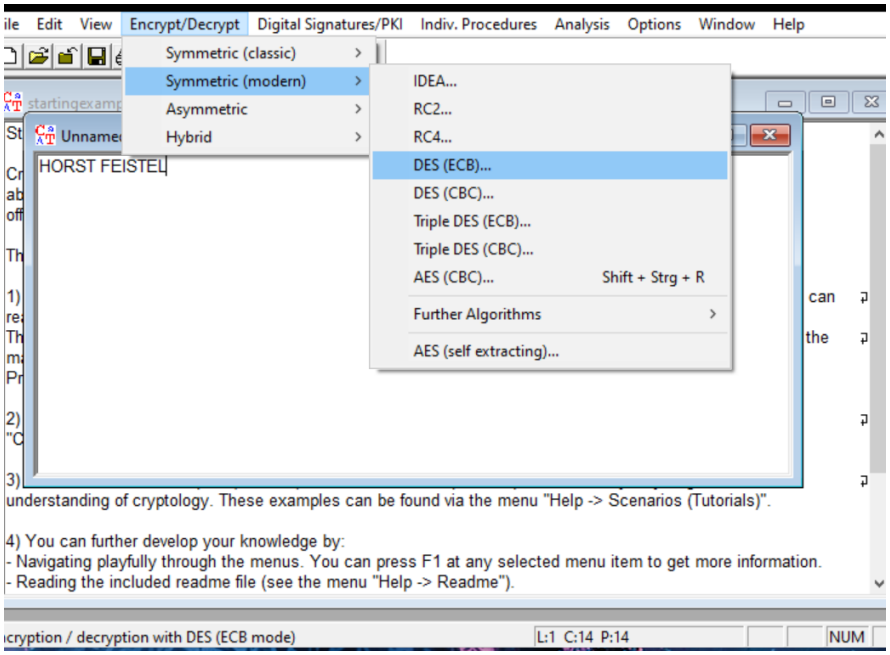
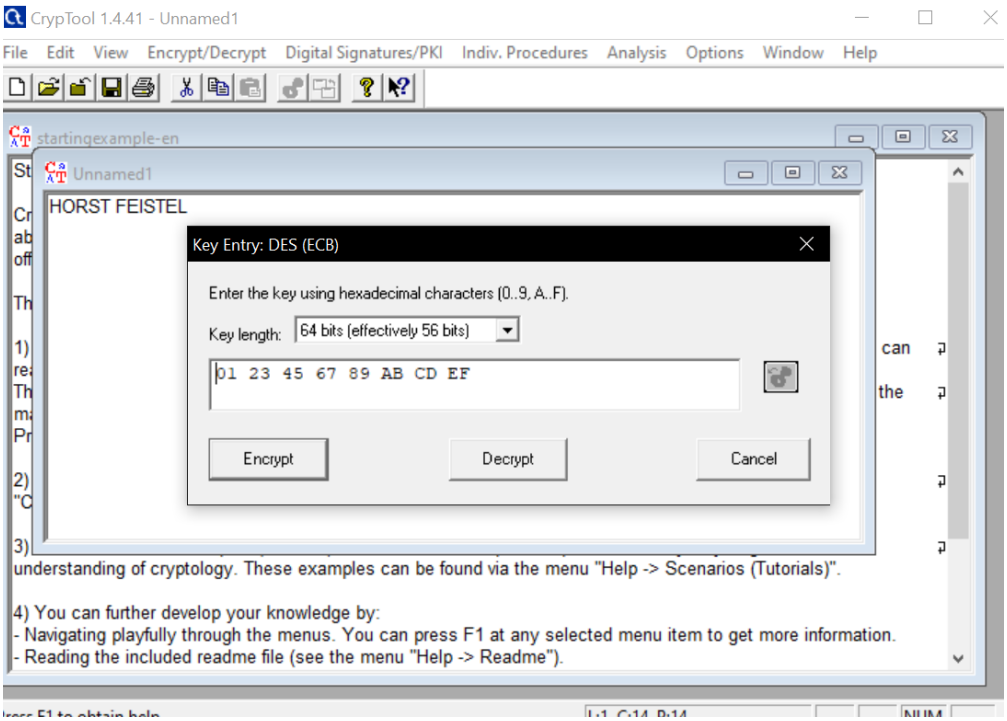
Laborator 3 – Rezolvare

