Cifras de Fluxo

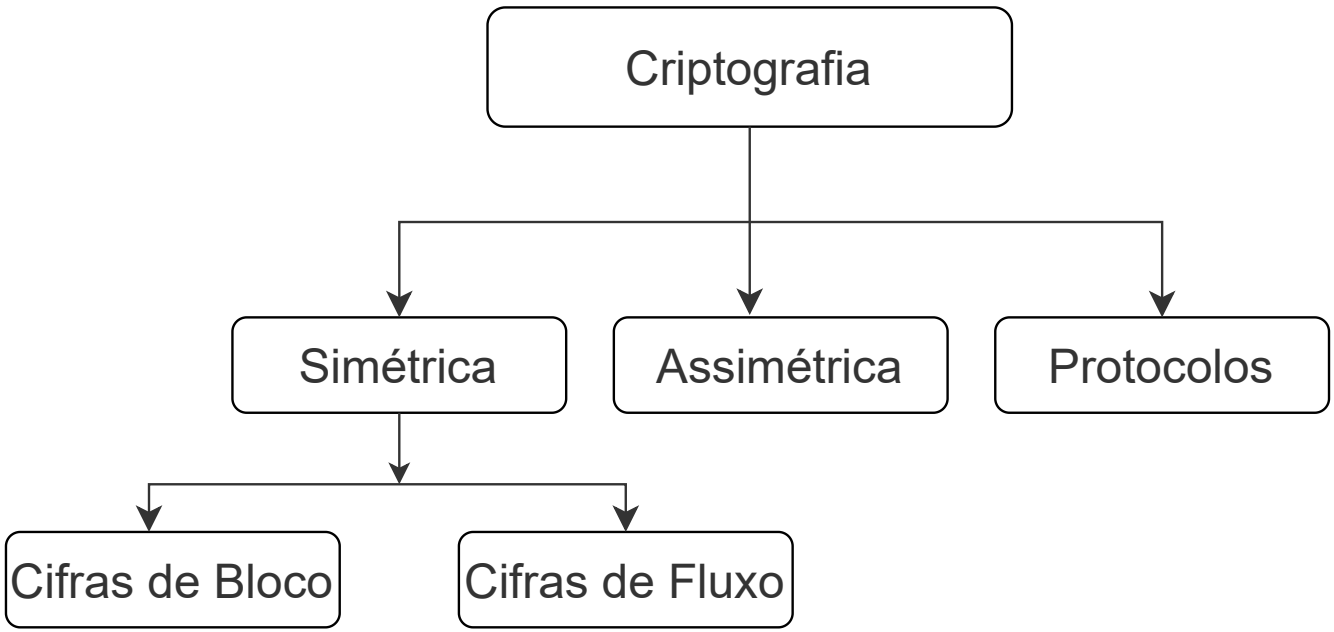
Auditoria e Segurança de SI

Prof. Roberto Cabral
rbcabral@ufc.br

Universidade Federal do Ceará

1º semestre/2023

Introdução


Criptografia
Simétrica
Assimétrica
Protocolos
Cifras de Bloco
Cifras de Fluxo

Cifras de fluxo

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Encriptam bits individualmente.
- A encriptação consiste em somar um bit da chave de fluxo com um bit do texto claro.
  - Cifra de fluxo síncrona: a chave de fluxo depende apenas da chave.
  - Cifra de fluxo assíncrona: a chave de fluxo também depende do texto encriptado.

