



CrypTool

dr Jasmina Novaković



10. CRYPTOOOL

- U ovom delu gradiva objasnićemo instalaciju i korišćenje alata CrypTool.
- U ovom delu daje se prikaz instalacije CrypTool-a.
- Razmatra se korišćenje programa CrypTool za: algoritme klasične kriptografije; simetrične blokovske algoritme i kriptografiju sa javnim ključem.
- Razmatra se korišćenje programa za generisanje digitalnog potpisa i heš funkcije.



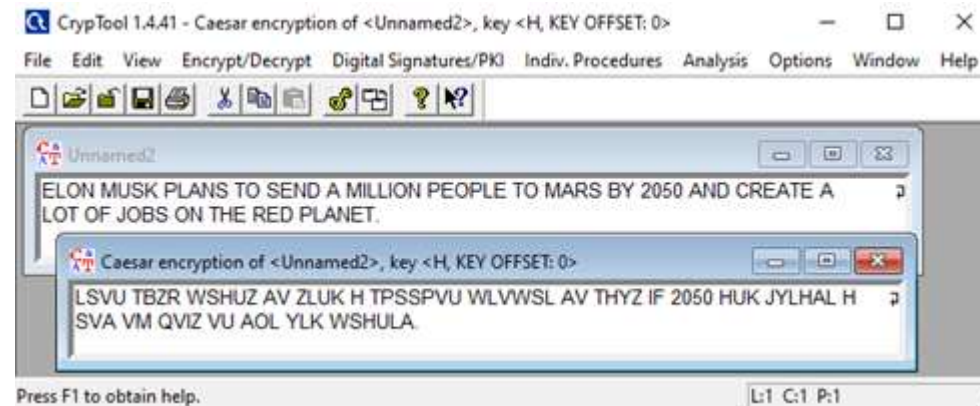
Nakon proučavanja ovog dela, trebalo bi da možete da:

- instalirate CrypTool;
- koristite alate za različite algoritme klasične kriptografije;
- koristite alate za simetrične blokove algoritme;
- koristite alate za kriptografiju sa javnim ključem;
- koristite alate za generisanje digitalnog potpisa i heš funkcija.

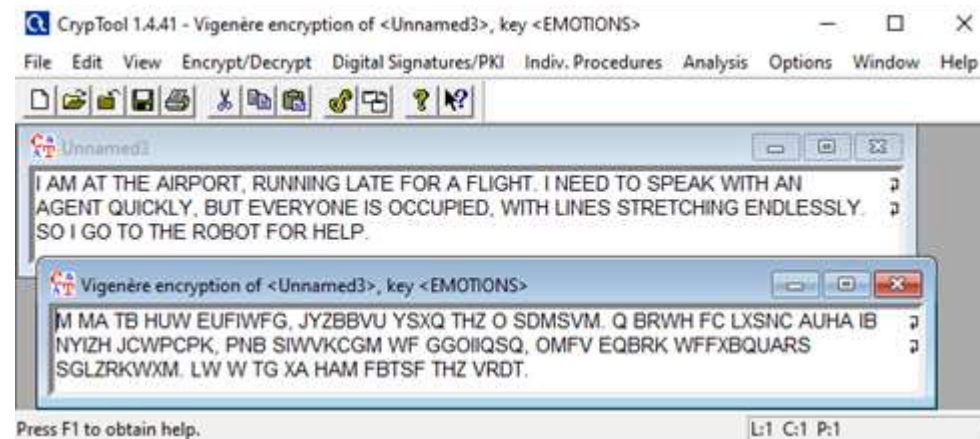
Početni ekran za instalaciju CrypTool-a



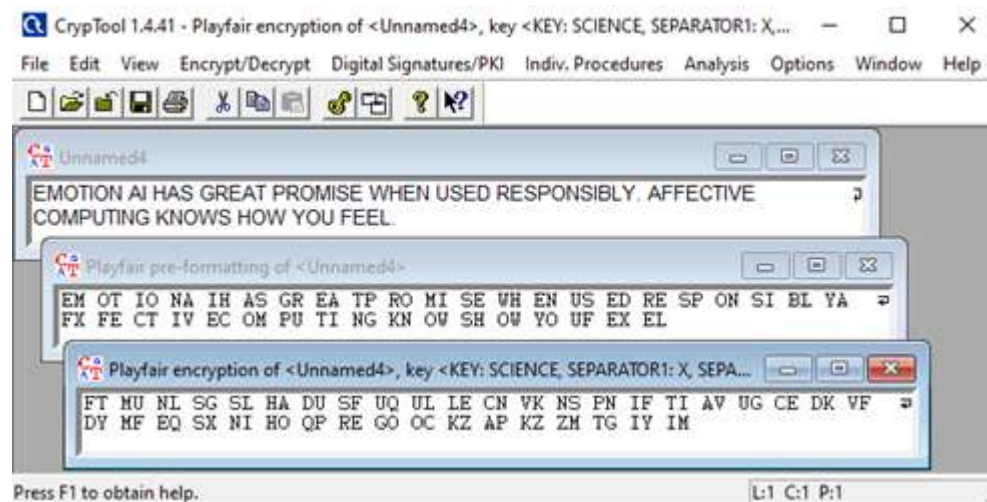
Rezultat šifrovanja koristeći Cezarov algoritam