CrypTool

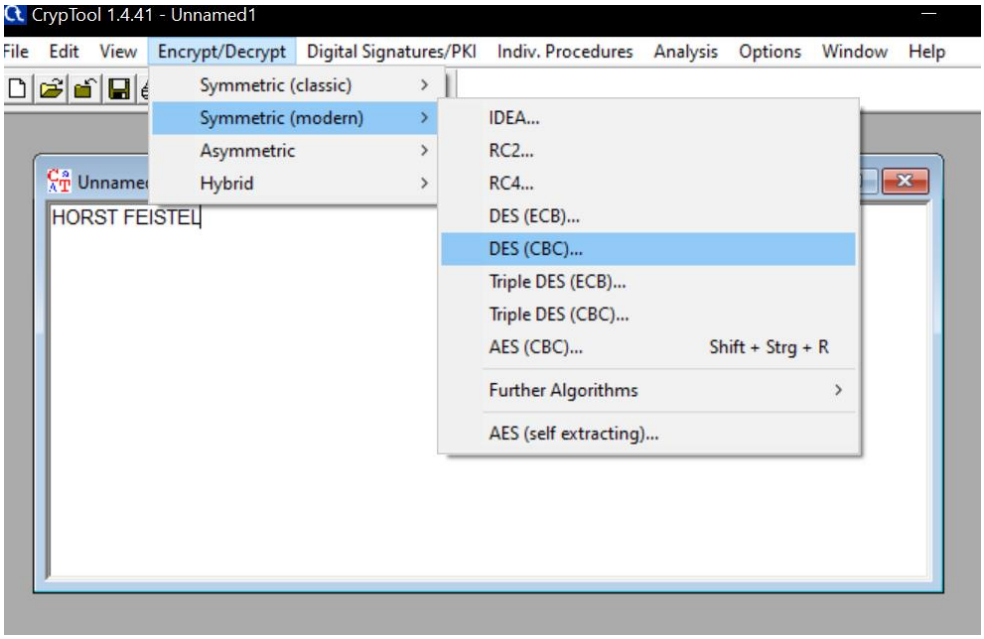
II. Criptare:

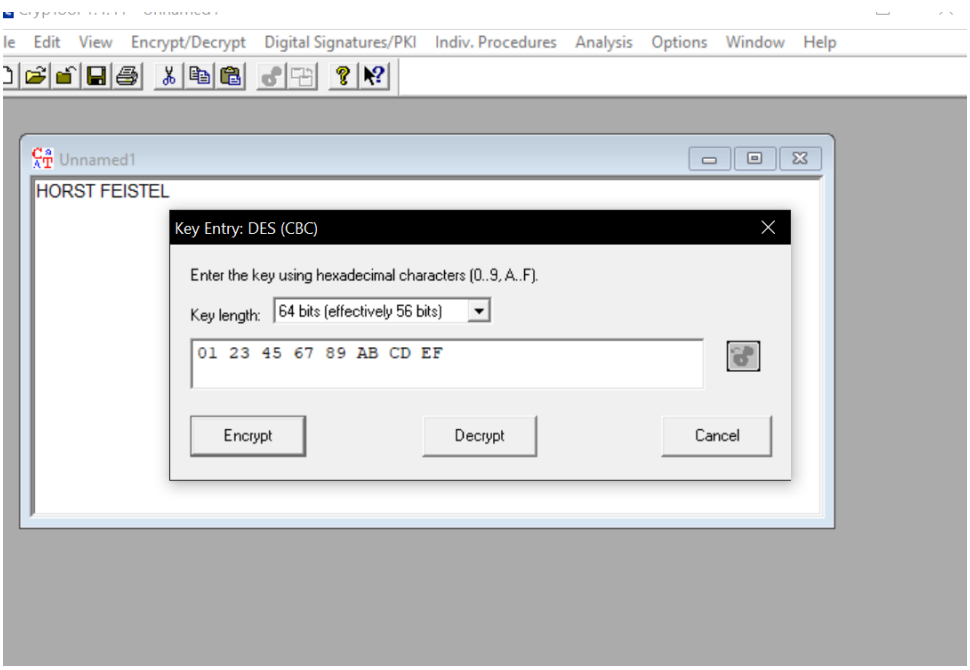
i) HORST FEISTEL → DA 04 97 C2 59 D4 15 71 24 C1 F2 83 A2 4F 3D 83 (**ECB**)





