Universidade Tecnológica Federal do Paraná (UTFPR)
Departamento Acadêmico de Informática (DAINF)

Introdução à Criptografia

Professor: Rodrigo Minetto (rodrigo.minetto@gmail.com)

Lista de exercícios

O algoritmo S-DES (Simplified DES) desenvolvido pelo Prof. Edward Schaefer da Universidade de Santa Clara (USA) tem propriedades similares ao DES original e é muito utilizado para propósitos educacionais. Para maiores informações sobre esse algoritmo leia o arquivo "**sdes.pdf**" (em anexo a esta aula). Para os exercícios abaixo utilize o algoritmo "**sdes.c**" (também em anexo ao material da aula).

1) Qual o principal módulo, em termos de segurança, no algoritmo DES?

2) Algoritmos modernos para cifragem por bloco têm excelente difusão. Quais são os bits originais e cifrados para a letra 'e' ao se utilizar a chave 473 no algoritmo **sdes.c**? Quantos bits mudaram no total? E ao se utilizar a chave 472?

3) Faça um ataque por força bruta no arquivo "misterio_sdes.txt" (cifrado com **sdes.c**) e descubra a chave utilizada e o conteúdo do arquivo.

4) Cifre um arquivo com o "**3-SDES**" (três rodadas do **sdes.c**) e teste com um ataque por força-bruta semelhante ao exercício 2. O arquivo consegue ser decifrado?

5) Utilize o código "**ides.c**" (Simplified-DES **para imagens**) para criptografar a imagem lena.pgm e arma.pgm com a técnica ECB. Questão: é possível ter noção do conteúdo da imagem? Modifique esse código para utilizar alguma outra técnica por bloco (por exemplo CBC). Agora é possível ter noção do conteúdo da imagem? Atribua zero para o vetor de inicialização (IV). Ps. para visualizar as imagens .pgm no windows use o software IrfanView.

6) O DES por ser inseguro não é mais incluído em aplicações para criptografia. No entanto, o 3-DES ainda é muito utilizado. Um modo de cifrar arquivos com o 3-DES no linux é através do software GPG (GNU Privacy Guard), que vem instalado por default em qualquer versão linux e pode ser baixado e instalado também no Windows (Gpg4win). Para cifrar com o 3-DES utilizando o GPG digite em um terminal linux:

```
a)  gpg --symmetric --cipher-algo 3DES arquivo.txt

b) Enter passphrase:                    (digite a chave de ciframento duas vezes!)

c) O saída do software é o arquivo: arquivo.txt.gpg

d) Para decifrar o arquivo faça:

   gpg -o decifrado.txt -d arquivo.txt.gpg          (digite a chave de ciframento)

e) O resultado do deciframento é armazenado no arquivo 'decifrado.txt'.
```

Teste o software em questão decifrando o arquivo "**misterio_gpg.txt.gpg**" que foi cifrado com a chave "**segredo**".