Lista de exercícios 6
Chosen cypher-text Attacks
Segurança da Informação

3 de Outubro de 2016

1. Explique o cenário de segurança de um atacante capaz de escolher textos cifrados para a vítima decriptá-los.

2. Para que são úteis algoritmos codificação de padding.

3. O que é um oráculo de padding?

4. Que tipo de modelo de ameaça considera o uso de oráculos de padding?

5. Um pesquisador da área de criptografia afirmou que é possível construir um esquema determinístico que é seguro contra ataques do tipo CPA. Discuta essa afirmação.