CHATONS
Diana David
Diana Hîncu

Electronică Aplicată – Enigma Machine 1

1. Introducere

Mașina Enigma 1 este un sistem de criptare utilizat în Al Doilea Război Mondial. Un aparat mecanic format dintr-o tastatură, rotoare, cablaj și tipar/lămpi (unde era văzut mesajul codat).

Ne propunem să implementăm acest mecanism ce criptare folosind o placă FPGA (Nexys A7), care va comunica prin UART cu interfața vizuală (monitor) și va primi un input (mesajul) prin tastatură. Rotoarele vor fi implementate software și vor fi setate cu ajutorul switch-urilor plăcuței. Urmând ca mesajul să fie criptat și afișat.

2. Mașina Enigma 1

Mașina Enigmă este o mașină de criptare dezvoltată în secolul XX, folosit atât comercial cât și în unitățile militare. Mașina este dotată cu o tastatură prin care se introduce textul simbol cu simbol, iar la capătul celălalt rezultă simbolurile criptate, calculate în funcție de starea rotoarelor.

Rotoare

Rotorul este un disc, cu o serie de ace de bronz, aranjate în cerc, pe partea opusă a discului având un număr corespunzător de contacte electrice circulare. De regulă, acestea sunt în număr de 26 (reprezentând alfabetul A-Z).

Când plasăm două rotoare unul lângă celălalt, acestea intră în contact electric și se formează astfel o legătură între literele fiecăruia (de exemplu, litera A de la primul rotor este conectată de litera Q de la al doilea rotor). Astfel, efectuăm în cascadă mai multe criptări (depinde de numărul de rotoare pe care le avem), cu o cheie dinamică (pozițiile rotoarelor se modifică după fiecare literă tastată).

Au fost dezvoltate mai multe tipuri de rotoare. Pentru proiectul de față vor fi folosite primele 3:

Rotorul I

Notch: Q

Alfabetul: EKMFLGDQVZNTOWYHXUSPAIBRCJ

Rotorul II

Alfabetul: AJDKSIRUXBLHWTMCQGZNPYFVOE

Notch: E

Rotorul III

Notch: V

CHATONS
Diana David
Diana Hîncu

Alfabetul: BDFHJLCPRTXVZNYEIWGAKMUSQO

Unde *notch* reprezintă litera pe care se află rotorul la poziția inițială. Primul rotor se rotește cu 1 după fiecare literă primită, iar rotoarele următoare se rotesc doar când rotorul anterior ajunge din nou la poziția de notch.

Plugboard

Reflector