Lab Manual for TYBSc CS 2020-2021 USCS607:Ethical Hacking

Roll No :18043 Date:30/01/2021

**Practical 2**

**Aim: Use CrypTool to encrypt and decrypt passwords using RC4 algorithm**

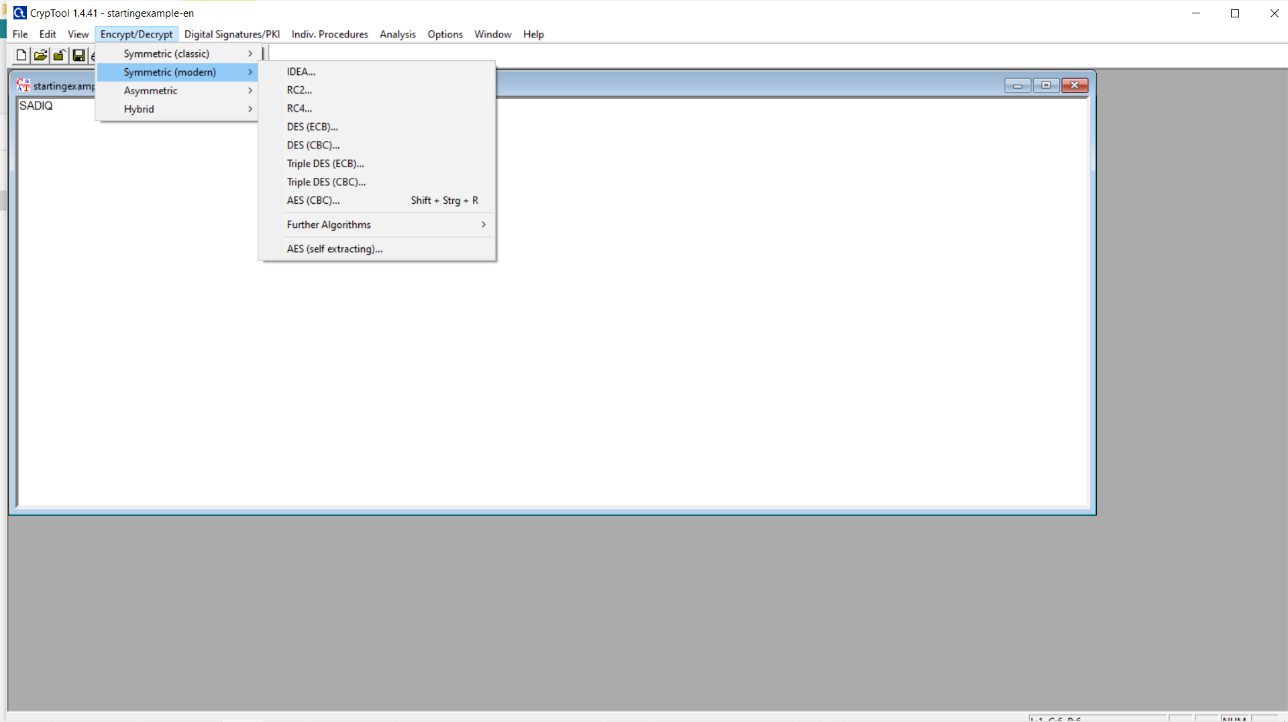
**RC4 Encryption Algorithm:**

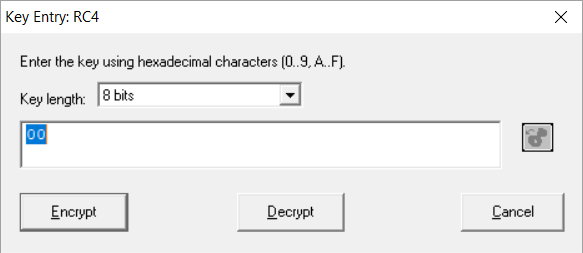
**RC4**is a stream cipher and variable length key algorithm. This algorithm encrypts one byte at a time (or larger units on a time).  
A key input is pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of input key, The output of the generator is called key-stream, is combined one byte at a time with the plaintext stream cipher using X-OR operation.

