UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Criptografia com One-Time Pad

Aluno: Lucas de Oliveira Araújo

Matrícula: 333

Belo Horizonte, MG
2023

Sumário

---

1 Introdução

A criptografia é uma técnica amplamente utilizada para proteger a confidencialidade e integridade das informações transmitidas ou armazenadas. Uma das técnicas de criptografia mais seguras é o One-Time Pad (OTP), que deriva da cifra de Vernam. O OTP utiliza uma chave secreta aleatória do mesmo tamanho (ou maior) da mensagem a ser cifrada, tornando-se praticamente invulnerável a ataques criptográficos [1].

Neste projeto, foi implementado o stream cipher utilizando a linguagem Verilog e o compilador Icarus Verilog versão 12. O objetivo foi desenvolver um sistema capaz de realizar a cifragem e decifragem de mensagens utilizando o algoritmo OTP e a operação XOR.

2 Método

A implementação do sistema em Verilog foi dividida em etapas distintas. Primeiramente, foram criados os registradores para armazenar o OTP e a mensagem a ser cifrada. O OTP é gerado no módulo `shifter` através de uma seed de 8 bits escolhida pelo usuário. Após a geração do OTP, a mensagem que deve ser encriptada é encaminhada conjuntamente com o OTP para o módulo `cypher`, o qual realizada a operação XOR e devolve o texto criptografado.

Com o intuito de facilitar a encriptação de mensagens diferentes, o arquivo `definitions.v` foi criado. Nele são inseridos o código binário da mensagem e o seu número de bits. Assim, todos os módulos puderam incluir este arquivo de definições e, sem mais alterações em outras partes do código, diferentes mensagens podem ser criptografadas.

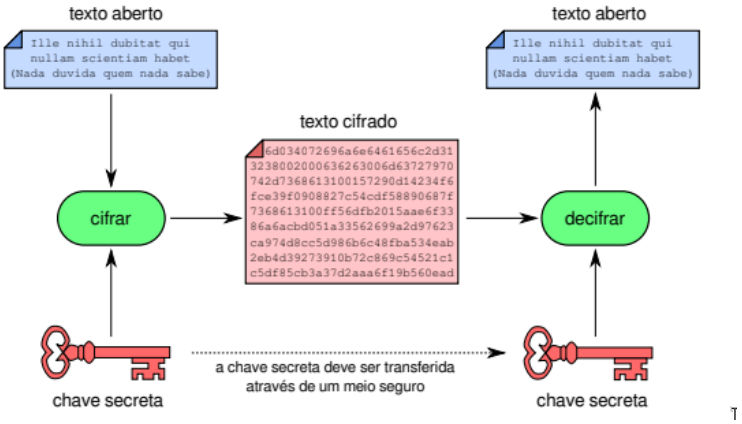

Figura 1: Algoritmos simétricos

Por fim, foi implementada a decifragem da mensagem. Sendo o OTP um algoritmo de criptografia simétrico, isto é, a chave de cifragem é a mesma utilizada para decifrar a mensagem, essa etapa consistiu em aplicar novamente a operação XOR utilizando o OTP sobre a mensagem cifrada. Dessa forma, obtemos a mensagem original. O exemplo de utilização do programa é exposto na figura 2.

```
~/Projects/ISL_VERILOG/cypher
❯ iverilog shifter.v cypher.v cypher_tb.v definitions.v -o cypher.exe

~/Projects/ISL_VERILOG/cypher
❯ vvp cypher.exe
VCD info: dumpfile waveform.vcd opened for output.
plaintext : Blind Melon - Mouthful of Cavities
ciphertext: q_Z]W~V_\]~\FG[UF_\UpREZGZV@
decrypted : Blind Melon - Mouthful of Cavities
cypher_tb.v:36: $finish called at 13 (1s)
```

Figura 2: Criptografando mensagens

3 Conclusão

Neste trabalho, foi implementado a criptografia de mensagens utilizando o método OTP em conjunto com a operação lógica XOR. Essa implementação foi realizada utilizando a linguagem Verilog, de forma que fosse possível representar o circuito sequencial para o método de criptografia citado.

Durante a implementação, foram adquiridos conhecimentos sobre a utilização da linguagem Verilog para construção de sistemas digitais, bem como a compreensão dos princípios básicos da criptografia e a importância da escolha de algoritmos seguros para a proteção das informações.

Referências

[1] *One-time Pad*. URL: `http://xingu.fisica.ufmg.br:8087/~inetsec/site2/left-sidebar.html` (acesso em 06/07/2023).