Revisão

- Sigilo perfeito tem 2 limitações
  - Chave tem que ter o comprimento da mensagem
  - Chave só poder ser usada apenas uma vez
- Com Pseudo-OTP é possível superar a primeira limitação
- Mas ainda tem a segunda, como evitá-la?

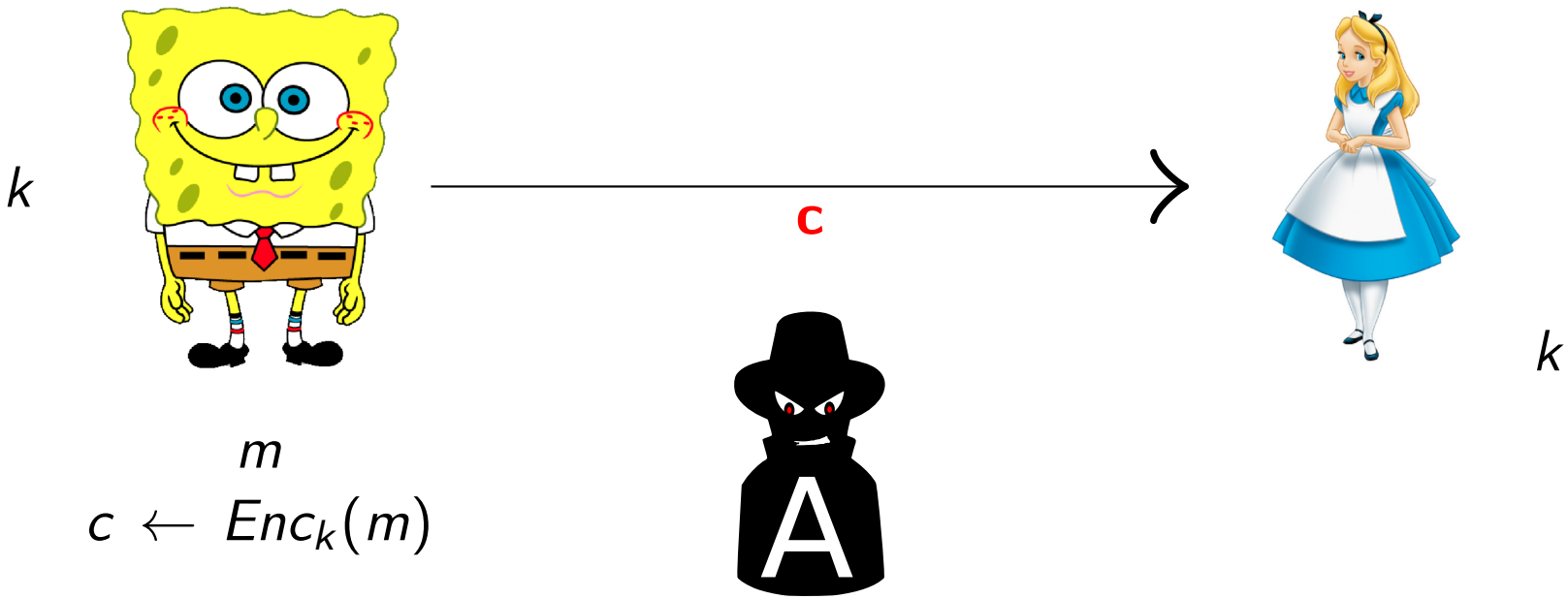
Revendo definição de segurança

- Definir definição de segurança mais apropriada
- Definição de segurança tem 2 partes
  - Objetivo da segurança
  - Modelo de ameaça
- Vamos manter o objetivo da segurança e melhorar o modelo de ameaça

Revisão: modelos de ameaça

- Ataque usando somente texto cifrado – OTP
  - Somente um ou vários?
- Ataque usando texto em claro conhecido
  - Atacante conhece o texto sendo enviado
  - Exemplo: mensagem começa com “Bom dia ...”
- Ataque escolhendo texto em claro – esta aula
  - **Chosen-plaintext attack**
  - Atacante consegue encriptar mensagens
  - Midway
- Ataque escolhendo texto (de)cifrado
  - Atacante consegue decriptar mensagens

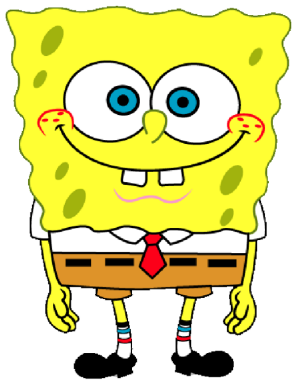
Sigilo de mensagem única



Ataques de textos em claro escolhidos

- Definição de segurança contra ataques de textos em claro escolhidos (chosen-plaintext attacks – CPA-security)
  - Hoje em dia, esta é a noção mínima de segurança que um esquema de encriptação deve usar

CPA-security

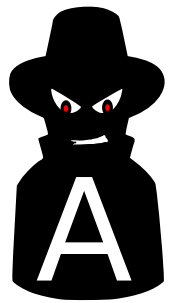


k

c_1, c_2

k

m_1, m_2



m_1, m_2

$c_1 \leftarrow Enc_k(m_1)$

$c_2 \leftarrow Enc_k(m_2)$

O modelo de segurança CPA é forte demais?