RC4 means Rivest Cipher 4 invented by Ron Rivest in 1987 for RSA Security. It is a Stream Ciphers. Stream Ciphers operate on a stream of data byte by byte. RC4 stream cipher is one of the most widely used stream ciphers because of its simplicity and speed of operation. It is a variable key-size stream cipher with byte-oriented operations.

It uses either 64 bit or 128-bit key sizes. It is generally used in applications such as Secure Socket Layer (SSL), Transport Layer Security (TSL), and also used in IEEE 802.11 wireless LAN std.

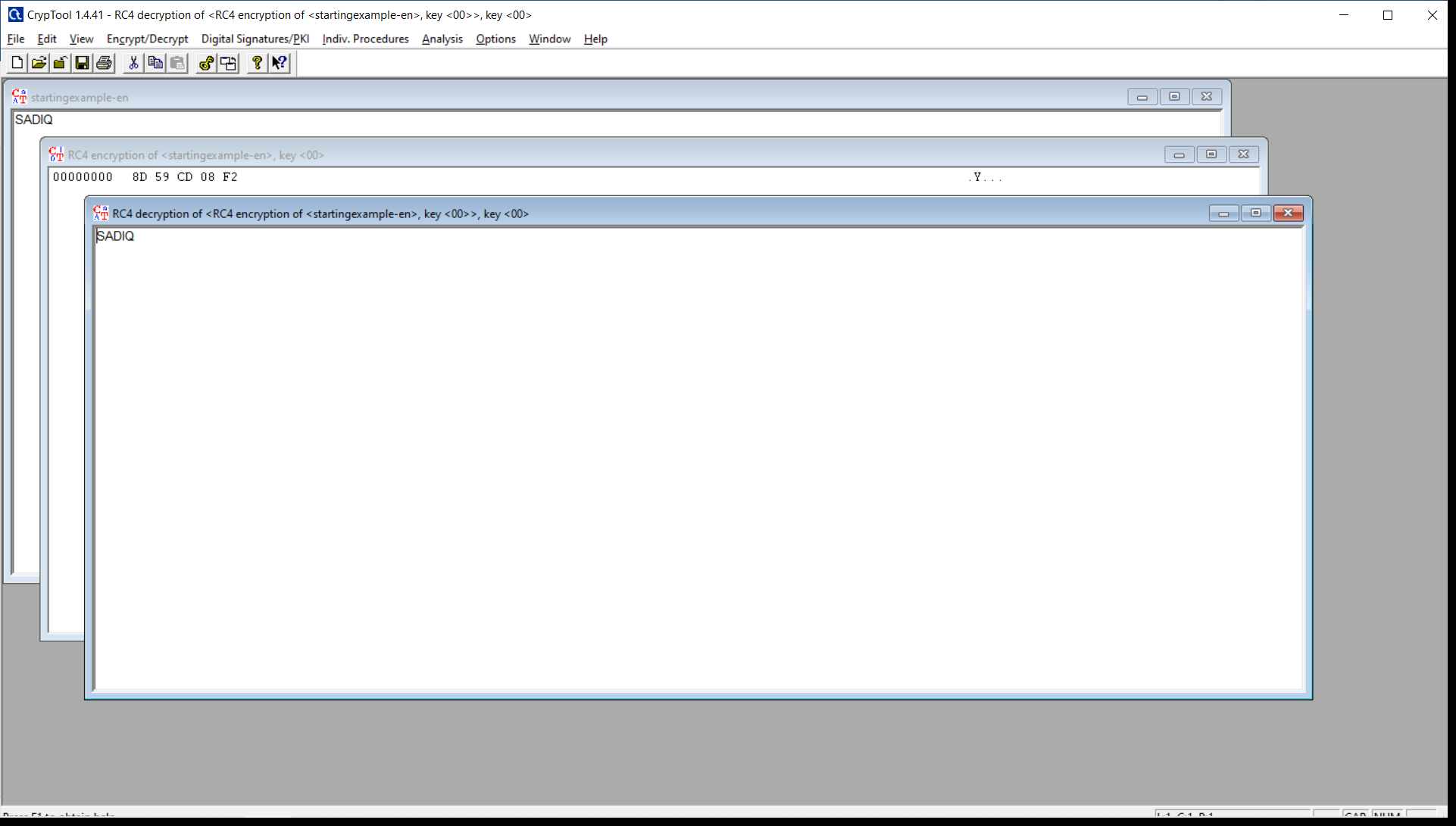
**Step1: Enter the word and select RC4 algorithm.**



