Rezumat

Standardul Avansat de Criptare (AES – Advanced Encryption Standard), cunoscut și sub numele de Rijndael, este un algoritm de criptare simetrică, folosit astăzi pe scara largă în aplicații și adoptat în 2001 ca standard de organizația guvernamentală americană NIST.

Cei doi autori ai algoritmului Rijndael, Joan Daemen și Vincent Rijmen, au definit un algoritm de criptare pe blocuri în care lungimea blocului și cea a cheii puteau fi independente, de 128 de biți, 192 de biți, sau 256 de biți. Specificația AES standardizează toate cele trei dimensiuni posibile pentru lungimea cheii, dar restricționează lungimea blocului la 128 de biți.[1]

În lucrarea de față ne propunem să implementăm algoritmul de criptare AES pe o platformă FPGA (Field Programmable Gate Array), configurarea algoritmului fiind făcută prin intermediul unui limbaj de descriere hardware, și anume Verilog. Conexiunea dintre FPGA si PC va fi realizată cu ajutorul unui cablu USB-SERIALĂ RS232, prin intermediul căruia vor fi trimise mesaje/text pentru codificare și cheia secretă de pe PC către FPGA, și se va aștepta un mesaj codificat.

Descrierea problemei

Operațiile AES sunt definite sub formă de operații pe matrice, unde atât blocul, cât și cheia sunt scrise sub formă de matrice. Scrierea se realizează la începutul rulării cifrului, blocul este copiat într-un tablou denumit *state*, primii patru octeți pe prima coloană, apoi următorii patru pe a doua coloană, și tot asa pâna la completarea tabloului.

Deoarece AES este o criptare pe blocuri, rezultă că algoritmul funcționează prin repetarea acelorași pași de mai multe ori, acești pasi fiind:

- ADD ROUND KEY
- BYTE SUB
- SHIFT ROW
- MIX COLUMN

Pentru primul pas, vom efectua operația ADD ROUND KEY, în care executam un "XOR exclusiv" între biții din matricea state și biții din matricea cheii. Pasul următor este BYTE SUB în care facem o substituție între fiecare element din matricea state cu o valoare din SBOX. Următorul pas deplasează la stânga a doua linie din matricea state, cu două poziții a treia linie și cu trei poziții ultima linie. Acest pas este esențial în criptarea AES deoarece tabloul state este populat inițial pe coloane, astfel rezultă o securitate mult mai sporită. Ultimul pas este MIX COLUMN în care elementele din matricea state se înmulțesc cu o matrice predefinită, valoarea rezultată fiind noua valoare din matricea de stare.

În funcție de dimensiunea cheii, pașii de mai sus se vor repeta de un număr diferit de ori, exact în această ordine. Excepție face ultimul pas în care nu mai avem MIX COLUMN, iar rezultatul este trimis către output.