Departamento de Ciência da Computação

Introdução à Criptografia

Prof. Charles F. de Barros

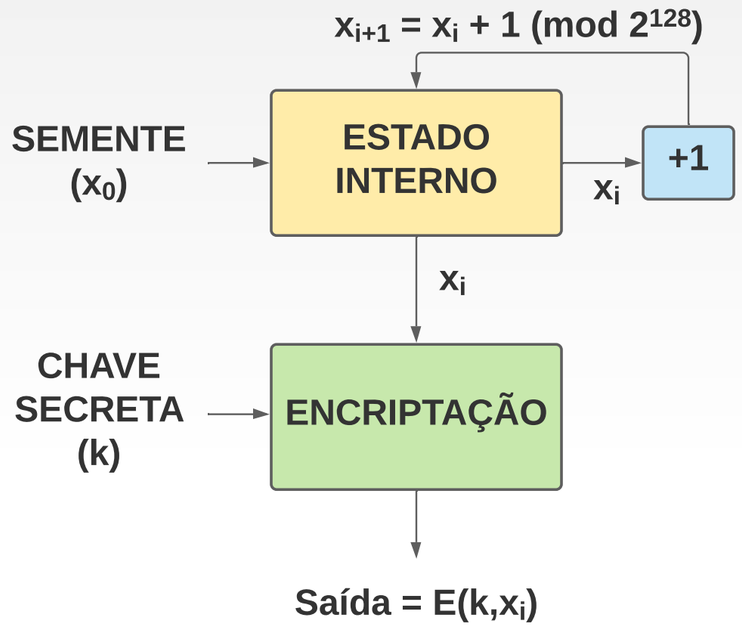
ATIVIDADE 1 (A1)

INSTRUÇÕES

- Esta é uma atividade **INDIVIDUAL**
- Prazo para entrega: até as 23:59 do dia 15/10/2020
- Forma de entrega: Portal Didático
- **Objetivo: implementar dois tipos de gerador pseudo-aleatório, utilizando a cifra de bloco AES.**
- A implementação pode ser feita em qualquer linguagem. No entanto, recomenda-se a linguagem Python, com o uso da biblioteca PyCryptodome
- O arquivo com o código-fonte deve ser salvo com o seu nome. Por exemplo: CHARLES_BARROS.py
- Não é necessário fazer documentação.
- Você deve pesquisar sobre a utilização da cifra AES na biblioteca PyCryptodome (ou na biblioteca de sua escolha)

GERADOR 1

- O estado interno é um contador, que a cada iteração é incrementado de uma unidade
- A saída do gerador é a encriptação do estado atual, utilizando a chave secreta
- A semente é o valor inicial do contador



GERADOR 2

- O estado interno é atualizado a cada iteração, encriptando-se o estado anterior com a chave secreta
- A saída do gerador é o próprio estado interno a cada iteração