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

Introdução à Criptografia

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

Lista de exercícios (escolha três exercícios para entregar)

1) Utilize o programa "sorteio.c" em anexo ao material da aula, que dado um nome de entrada — no caso deste exercício utilize o seu primeiro nome — sorteia uma entrada para a tabela S-Box do algoritmo AES. Dado a entrada sorteada para o seu nome, calcule o inverso multiplicativo desse número (conforme visto na seção 6 dos slides "Construindo uma S-Box").

```
Exemplo:

gcc -o sorteio sorteio.c        (compilando o programa que sorteia a entrada!)

./sorteio
 Digite o seu nome: rodrigo        (executando o sorteio com o primeiro nome!)
 Calcula a entrada: 6c (S-Box)

Ao realizar os cálculos para 6C (com teoria de Galois) obtemos o resultado 50!
```

2) Sejam w_0, w_1, w_2 e w_3, as quatro primeiras palavras utilizadas no escalonamento de chaves. Explique como são obtidas as próximas palavras: $w_4, w_5, \ldots$. Qual a mágica para lidar com 3 tamanhos de chaves diferentes? Em teoria, qual a segurança de um AES com 128 bits de chave?

3) Qual dos seguintes polinômios é irredutível? (a) $x^4 + x + 1$ ou (b) $x^2 + 4x + 4$?

4) Para fins educacionais, o código fonte do algoritmo AES está em anexo ao material da aula (veja o código "**aes.c**" e tente identificar como as estruturas do algoritmo foram codificadas). Assim como visto na aula passada, o software GPG (GNU Privacy Guard) — instalado por default em qualquer versão linux (e que pode ser instalado no windows Gpg4win) — possui uma opção para ciframento através do algoritmo AES:

```
gpg --symmetric --cipher-algo AES256 arquivo  (cifrando AES, chave 256 bits!)

gpg -o decifrado.txt -d arquivo.gpg           (decifrando!)
```

5) Este exercício é aberto para que você possa descrever alguma etapa do algoritmo AES em detalhes.