

SEGUNDA LISTA DE EXERCÍCIOS

Criptografia e Segurança de redes – 01-2017

Disponibilizada em 26/04/2017 – A ser entregue em 24/05/2017

1. Create a program that can encrypt and decrypt using the AES algorithm. Use the AES example in Section 5.5 of the Stallings book as step-by-step testing data.
2. Create a program that can encrypt and decrypt using one the ciphering/deciphering modes:
 - a) Cipher block chaining mode (CBC), using DES as the basic cipher.
 - b) 16-bit cipher feedback mode (CFB), using AES as the basic cipher.
 - c) Counter mode (CTR), using DES as the basic cipher.
 - d) Output feedback mode (OFB), using AES as the basic cipher.

Each student should choose one of the options above.