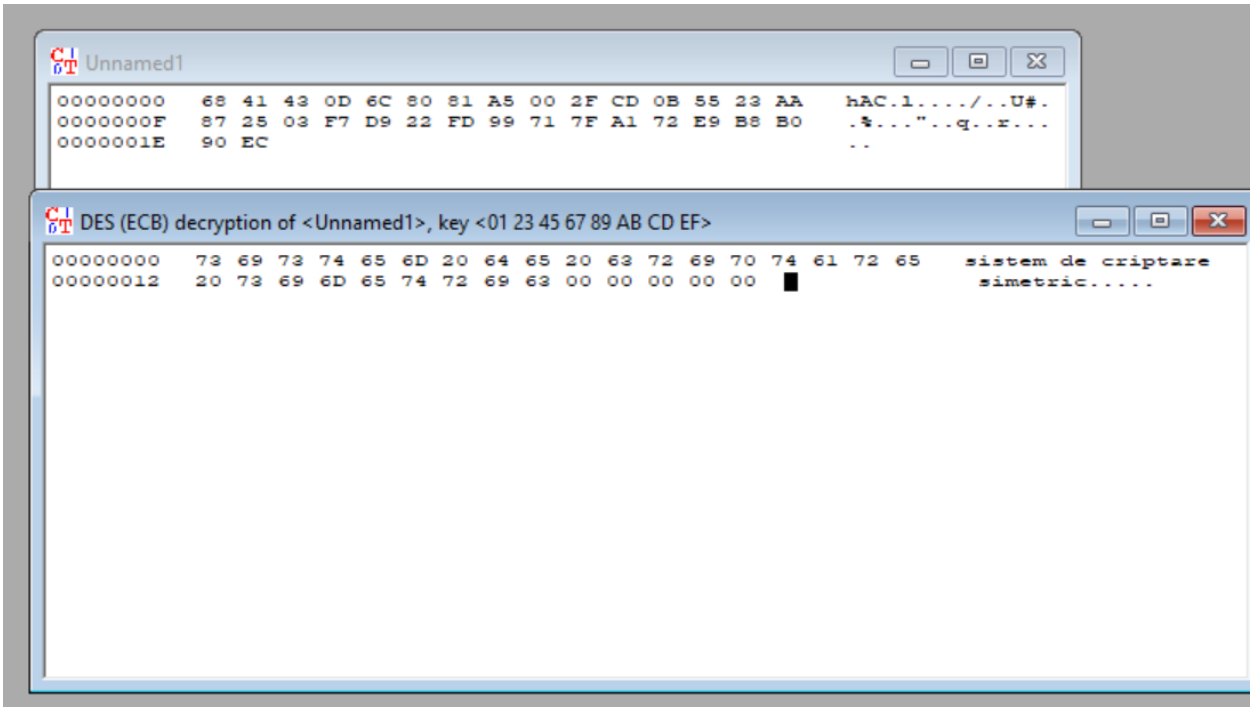
ii) HORST FEISTEL → DA 04 97 C2 59 D4 15 71 65 47 E0 51 51 E2 95 E0 (**CBC**)





III. DECRIPTARE:

68 41 43 0D 6C 80 81 A5 00 2F CD 0B 55 23 AA 87 25 03 F7 D9 22 FD 99 71 7F A1 72 E9 B8 B0 90 EC → sistem de criptare simetric (**ECB**)



IV. PROPRIETATEA DE DIFUZIE:

(Se folosesc efectiv 56 biți: în funcție de cum modifici bitul, e posibil să obții același mesaj criptat.)

