Cifra de fluxo: chave de uso único
One Time Pad

Prof. Avelino Francisco Zorzo
Faculdade de Informática - PUCRS

Cifras de fluxo

- Como funciona: cifrar caracteres individuais, um de cada vez.

Cifras de fluxo

Def: uma **cifra** definida sobre (K,M,C)
é um par de algoritmos "eficientes" (***E***, ***D***)
onde

E: KxM → C e ***D***: KxC → M
de forma que

Equação de consistência

$$\forall m \in M, k \in K : D(k, E(k,m)) = m$$

- ***E*** é frequentemente aleatorizada.
- ***D*** é sempre determinística.

One Time Pad (Vernam 1917)

- **Cifra de uso único** ou **chave de uso único**
- Primeiro exemplo de cifra "segura"
- M=C={0,1}^{n}
- K={0,1}^{n}
- Chave = uma sequência de bits aleatórios do mesmo tamanho que a mensagem.

One Time Pad

- c := E(k,m) = k ⊕ m
- m := D(k,c) = k ⊕ c

msg:	0	1	1	0	1	1	1
chave:		1	0	1	1	0	1 ⊕
	0						
CT:		1	1	0	1	1	0 1

- D(k,E(k,m)) = D(k,k⊕ m) = k⊕ (k⊕ m) = (k⊕ k) ⊕ m = m

One Time Pad

- Dado a mensagem *m* e seu texto cifrado *c*.
- Tem como computar a chave a partir de *m* e *c?*
  a. Não, eu não consigo computar a chave.
  b. Sim, a chave é k = m ⊕ c.
  c. Eu só consigo computar a metade dos bits da chave.
  d. Sim, a chave é k = m ⊕ m.

One Time Pad

- Cifrar e decifrar é muito rápido!!
  - … mas precisa chave longa
  - … tão longa quanto o texto claro
- OTP é segura?
- O que é uma cifra segura?

Sigilo da cifra *one time pad*

- Por muitos anos, acreditava-se que OTP era "inquebrável", mas não existia prova.
- Até 30 anos mais tarde quando Shannon definiu o conceito de "sigilo prfeito" ("*perfect secrecy*") (1949)

O que é uma cifra segura?

- Habilidade do atacante: ataque só com texto cifrado
- Possíveis requisitos de segurança:
  - Tentativa #1: atacante não pode recuperar a chave
  - Tentativa #2: atacante não pode recuperar o texto claro
- Ideia de Shannon:
  Texto cifrado não pode revelar qualquer informação sobre o texto claro.

Sigilo perfeito

- Def: uma cifra (***E,D***) sobre (K,M,C) tem um sigilo perfeito se

$$\forall m_0, m_1 \in M\left(len(m_0) = len(m_1)\right) \wedge \forall c \in C$$

Prob[E(k,m_0)=c] = Prob[E(k,m1)=c]

onde k é uma distribuição uniforme em K

Sigilo perfeito

- Dado um texto cifrado, um adversário não consegue distinguir se a mensagem é m_0 ou m_1 para todas m_0 ou m_1.
- O adversário mais poderoso não aprende algo sobre o texto claro a partir do texto cifrado..
- Não existe ataque só com o texto cifrado.

Sigilo perfeito

- Seja m ∈ M e c ∈ C.
- Quantas chaves OTP mapeiam m para c?
  a. Nenhuma
  b. 1
  c. 2
  d. Depende de m

OTP não é prática

- Teorema: Sigilo perfeito requer $|K| \geq |M|$
- Tamanho da chave deve ser pelo menos tão grande quanto o tamanho da mensagem.
- Por isto éla é chamada de *ONE TIME pad*
- OTP tem sigilo perfeito mas não é prática.