Cifras de bloco

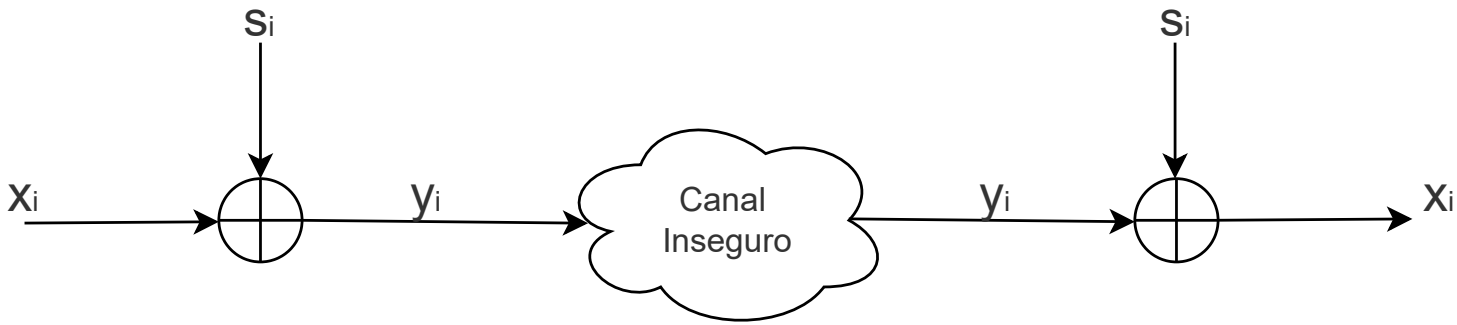
- Encriptam um bloco inteiro do texto claro com uma mesma chave.
- Nessas cifras, a encriptação de qualquer bit de um dado bloco depende de todos os outros bits desse bloco.
- Na prática, a grande maioria das cifras de blocos possuem blocos de 128 bits.

Encriptação e decriptação com Cifras de fluxo

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Definição

Em uma cifra de fluxo, o texto claro, o texto encriptado e a chave de fluxo consistem de bits individuais. Sejam $x_i, y_i, s_i \in \{0, 1\}$.
Encriptação: $y_i = e_{s_i}(x_i) \equiv x_i + s_i \mod 2$.
Decriptação: $x_i = d_{s_i}(y_i) \equiv y_i + s_i \mod 2$.



Encriptação e decriptação com Cifras de fluxo

1. A encriptação e a decriptação usam a mesma função!
2. Porque uma simples adição módulo 2 por ser usada como encriptação?
3. Qual a natureza dos bits da chave de fluxo?

Porque a encriptação e a decriptação podem usar a mesma função?

- Sabemos que o texto encriptado y_i foi computado por $y_i \equiv x_i + s_i \mod 2$.
- Se colocarmos a expressão de encriptação na função de decriptação temos:

$$\begin{aligned} d_{s_i} &\equiv y_i + s_i \mod 2 \\ &\equiv (x_i + s_i) + s_i \mod 2 \\ &\equiv x_i + 2s_i \mod 2 \\ &\equiv x_i + 0 \mod 2 \\ &\equiv x_i \mod 2 \end{aligned}$$

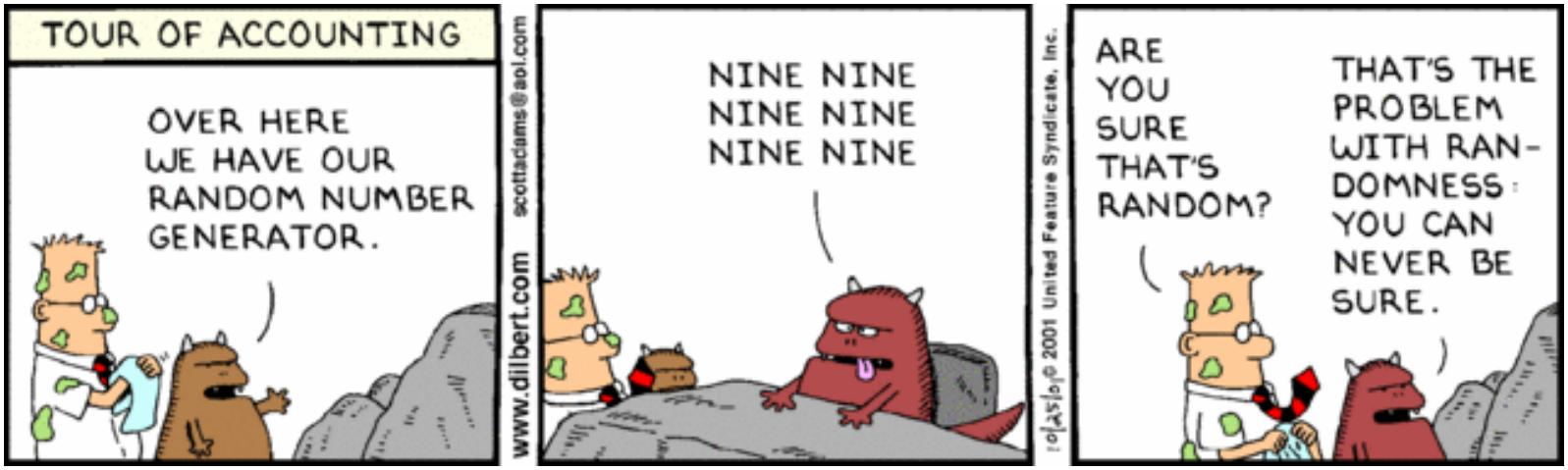
Porque uma adição módulo 2 é uma boa função de encriptação?

