Segurança de Redes
Prof. João Henrique Kleinschmidt

Para as questões 1 a 6 utilize o software *WEBCry*:

1) Criptografe uma mensagem de texto usando os algoritmos DES e AES. Mostre e compare a saída do texto criptografado (em hexadecimal) com os dois algoritmos. Faça também o processo inverso (decifrar a mensagem). O texto voltou ao original? O que acontece se você usar uma chave diferente na decriptografia?

2) Faça a criptografia de uma mensagem de texto usando o algoritmo DES e verifique a saída (texto criptografado). Faça novamente a criptografia, usando a mesma chave. A saída permanece igual? Altere um caractere na mensagem de texto e faça a criptografia com a mesma chave usada anteriormente. O que é possível observar?

3) Gere uma chave do algoritmo RSA. Faça a criptografia de mensagens de texto usando diferentes tamanhos de chave do RSA. Mostre e compare a saída (texto criptografado).

4) Cifre um arquivo *JPEG* usando um algoritmo simétrico. Tente abrir o arquivo cifrado. Faça a decifragem do arquivo e tente abrir novamente. Descreva o que foi observado.

5) Criptografe arquivos de diversos tamanhos (de poucos kB até vários MB) usando os algoritmos DES, AES e RSA. Faça uma tabela comparativa em relação ao tempo de execução e explique os resultados obtidos.

6) Criptografe alguns arquivos diferentes como textos, imagens JPEG e bmp, vídeos, entre outros, utilizando os algoritmos DES e AES. Compacte os arquivos originais e criptografados (usando WinZip, WinRAR, etc). Compare e explique os resultados obtidos em relação ao tamanho dos arquivos compactados (originais e criptografados).

7) Execute o programa *StringEncrypter.java* (usando *NetBeans* ou outro compilador Java):

a) Verifique o funcionamento do programa (cifragem/decifragem).

b) A chave de criptografia pode ser gerada a partir de uma senha. Esta senha é combinada com um número, chamado de *salt*, servindo como semente para geração da chave. Modifique a senha de geração de chave (*testUsingPassPhrase*) para “teste2019". Execute o programa várias vezes. O texto criptografado é sempre igual para uma mesma senha? E para senhas diferentes? Explique.

8) Crie e implemente (em qualquer linguagem de programação) um algoritmo de criptografia de bloco usando a cifra de Feistel com dois estágios, conforme figura abaixo. A entrada deve ser um bloco de 8 bits. A chave deve ter 4 bits (escolha uma chave qualquer). Mostre passo a passo o processo de criptografia E decriptografia. (obs: o algoritmo criado deve ser aplicado na função F).