Segundo trabalho

- Dados TCs (em hex) criptografados com OTP:
  - 2d0f1004 1 d4 4 0a 4 60 b 0 a0 6 0f 0 20 8 0c 1 c0 f 12 4 51 3 19 1 15 6 02 1 40 1 0c 1 1 1e 1 50 a 0e 5 41 5 00 0 2020c134 6 05 1 d0 0 19 0 a 08 0 31 a 05 1 00 a 4e 0 f0 3 41 1 90 d 19 1 70 4 04 1 d4 7 0 f1 5 44 0 c0 0 4c 0 c1 0 430b5744 0 20 5 08 4 d0 5 0 e0 8 48 0 b4 6 4b 1 c1 4 53 1 c4 1 4d
  - 27091515 5 31 4 04 1 10 d 1 11 0 12 0 b5 a 19 1 d0 1 03 1 70 1 16 0 70 f 43 1 c1 2 08 1 1 03 0 75 8 19 1 b0 2 09 0 50204470 7 03 1 b0 6 19 4 3 12 0 c0 a 4c 1 30 e 0f 0 f0 b 15 1 11 0 1e 4 40 3 11 1 70 a 4 61 2 0c 0 41 0 0f 0 a1 2 0b031410 0 11 2 0e 4 3
  - 29141f11 0 70 b 0c 1 40 9 1 31 e 1e 4 71 9 17 1 71 4 03 1 71 c 04 5 50 2 0b 1 55 7 19 1 1 02 1 e1 d 14 0 01 f 0e 0 24c0c014 6 15 0 60 6 1e 1 7 5c 4 41 b 0d 0 80 b 00 0 14 5 15 0 61 d 19 1 04 5 05 0 a0 8 0 b4 6 13 0 95 5 1e 0 64 2 0a124601 1 c0 3 09 1 91 7 4 21 0 07 4 60 1 03 1 61 4 16 5 11 9 17 4 c1 1 1d 5 30 8 02 1 4 13 0 71 c 48
  - 3e0e0341 0 00 1 08 1 40 d 0 00 f 47 0 a0 f 0b 0 d5 7 14 0 00 1 1e 1 11 3 43 1 51 9 1d 0 a 1f 1 11 4 0e 5 41 9 0f 4 c180b024 6 0a 1 10 a 41 4 3 08 0 b1 b 4c 1 70 a 0b 4 60 6 08 0 40 0 0f 1 64 5 02 1 40 0 0 91 4 0d 1 55 8 01 4 d
  - 3e0e0341 1 70 1 18 0 f0 f 0 d5 6 08 0 15 a 19 5 90 4 1f 1 60 6 12 1 85 6 10 1 81 8 1c 0 f 09 5 41 6 18 0 05 6 13 0 91d160e1 4 04 5 40 0 08 0 0 14 0 10 c 15 4 30 d 08 4 61 1 09 1 14 8 19 1 d1 6 17 1 d0 a 4 8
  - 29141f11 0 70 5 05 0 70 4 1 a0 5 0e 1 45 a 2c 1 11 2 46 0 40 0 03 5 51 7 0d 1 45 7 1a 0 0 04 1 11 6 14 1 15 6 0e 0 a4c02090 7 0d 0 d0 9 04 0 d 01 4 41 8 09 0 20 9 00 0 31 6 12 1 11 b 4a 0 b0 3 43 1 b0 e 1 60 e 01 1 31 0 0d 0 f0 5 0c140f10 0 c0 7 09 4 3
  - 29141f11 0 70 b 0c 1 40 9 1 31 e 1e 4 71 3 0b 5 90 3 1f 1 51 b 14 1 41 a 0f 0 95 7 0b 1 a 1d 1 50 b 04 1 11 2 4d 4 c020c134 6 11 1 11 d 08 1 7 14 0 51 b 09 0 74 c
  - 4772656d 6 96 f 20 7 76 1 7 32 0 74 6 86 5 20 6 66 9 72 7 37 4 20 7 46 5 61 6 d2 0 69 6 e 20 5 26 9 6f 2 04 7 72 6 16e64652 0 64 6 f2 0 53 7 5 6c 2 07 4 6f 2 06 2 65 6 36 f 6d 6 52 0 43 6 86 1 6d 7 06 9 6 f6 e 20 6 f6 6 20 5 36 f 75746820 4 16 d 65 7 26 9 6 36 1 2c 2 04 9 6e 7 46 5 72 2 07 7 61 7 32 0 74 6 86 5 20 7 3 65 6 36 f 6e 6 42 e
- Quais são estas mensagens?