- Se fizermos aritmética módulo 2, os únicos valores possíveis são 0 e 1.
- Assim, podemos tratar uma aritmética módulo 2 como uma função booleana.
- A aritmética módulo 2 é equivalente a operação XOR.
- Porque usar a função XOR e não outra função booleana?

Qual a natureza dos bits da chave de fluxo?

- A segurança de uma cifra de fluxo depende diretamente da chave de fluxo!
- A geração da chave de fluxo é a principal questão no projeto de uma cifra de fluxo.
- Basicamente, uma boa chave de fluxo deve ser vista por um atacante como uma sequencia de bits aleatórios.
- Desse modo, precisamos de bons Geradores de números aleatórios (RNG).

Geração de números aleatórios verdadeiros (TRNG)



Geração de números aleatórios verdadeiros (TRNG)

- Possuem a propriedade de que não podem ser reproduzidos.
- Por exemplo, se rolarmos uma moeda 100 vezes e guardarmos o a sequência resultante de 100 bits, será virtualmente impossível alguma outra pessoa na terra conseguir a mesma sequência.
- Os TRNGs são baseados em processos físicos, como lançar moedas, rolar dados, ruídos de semicondutores clock de circuitos digitas e decaimento radioativo.
- Na criptografia, TRNGs são normalmente necessários para gerar chaves de sessão, que são distribuídas entre as entidades.

Geração de números pseudoaleatórios (PRNG)

- Geram sequências que são calculadas a partir de um valor inicial. Normalmente são computadas recursivamente da seguinte forma: $s_0 = \text{seed};$ $\quad s_{i+1} = f(s_i), , i = 0, 1, \ldots$
- Note que os PRNGs não são aleatórios em um verdadeiro sentido da palavra, pois podem ser computados e são, portanto, completamente deterministas.
- Um requisito importante para um PRNG é que ele deve satisfazer propriedades estatísticas, ou seja, sua saída deve se aproximar a uma sequência verdadeiramente aleatória.

Geração de números pseudoaleatórios criptograficamente seguros(CSPRNG)

- São um tipo especial de PRNG.
- Um CSPRNG é um PRNG que é imprevisível.
- Informalmente falando, significa que dado n bits de de saída de uma chave de fluxo $s_i, s_{i+1}, \ldots, s_{i+n-1}$ é computacionalmente inviável computar os bits subsequentes $s_{i+n}, s_{i+n+1}, \ldots$.
- Uma outra propriedade dos CSPRNG é que dada a mesma sequencia a cima, deve ser computacionalmente inviável computar qualquer bit precedente $s_{i-1}, s_{i-2}, \ldots$.

Segurança incondicional

Definição - Segurança incondicional

Um criptosistema é incondicionalmente seguro se não pode ser quebrado mesmo com recursos computacionais infinitos.

- Uma cifra com segurança de 10000 bits e com o ataque de força bruta sendo o mais viável, é incondicionalmente segura?
- Número de átomos que formam o universo conhecido é aproximadamente 2^{266}.

One-time Pad

Definição - One-time pad (OTP)

Uma cifra de fluxo onde:

1. a chave de fluxo $s_0, s_1, \ldots$ é gerada por um TRNG, e
2. a chave de fluxo é conhecida apenas entre as entidades legítimas, e
3. cada chave de fluxo s_i é usada apenas uma vez.

é conhecida como *one-time pad*. Essa cifra é incondicionalmente segura.

One-time Pad é prático?

- Não é fácil gerar números verdadeiramente aleatórios!
- É viável passar a chave de forma segura.
- O principal problema é não reusar a chave! Na prática, as chaves teriam que ser muito grandes.

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM