Redes de Computadores II – DES e AES

Daniel Veiga da Silva Antunes

1 Data Encryption Standard (DES)

Baseado no algoritmo de Feistel, trata-se de uma criptografia simétrica que cifra blocos de 64 bits, utilizando uma chave de 52 bits + 8 bits de paridade. Posteriormente gerou o outro algoritmo 3DES, que utiliza 3 chaves e é considerado mais seguro.

1.1 Vantagens

Fácil implementação.

1.2 Desvantagens

Considerado inseguro para diversas aplicações, devido ao tamanho reduzido de sua chave, podendo ser quebrada via força bruta. Por se tratar de uma criptografia simétrica, uma única chave realizada a encriptação e a decriptação, podendo ser uma vulnerabilidade

2 Advanced Encryption Standard (AES)

Criptografia simétrica de blocos de 128 bits, que utiliza chaves de 128, 192 e 256 bits. Baseada em no princípio de design conhecido como rede de substituição-permutação.

2.1 Vantagens

De fácil implementação. Possui um bom desempenho, não exige muito processamento.

2.2Desvantagens

A implementação da inversa é diferente da encriptação e exige mais processamento e complexidade. Por se tratar de uma criptografia simétrica, uma única chave realizada a encriptação e a decriptação, podendo ser uma vulnerabilidade