- Na prática, existem muitas maneiras de um atacante influenciar o que é encriptado
  - Não é claro qual é a melhor forma de como modelar tal influência
  - O modelo de ataque de texto em claro escolhido considera essa influência
- Em certos casos o atacante pode ter controle significativo sobre o que é encriptado

História da Ilha de Midway, 2a Guerra Mundial

- EUA querem descobrir qual é o próximo alvo dos Japoneses, identificado por AF
- EUA envia mensagem sem encriptção a partir da Ilha de Midway para Japoneses acreditarem que ilha precisa de água
- Japoneses retransmitem mensagem com criptografia para comando dizendo que em PA falta água
- Filmes: Midway (1976), A Beautiful Mind (2001)
- História da batalha de Midway

Cenário de segurança contra textos em claro escolhidos (CPA-security)

- Escolher Π, A
- Definir experimento aleatório $PrivCPA_{A,\Pi}(n)$:
  - $k \leftarrow Gen(1^n)$
  - $A(1^n)$ interage com um oráculo de encriptação $Enc_k(\cdot)$ e então produz m_0 e m_1 de mesmo tamanho
  - $b \leftarrow \{0,1\}$, $c \leftarrow Enc_k(m_b)$ e passa c para A
  - A continua a interagir com $Enc_k(\cdot)$
  - A produz b'; A é bem sucedido se $b = b'$, e experimento produz 1 neste caso

CPA-security

- Π é seguro contra ataques de textos em claro escolhidos se para todo atacante eficiente TPP A, existe função negligível ϵ tal que

$$P(PrivCPA_{A,\Pi}(n) = 1) \leq 0.5 + \epsilon(n)$$

Impossível?

- Considere o segunte atacante A:
  - Obter $c_0 = Enc_k(m_0)$ e $c_1 = Enc_k(m_1)$ usando ataque de texto em claro escolhido
  - Produzir m_0 e m_1; obter texto cifrado c
  - Se $c = c_0$ produz 0; se $c = c_1$ produz 1
  - A é bem sucedido com probabilidade 1 (?)
- Esse ataque só funciona se encriptação for determinística!
- Moral da história: usar encriptação aleatória!

Encriptação aleatória

- Problema sério se um atacante sabe quando uma mensagem é encriptada duas vezes
- Próximas aulas: primitivas de funções pseudo-aleatórias para construir encriptação segura contra CPA

Funções pseudo-aleatórias e cifras de bloco

- Informalmente, função pseudo-aleatória que parece uma função aleatória

Função aleatória

- $Func_n$ = todas as função mapeando $\{0,1\}^n$ para $\{0,1\}^n$
- Tamanho de $Func_n$?
  - Possível representar uma função em $Func_n$ usando $n \cdot 2^n$ bits
  - Exemplo: se $n = 2$, cada função tem 2^2 elementos para serem mapeados e cada elemento tem 2 bits

$$\cdots \begin{array}{|c|c|c|} \hline 00 & 10 & 11 \\ \hline 01 & 11 & 11 \\ \hline 01 & 00 & 10 \\ \hline 11 & 01 & 01 \\ \hline \end{array} \cdots$$

  - Como cada bit que define uma função tem 2 possibilidades $\{0,1\}$ então o número de possíveis funções é:
    $\Rightarrow |Func_n| = 2^{n \cdot 2^n}$

Função aleatória

- Função uniforme: escolha de $f \in Func_n$ conforme distribuição de probabilidades uniforme
- De modo equivalente para cada $x \in \{0,1\}^n$, escolher $f(x)$ uniformemente em $\{0,1\}^n$
  - Preencher a tabela da função com valores uniformes
  - Pode também pensar como sendo em tempo de execução

Funções pseudo-aleatórias

- Informalmente, a função pseudo-aleatória parece ser uma função aleatória
- Como na nossa discussão sobre geradores de números pseudo-aleatórios, não faz sentido falar sobre qualquer função fixa como sendo pseudo-aleatória
  - Em vez disso, consideraremos em funções pseudo-aleatórias chaveadas

Funções aleatórias chaveadas

- Seja $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ uma função eficientemente computável
  - Definir $F_k(x) = F(k,x)$
  - A primeira entrada é a chave
- Usar F que preserva comprimento $F(k,x)$, ou seja,

$$|F(k,x)| = |k| = |x|$$

- Escolher uma chave uniforme $k \in \{0,1\}^n$ é equivalente a escolher a função

