A7 CB C2 EC 1A A0 5A AC 6F 70 7E

EK: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

AK: D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF

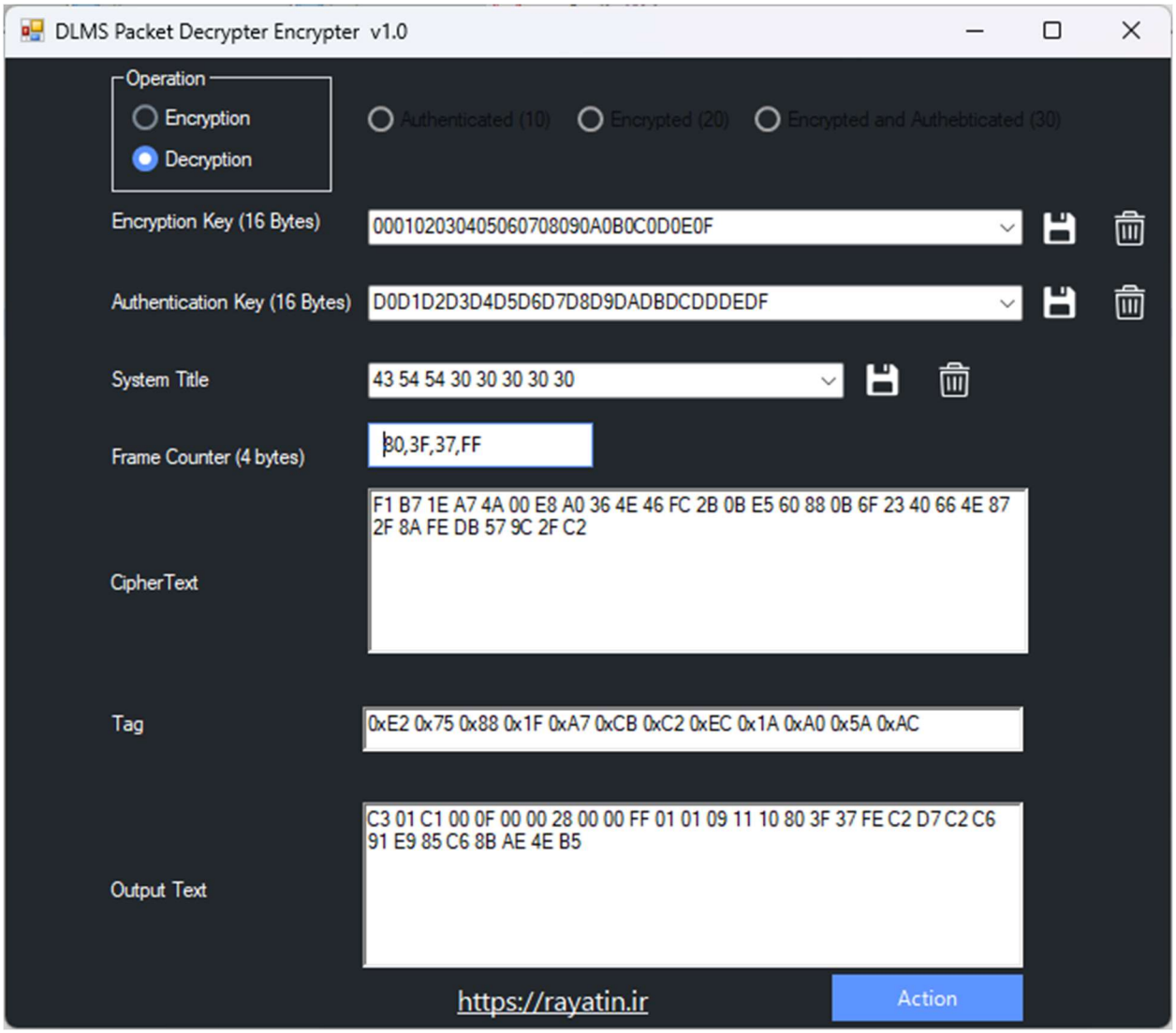
System Title: 43 54 54 30 30 30 30 30

Red segment is frame counter : 80 3F 37 FF

Purple segment is ciphered text: F1 B7 1E A7 4A 00 E8 A0 36 4E 46 FC 2B 0B E5 60 88 0B 6F 23 40 66 4E 87 2F 8A FE DB 57 9C 2F C2 AE 4E

Green segment is the Tag: B5 E2 75 88 1F A7 CB C2 EC 1A A0 5A AC

Replace these in the software and click on the Action button:



All inputs can be with or without space. Also can be with “,” and “0x” character. It is not important. Software detect remove these automatically.

Result Plain Text: C3 01 C1 00 0F 00 00 28 00 00 FF 01 01 09 11 10 80 3F 37 FE C2 D7 C2 C6 91 E9 85 C6 8B AE 4E B5