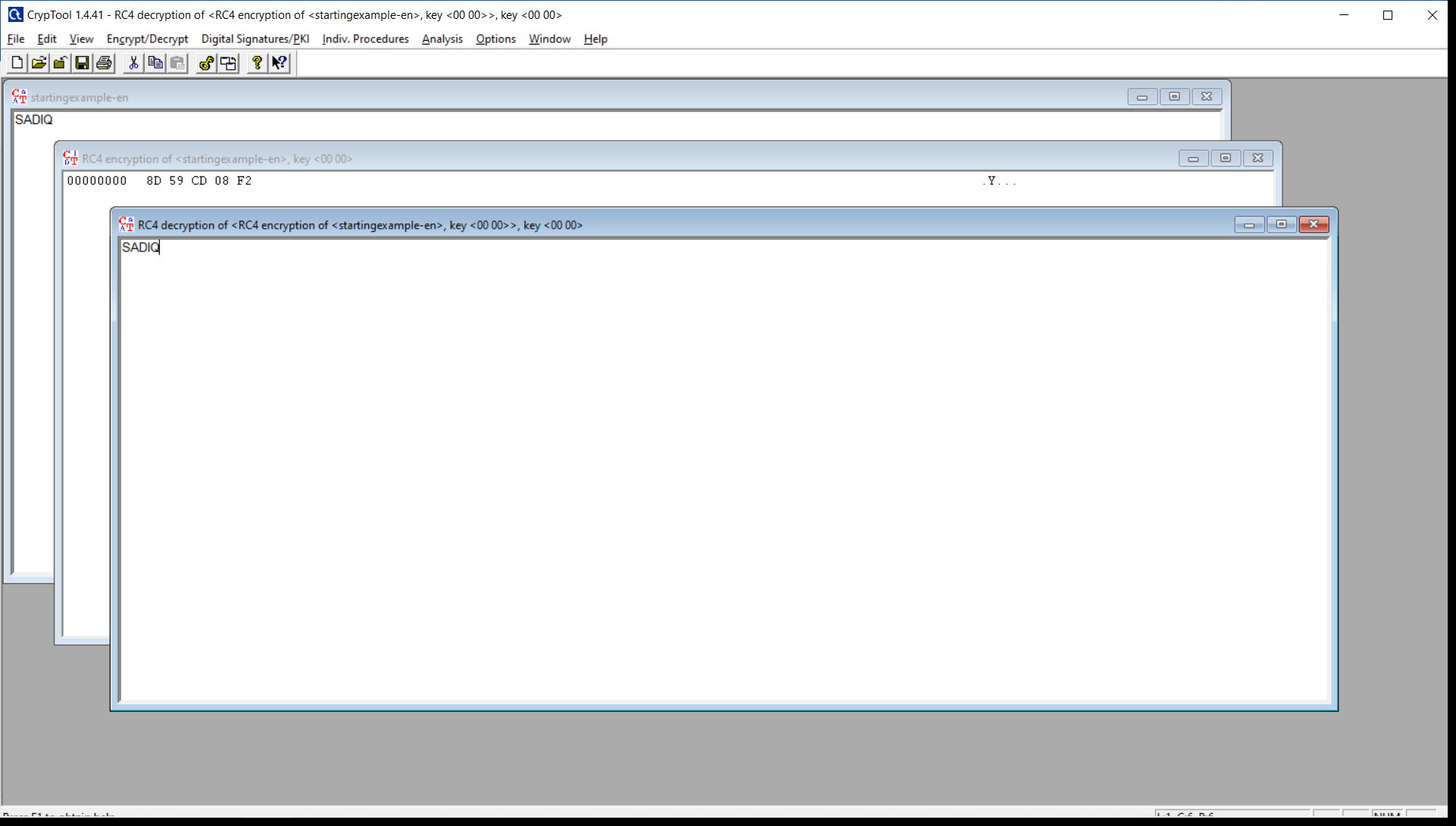


**Here I have put SADIQ as the word then its encryption and its decryption**