$$F_k : \{0,1\}^n \to \{0,1\}^n$$

  - Ou seja, F define uma distribuição sobre funções em $Func_n$

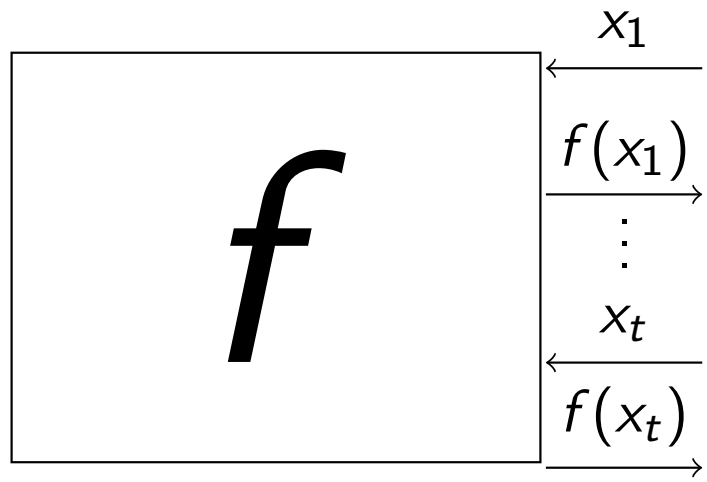
Funções pseudo-aleatórias (FPA)

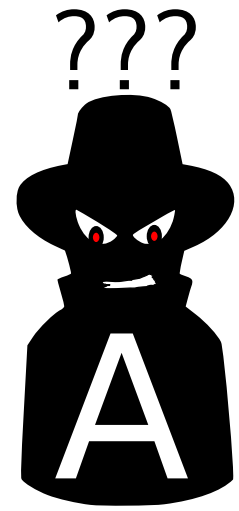
- F é uma função pseudo-aleatória se F_k, para uma chave uniforme $k \in \{0,1\}^n$, é indiscernível de uma função uniforme $f \in Func_n$
- Formalmente, para todo D de tempo polinomial:

$$|P_{k \leftarrow \{0,1\}^n}(D^{F_k(\cdot)} = 1) - P_{f \leftarrow Func_n}(D^{f(\cdot)} = 1)| \leq \epsilon(n)$$

$f \in Func_n$ escolhido de maneira uniforme aleatória

Mundo 0

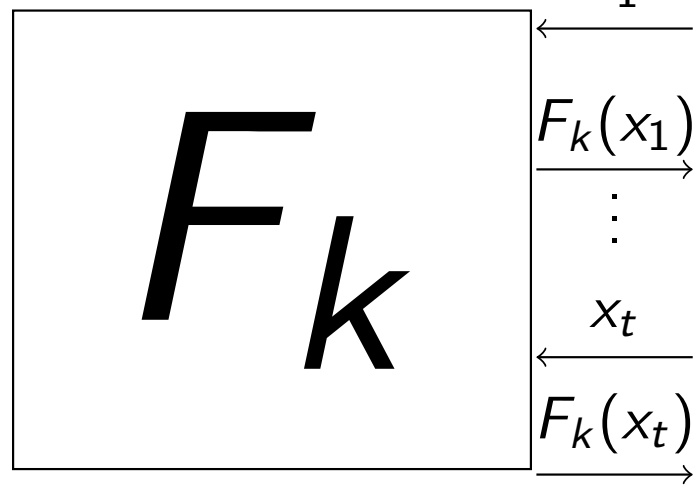




tempo poly

Mundo 1

$k \in \{0,1\}^n$ escolhido de maneira uniforme aleatória



Funções pseudo-aleatórias vs. Geradores pseudo-aleatórios

- Uma FPA F imediatamente implica existência de um GPA G
  - Definir $G(k) = F_k(0 \ldots 0)|F_k(0 \ldots 1)$
  - Ou $G(k) = F_k(0)|F_k(1)|F_k(2)|\ldots$
- Uma FPA pode ser vista como um GPA com acesso aleatório para saídas exponencialmente longas
  - $F_k \Leftrightarrow F_k(0 \ldots 0)| \ldots |F_k(1 \ldots 1)$

Permutações pseudo-aleatórias

- Seja F uma função chaveada que preserva comprimento
- F é uma função de permutação chaveada se
  - F_k é uma bijeção para todo k
  - F_k^{-1} é eficientemente computável tal que $F_k^{-1}(F_k(x)) = x$
- F é uma permutação pseudo-aleatória se F_k, para chave uniforme $k \in \{0,1\}^n$ é indistinguível de uma permutação uniforme $f \in Perm_n$

Cifras de bloco

- Cifras de bloco são construções práticas de permutações pseudo-aleatórias
- $F : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$
  - n é comprimento da chave
  - m é o comprimento do bloco
- Difícil diferenciar F_k de uniforme $f \in Perm_m$ mesmo para atacantes em tempo $\approx 2^n$

AES (2002)

- Advanced Encryption Standard (AES) ou Rijndael
  - Padronizado por NIST em 2000 basedo em uma competição pública mundial que durou 3 anos
  - Tamanho do bloco = 128 bits
  - Tamanho da chave = 128, 192 ou 256 bits
- Padrão mais usado atualmente

Nota sobre cifras de blocos

- Para n grande suficiente, uma permutação aleatória é indiscernível de uma função aleatórias
- Então cifras de blocos são boas FPA também