Fundamentos de Redes de Computadores, turma A / Prof.: Fernando W. Cruz

Laboratório sobre criptografia simétrica e assimétrica

A) Objetivos do laboratório

O objetivo deste laboratório é permitir que o aluno avance seus conhecimentos sobre criptografia simétrica/assimétrica por meio de atividades práticas.

B) Roteiro do laboratório

Considere o texto a seguir:

A geometria fractal é baseada no princípio de que um objeto geométrico pode ser dividido em partes menores, cada uma delas semelhante ao objeto original. São, portanto, objetos com muitos detalhes, com similaridade recursiva (os detalhes são similares ao objeto original). Um dos fractais interessantes de se observar é o fractal Julia. Um conjunto Julia (*Julia set*) é uma generalização do famoso conjunto Mandelbrot [https://pt.wikipedia.org/wiki/Conjunto_de_Mandelbrot], que está ilustrado na Figura 1.

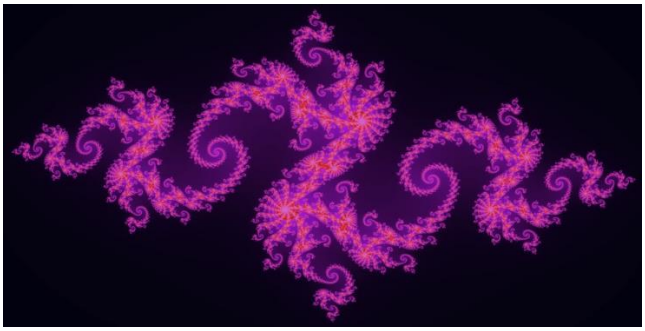

Figura 1 – Fractal Julia

Esse fractal é definido como segue. Dado `z` um ponto no plano complexo 2-D, calculamos a série definida como: $z_0 = z$ e $z_{n+1} = z_n^2 + c$, onde `c = -0,79 + i * 0,15`, ou seja, um número complexo. Valores diferentes de `c` levam a imagens diferentes, e conhecemos muitos valores que produzem imagens "bonitas". A cor de um pixel correspondente ao ponto z é determinada com base no número de iterações antes que o módulo de z_n seja superior a 2 (ou até que um número máximo de iterações seja atingido). O programa `fractal.c` (que está anexado a esta especificação) é o código que produz a imagem da Figura 1, mas é possível alterá-lo para criar imagens diferentes. Este programa pode ser compilado com o parâmetro a seguir:

```
$ gcc fractal.c -o fractal -lm
```

Para executá-lo, basta digitar o comando

`$ ./fractal` **<N>,** onde **N** é a altura da figura do fractal (ou número de linhas). Esse parâmetro é utilizado para o cálculo da largura (2*N) e o cálculo da área do fractal (altura * largura * 3).

A saída desse programa é um arquivo em formato bmp (Bitmap) que pode ser aberto com qualquer editor de imagens do seu sistema operacional.

1. Os alunos devem montar um diálogo TCP para repassar o fractal entre Alice e Bob (partes comunicantes) usando criptografia simétrica, considerando o seguinte:
   - Deve-se evitar que alguém perceba que a imagem BMP está encriptada. Para isso, deve-se aplicar a criptografia apenas no corpo do arquivo (não inclua o cabeçalho do arquivo BMP no processo de encriptação)

- Os alunos devem desenvolver (ou adotar uma solução pronta, com a respectiva citação) do algoritmo DES (*Data Encryption Standard*) para a encriptação do fractal
- Alice deve criar a chave de encriptação/desencriptação e repassá-la para Bob via conexão TCP. Portanto, é preciso definir um diálogo entre as partes para compartilhamento da chave gerada
- No lado remoto, Bob deve conseguir visualizar a imagem BMP como criptograma e como texto claro (sem criptografia) – não precisa criar programa de visualização (usar editores de imagem do ambiente operacional)

2. Os alunos devem montar um diálogo TCP para repassar o fractal usando criptografia assimétrica com RSA. Requisitos:
   - O programa deve permitir a criação de números primos (p e q). Sugere-se que estes números tenham entre cinco e seis dígitos e coloque-os num arquivo, separado por um "#". Por exemplo se o programa for acionado com o parâmetro -p, ele cria os primos e os apresenta na console ou envia-os para um arquivo, como ilustrado a seguir:
     ```
     $ gerarsa -p > primos.txt
     ```
   - O programa deve permitir a geração das chaves pública e privada a partir de p e q, colocando-as em arquivos `chave.pub` e `chave.priv`. Em cada um dos arquivos, é importante definir os separadores adequados, de modo que seja possível aplicar as fórmulas de encriptação/desencriptação do RSA
   - O programa deve, por fim, permitir encriptação/desencriptação de um arquivo com as chaves criadas. Obs.: Faça testes para garantir que esse procedimento está funcionando
   - Supondo que apenas Bob tem o par de chaves RSA (criado pelo algoritmo preparado nos passos anteriores), promova um diálogo TCP de modo que Alice consiga enviar o arquivo BMP para Bob.

C) Questões de Ordem

- O laboratório pode ser feito por grupos de até 4 alunos
- Este laboratório deve ter os artefatos entregues no Moodle (arquivo zipado) e apresentado em data estabelecida pelo professor. A entrega deve ser composta por: *(i)* relatório do laboratório + slides, e *(ii)* códigos, instruções de uso e todas as informações necessárias para esclarecimento e uso dos programas entregues.
- Os alunos podem realizar o experimento em ambientes Linux/gnu, linguagem C
- O relatório deve conter o seguinte:
  i) Identificação da disciplina/turma, do grupo (matrícula e nome) e o nome do laboratório
  ii) Introdução – pequeno texto indicando o objetivo e a organização do relatório
  iii) Descrição do experimento – **criptografia simétrica** e o diálogo TCP criado – Listagem dos códigos com comentários, instruções de execução e comentários sobre dificuldades e soluções encontradas
  iv) Descrição do experimento – **criptografia assimétrica** e o diálogo TCP criado – Listagem dos códigos com comentários, instruções de execução e comentários sobre dificuldades e soluções encontradas
  v) Conclusão – Gerar um texto conclusivo sobre o experimento, mostrando diferença de desempenho entre as duas soluções para encriptação/desencriptação. Ao final, cada membro do grupo deve apontar eventuais aprendizados, nível de participação no experimento e nota de auto-avaliação.