Mesaj: HORST FEISTEL

Cheie de Criptare: 01 23 45 67 89 AB CD EF

Mesaj Criptat: DA 04 97 C2 59 D4 15 71 24 C1 F2 83 A2 4F 3D 83 (**ECB**)

Cheie de Criptare Nouă: 00 23 45 67 89 AB CD EF

Mesaj Criptat Nou: 16 FA C5 EF AE F9 72 C7 F1 FC AE 60 6B 81 D9 AF (**ECB**)

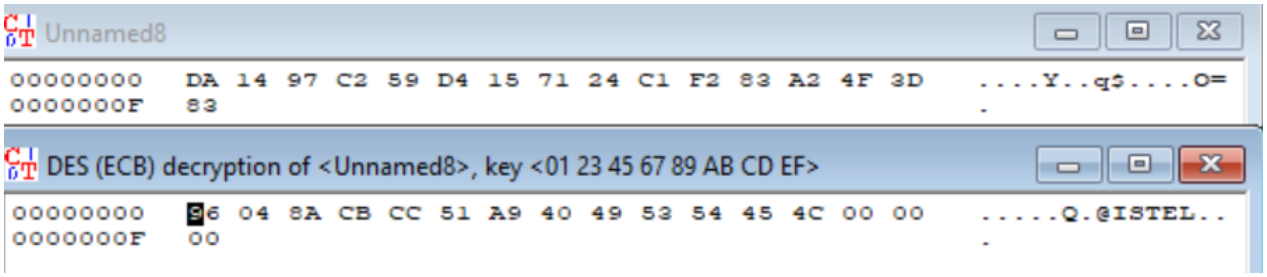
V. REZISTENȚA LA ERORILE DE TRANSMISIE:

Mesaj: HORST FEISTEL

Cheie de Criptare: 01 23 45 67 89 AB CD EF

Mesaj Criptat: DA **0**4 97 C2 59 D4 15 71 24 C1 F2 83 A2 4F 3D 83 (**ECB**)

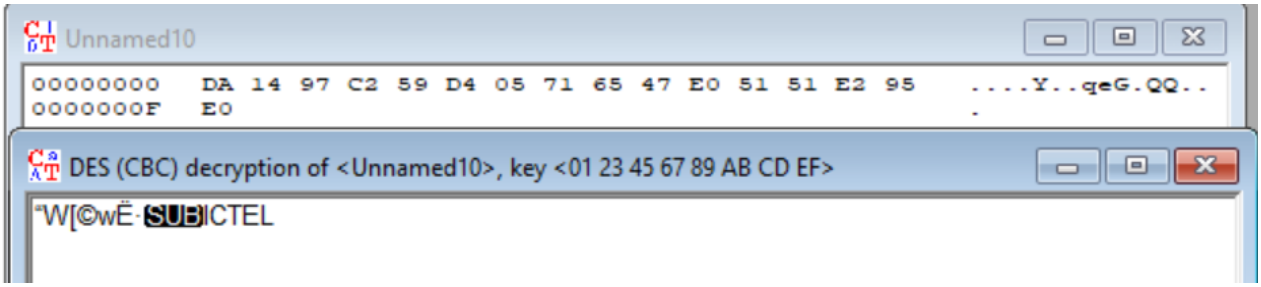
Mesaj Criptat Modificat: DA **1**4 97 C2 59 D4 15 71 24 C1 F2 83 A2 4F 3D 83 (**ECB**)



Mesaj: HORST FEISTEL

Cheie de Criptare: 01 23 45 67 89 AB CD EF

Mesaj Criptat: DA **0**4 97 C2 59 D4 15 71 65 47 E0 51 51 E2 95 E0 (**CBC**)



Mesaj Criptat Modificat: DA **1**4 97 C2 59 D4 05 71 65 47 E0 51 51 E2 95 E0 (**CBC**)

Concluzie: La CBC pierdem mai multă informație, datorită modului în care se realizează criptarea mesajului.