Trabalho Prático 1

Henrique Soares Assumpção e Silva

henriquesoares@dcc.ufmg.br

Universidade Federal de Minas Gerais

Julho 2021

1 Introdução

O objetivo deste trabalho é executar uma cifragem e de-cifragem de uma string de 32 bits, representando uma palavra de quatro caracteres em ASCII. Para isso, deve-se implementar uma porta XOR na linguagem Verilog, e, após se gerar uma OTP(One Time Pad) aleatória de 32 bits, realizar a operação XOR bit a bit entre o OTP e a palavra em ASCII.

2 Relatório

O programa foi desenvolvido na linguagem Verilog, compilada utilizando a ferramenta Icarus Verilog, no sistema operacional Windows 10. O programa foi inicialmente implementado e compilado em uma máquina com 16GB de RAM em um processador Intel Core I5-9400F.

Todo código deste trabalho está disponível no seguinte repositório do GitHub: https://github.com/HenrySilvaCS/Logical-Systems/tree/main/tp1

2.1 Detalhamento do código

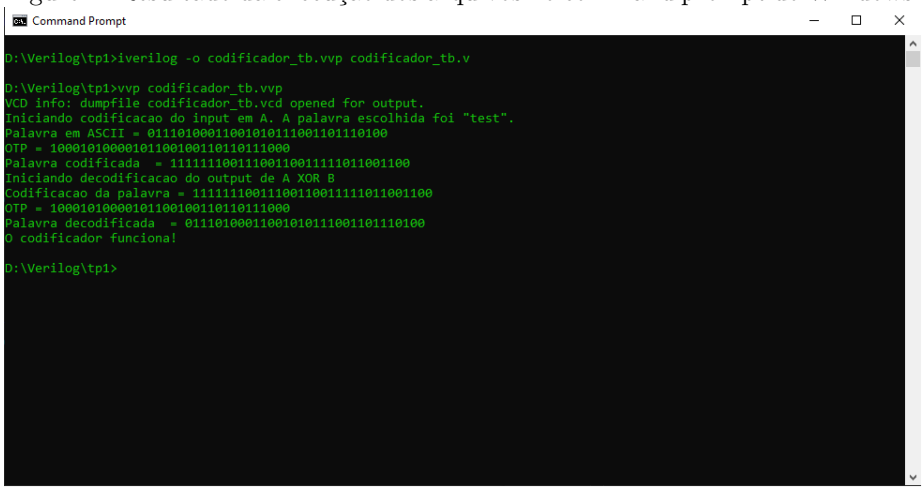
Para a realização do exercício, foi escolhida a palavra 'test' para ser cifrada. Além disso, foi gerado uma OTP de 32 bits verdadeiramente aleatórios. As representações em binário de cada um desses elementos são dadas a seguir:

- A palavra 'test' é representada por: 01110100 01100101 01110011 01110100
- A OTP gerada foi: 10001010 00010110 01001101 10111000

A porta XOR for implementada em Verilog, no arquivo `xor_logic.v`, utilizando-se de operadores lógicos a nível de bit. Foram instanciados dois vetores de 32 bits, um representando a palavra e outro a OTP, e então a operação XOR é

realizada bit a bit entre esses dois vetores. O test bench se localiza no arquivo `codificador_tb.v` e inicializa os vetores com as respectivas representações binárias da OTP e da palavra, e então executa a cifragem através do XOR. Após isso, se realiza a mesma operação com o output da cifragem, ou seja, realiza-se a operação XOR com a palavra cifrada e a OTP, obtendo-se assim a representação da palavra original. A figura 1 mostra o resultado da execução destes arquivos.

Figure 1: Resultado da execução dos arquivos no command prompt do Windows.



3 Resultados

O programa implementado funciona e realiza as atividades requisitadas. Isso pode ser observado ao se analizar os resultados obtidos. Os resultados são:

- A saída do XOR entre a palavra e a OTP foi: 11111110 01110011 00111110 11001100
- Após realizar o XOR desta saída com a OTP obtemos: 01110100 01100101 01110011 01110100

Nota-se que a saída final é exatamente igual à representação original da palavra 'test', ou seja, o programa consegue realizar a cifragem e de-cifragem com sucesso.