Lista de exercícios: Números aleatórios e cifras de bloco

Prof. Gabriel Rodrigues Caldas de Aquino

Compilado em:
September 19, 2025

1 PRNG e TRNG

Tradicionalmente, a preocupação na geração de uma sequência de números supostamente aleatórios é garantir que a sequência seja estatisticamente aleatória.

- Explique a diferença fundamental entre um TRNG e um PRNG.
- Cite dois critérios principais que são usados para validar a aleatoriedade.
- O que é propensão, que os TRNG costumam apresentar
- É comum que os TRNG sejam usados para alimentar um PRNG. Diga como e qual o motivo disso acontecer.

Justifique suas respostas.

2 Princípios de Shannon na Cifra de Feistel

Considere o código abaixo:

```
def funcao_F(R,K):
  return (R * K ) & 0xFF

chave = 0b10101010
bloco = 0b1100110010101010
L = (bloco >> 8) & 0xFF
R = bloco & 0xFF
F = funcao_F(R, chave)
L1 = R
R1 = L ^ F
cifrado = (L1 << 8) | R1
L = (cifrado >> 8) & 0xFF
R = cifrado & 0xFF
```

```
invertido = (R << 8) | L
print(f"Fim: {invertido:016b}")
```

- Explique os seguintes conceitos propostos por Claude Shannon: Confusão e Difusão.
- Relacione como cada um deles é implementado na estrutura de uma Cifra de Feistel, usando o a implementação de uma rodada de Feistel apresentada em aula.
- A Função F do código apresentado em aula é dado por: $(R * K)\&0xFF$. Essa função é linear. Shannon enfatizou a necessidade de não-linearidade para a função F. Discuta.
- Apesar de simples, a Cifra de Feistel é base para uma série de cifras comerciais, antigas e atuais. Diga quais são os principais parâmetros que podemos modificar em uma Cifra de Feistel que pode deixá-la mais robusta e resistente à ataques.

3 DES e o 3DES

O 3DES foi criado em resposta a problemas de segurança encontrados no DES.

1. Discorra sobre os motivos principais que motivaram a substituição do DES.
2. O 3DES teve como objetivo ser compatível com o DES. Explique como essa compatibilidade foi alcançada.
3. Considerando que o 3DES aplica o algoritmo DES três vezes, qual é o tamanho efetivo de chave quando utilizamos:
   (a) Três chaves independentes (K_1, K_2, K_3)?
   (b) Apenas duas chaves ($K_1 = K_3$)?
4. Apesar de o 3DES utilizar 3 chaves, o que na prática nos dá uma chave maior que o DES, ele tinha o mesmo tamanho de bloco. Qual era o problema disso? Justifique sua resposta.