Trabalho 02.1

Criptografia

Prof. Roberto Cabral

22 de Setembro de 2017

Introdução

Vimos que os algoritmos criptográficos de encriptação, muitas vezes, encriptam blocos de tamanho fixo. Como as mensagens podem ter tamanho arbitrário, foram propostos modos de operações que permitem encriptar mensagens de qualquer tamanho de forma segura. Este trabalho consiste em implementar dois modos de operações. O modo de operação CBC e o modo de operação CTR.

Objetivos

O objetivo do trabalho é implementar os modos de operações CBC e CTR usando o algoritmo de encriptação AES. Será fornecido uma implementação do AES em C, mas o aluno é livre para usar sua própria implementação do AES tal a linguagem que lhes for mais conveniente. Será acrescido um bônus para a dupla que implementar o modo de operação GCM.

Detalhes

Deverá ser submetido tanto o código fonte tal como o código executável, por email, até o dia 02 de Outubro de 2017; o programa deve ser acompanhado de um pequenos texto com instruções de uso. Deverá também ser entregue um relatório em PDF detalhando o que foi feito e descrevendo as dificuldades encontradas. O trabalho poderá ser feito em dupla. A avaliação do trabalho levará em conta o código, o relatório e uma pequena apresentação para o professor. Vale ressaltar que, embora o trabalho seja feito em dupla, a nota será atribuída individualmente.