Universidade Federal do Rio Grande do Sul - UFRGS
Disciplina: Segurança em Sistemas de Computação
Prof. Dr. Jéferson Campos Nobre

Atividade Aula 07

Exercício 1

1. Obtenha o histograma do texto plano indicado.
2. Criptografe o texto plano indicado usando Cifra de César.
3. Criptografe o texto plano indicado usando DES (CBC) com a chave indicada.
4. Obtenha o histograma dos textos criptografados.
5. Compare os histogramas. Como é possível explicar suas observações?

Exercício 2

1. Criptografe o texto plano indicado (M=Bob's salary is $25000--Tom's salary is $15000) usando DES (ECB) com a chave indicada (K = 11 22 33 44 55 66 77 88).
2. Copie os blocos cifrados resultantes (C1, C2, ... Ck).
3. Troque os blocos resultantes C1 e C4 para obter uma sequência de blocos cifrados (C4, C2, C3, C1 ... Ck).
4. Decriptografe o texto cifrado resultante. Qual a mensagem obtida? Explique.
5. Repita os passos 1-4, porém com DES (CBC). Compare os resultados. Explique.

Exercício 3

1. Encripte o texto indicado (M=Bob's salary is $25000--Tom's salary is $15000) com DES(CBC). Escolha a chave.
2. Considerando a sequência criptografada, modifique os blocos para causar a seguinte modificação na mensagem decriptografada: $15000 -> $.5000. Explique como isso foi realizado.
3. Todos os blocos criptografados são decriptados corretamente depois dessa modificação? Explique.
4. O modo de operação CBC assegura integridade? Explique considerando o exercício realizado.

Referências

- Baseado em material do Prof. Mario Cagalj (University of Split)