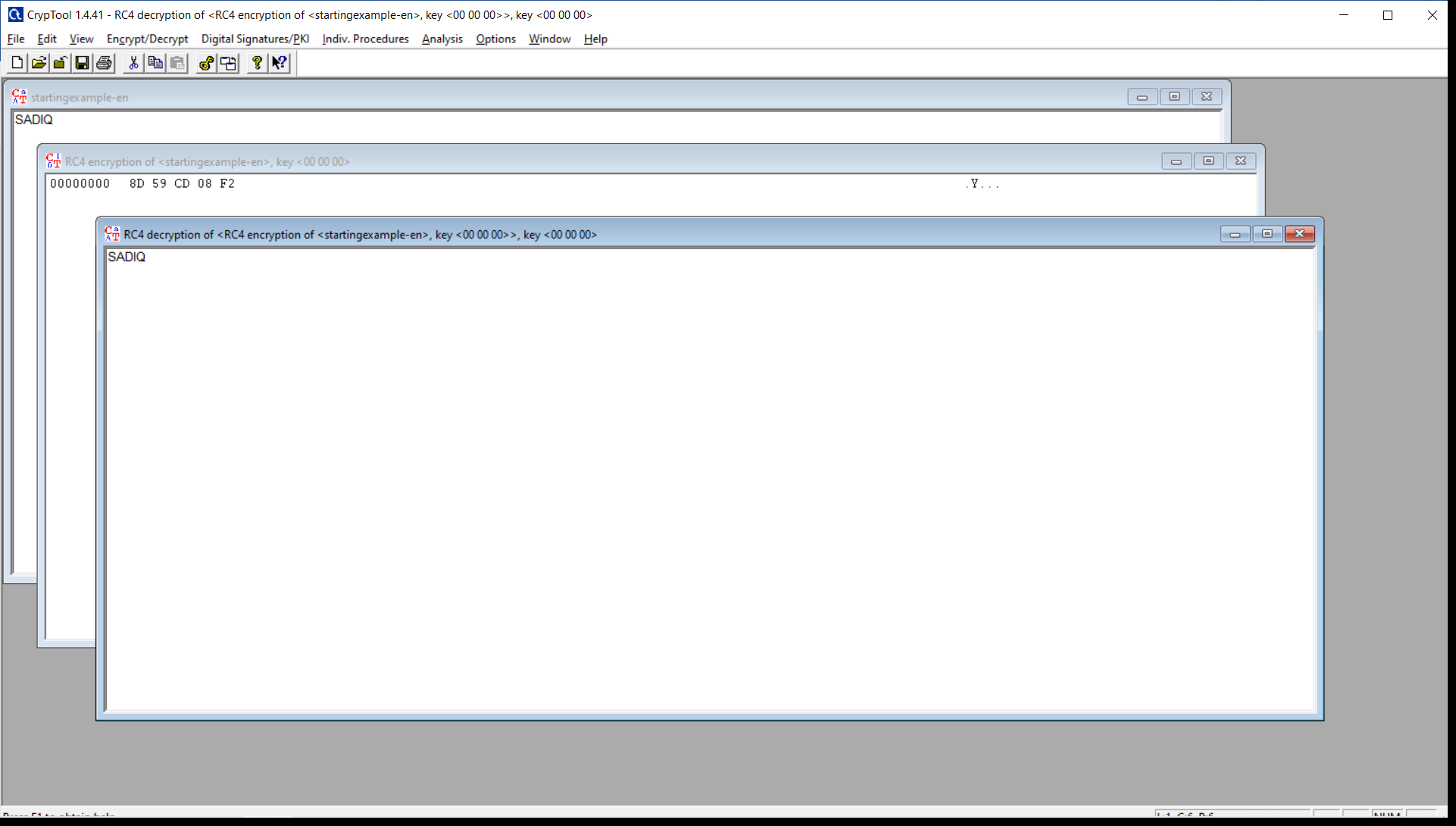
**For 8 Bits:**



**For 16 Bits:**



**For 24 Bits:**



**For 32 Bits:**