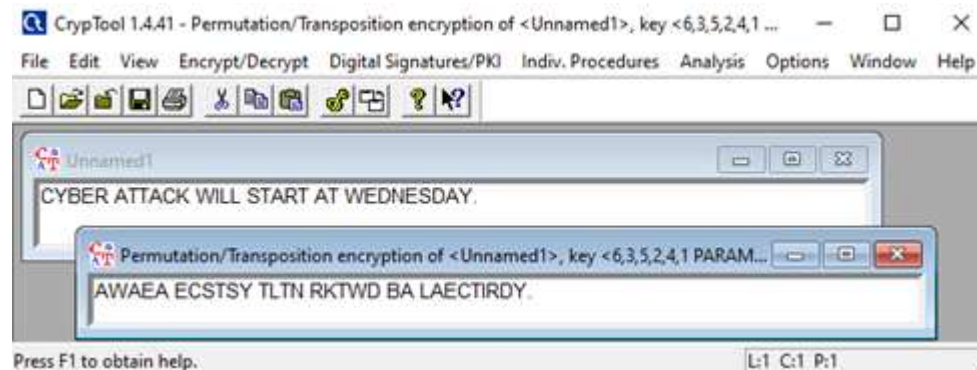
Šifrat kod Vižnerove šifre



Playfair-ova šifra



Prikaz šifrovanog teksta - algoritam transpozicije po kolonama



One-Time Pad šifra

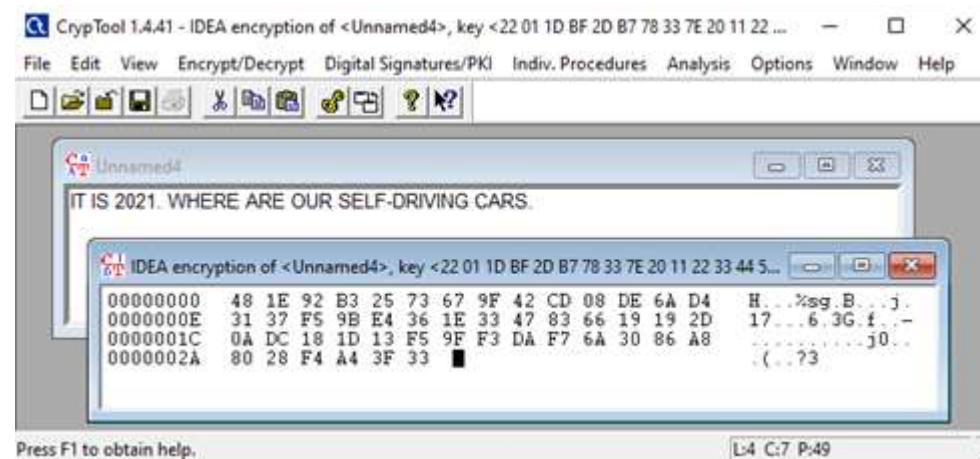


The screenshot shows the CrypTool 1.4.41 interface. The main window displays the message: "WITHIN A DECADE SELF-DRIVING CARS WILL BE AS COMMON AS ELEVATORS." An overlay window titled "Vernam encryption of <Unnamed5> and <SifraOTP.txt>" shows the encryption process. The message is converted into a grid of hexadecimal values, which are then XORed with a key to produce ciphertext. The ciphertext is displayed in a grid format, with the original message text visible on the right side of the grid.

```
00000000 16 1C 00 07 07 01 6D 0E 75 17 65 00 00 16 .....n.u.e...
0000000E 16 00 12 17 09 66 63 0B 72 05 19 07 09 02 .....fc.r...
0000001C 72 63 03 17 1B 6F 1B 0D 09 02 00 16 0A 00 rc...o...
0000002A 09 1C 6C 0F 16 1A 02 00 0A 00 12 10 69 65 ..l.....ie
00000038 0A 0C 76 07 1D 03 1F 00 00 ..v.....
```

Press F1 to obtain help. L:1 C:1 P:1

Šifrovani tekst uz pomoć IDEA



```
CrypTool 1.4.41 - IDEA encryption of <Unnamed4>, key <22 01 1D BF 2D B7 78 33 7E 20 11 22 ...
```

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

IT IS 2021. WHERE ARE OUR SELF-DRIVING CARS.

```
IDEA encryption of <Unnamed4>, key <22 01 1D BF 2D B7 78 33 7E 20 11 22 33 44 5...
```

00000000	48 1E 92 B3 25 73 67 9F 42 CD 08 DE 6A D4	H...%g.B...j.
0000000E	31 37 F5 9B E4 36 1E 33 47 83 66 19 19 2D	17...6.3G.f...-
0000001C	0A DC 18 1D 13 F5 9F F3 DA F7 6A 30 86 A8j0..
0000002A	80 28 F4 A4 3F 33	{...?3

Press F1 to obtain help. L4 C:7 P:49