Troca de Chaves

Faculdade de Informática- PUCRS
Prof. Avelino Francisco Zorzo

Sumário

- Troca de chave de maneira simétrica
  - Quebra-cabeças (*puzzle*) de Merkle
- Troca de chave de maneira assimétrica
  - Diffie-Hellman

Quebra-cabeças de Merkle (*Merkle puzzles*)

Troca de chave

Meta: Alice e Bob querem compartilhar uma chave, que fique desconhecido por um espião.

- Agora: segurança contra espionagem (sem alteração)

Espião??

Isto pode ser feito através de criptografia simétrica?

Quebra-cabeças de Merkle (1974)

Resposta: sim, mas muito ineficiente.

Forma: quebra-cabeças (*puzzle*).

- Problemas resolvidos com algum esforço.
- Exemplo: cifra simétrica E(k,m), $k \in \{0,1\}^{128}$
  - ***puzzle*(P) = E(P, "mensagem")** onde

    $P = 0^{96} \,||\, b_1 \ldots b_{32}$
  - **Meta**: encontrar P tentando as 2^{32} possibilidades

Quebra-cabeças de Merkle

Alice: prepara 2^{32} quebra-cabeças

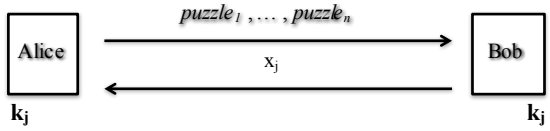
- Para i=1, …, 2^{32} escolha aleatoriamente $P_i \in \{0,1\}^{32}$ e $x_i, k_i \in \{0,1\}^{128}$
- $puzzle_i \leftarrow E(0^{96} \,||\, P_i$, "***Puzzle* # x_i" $||$ $k_i)$
- Envie $puzzle_1$, … , $puzzle_{232}$ para o Bob

Bob: escolhe aleatoriamente um $puzzle_j$ e resolva ele.

- Obtenha (x_j, k_j).
- Envie x_j para Alice

Alice: procure o quebra-cabeças com x_j. use k_j como chave compartilhada

Quebra-cabeças de Merkle



Trabalho da Alice: O(n) (preparar n quebra-cabeças)
Trabalho do Bob: O(n) (resolver um quebra-cabeça)

Trabalho do espião: $O(n^2)$ (e.g. 2^{64})

Resultado impossível?

Podemos ter um diferença melhor usando troca de chaves de maneira simétrica?

Resposta: desconhecida

Mas: de maneira geral,

uma diferença quadrática é o melhor possível se tratarmos uma cifra como um oráculo caixa preta

[IR'89, BM'09]

Diffie-Hellman

O Protocolo Diffie-Hellman

Escolha um grande número primo p (e.g. 600 digitos)
Escolha um g que gera Z_p^*
p e g são conhecidos por todos.

Alice **Bob**

Escolha um número a em {1,…,p-1} | Escolha um número **b** em {1,…,p-1}

$A \leftarrow g^a \bmod p$

$B \leftarrow g^b \bmod p$

$\mathbf{B^a} \pmod p = (g^b)^a = \mathbf{k_{AB}} = \mathbf{g^{ab}} \pmod p = (g^a)^b = \mathbf{A^b} \pmod p$

Segurança

Espião vê: p, g, $A=g^a \pmod p$,
e $B=g^b \pmod p$

Consegue computar $g^{ab} \pmod p$??

Mais genericamente:
defina $DH_g(g^a, g^b) = g^{ab} \pmod p$

Quão difícil é calcular a função DH mod p?