Diffie-Hellman

Acordo de Chave Compartilhada

Estabelecendo uma Chave Compartilhada

- Diffie-Hellman, 1976
- Resolve problema de **distribuição de chave simétrica**, criando uma **chave compartilhada**.
- É preciso **encriptar uma chave simétrica de sessão** para criar o envelope digital.

Acordo de chave Diffie-Hellman

- Usa-se para tal, a **criptografia de chave pública**, para criar o **envelope digital**.

- É utilizada a **tecnologia de chave pública** para gerar a chave de sessão simétrica.

Acordo de Chave Diffie-Hellman

- Alice e Bob têm que concordar sobre dois grandes números:

  - **p** (um número primo)
  - **g** (um número pseudo-aleatório)

  onde **(p-1)/2** é também um primo e certas condições se aplicam a **g**.

Acordo de Diffie-Hellman

- **p** é um número primo gerado a partir de um PRNG (**gerador de números pseudoaleatórios)**, sendo verificado se é primo pelo Teste de Fermat.

- **g** é um número gerado por um PRNG, que se relaciona bem com o valor de **p**.

Acordo de Diffie-Hellman

- Estes números podem ser **públicos**, assim, **qualquer uma** das partes pode escolher **p** e **g** e dizer ao outro abertamente.

- Seja Alice gerar, por um PRNG, um número grande (digamos 512 bits), chamado **x.** Ela guarda **x** como **secreto**.

Acordo de Diffie-Hellman

- Alice calcula **$y = g^x \bmod p$** . Alice tem, então, um **expoente privado x**.

- Alice inicia o protocolo do acordo de chave enviando a Bob uma mensagem contendo **(p, g, y)** .

- **y** é um valor transmitido, portanto, público.

Acordo de Diffie-Hellman

- Bob tem agora um número grande **g^x mod p** (512 bits) definindo a tripla **(p, g, g^x mod p)** a qual é transmitida para Bob, como a **chave pública** DH de Alice.

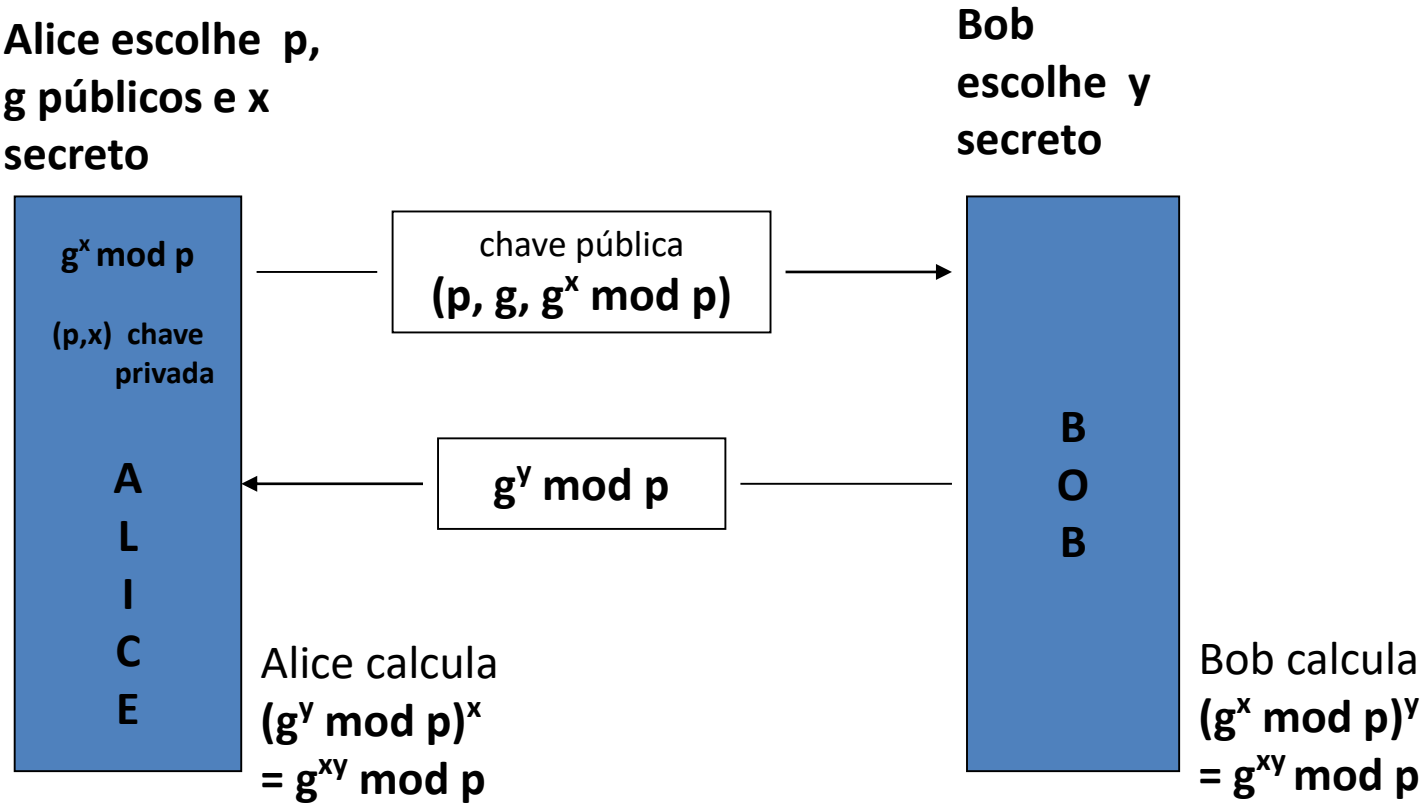
- Bob escolhe um número **y** secreto.

- Bob responde enviando a Alice uma mensagem contendo **(g^y mod p)** .

Acordo de Diffie-Hellman

- Alice calcula **$(g^y \bmod p)^x$**
- Bob calcula **$(g^x \bmod p)^y$**
- Pela lei da aritmética modular, ambos os cálculos resultam em **$g^{xy} \bmod p$** .
- Alice e Bob, agora **compartilham uma chave secreta**: **$g^{xy} \bmod p$**

Acordo de Diffie-Hellman



Acordo de Chaves Diffie-Hellman

- O algoritmo não criptografa os dados.
- Duas partes geram o mesmo segredo e então utilizam para ser uma chave de sessão para uso em um algoritmo simétrico, ou seja, **g^{xy} mod p)** .
- Este procedimento é chamado **Acordo de Chave**.

O acordo de Diffie-Hellman

- **Dificuldade de quebra do algoritmo**:

  Trudy conhece **g** e **p**. Se ela pudesse descobrir **x** e **y**, ela descobriria a chave secreta.

  O problema é que dado (**g^x mod p**) e (**g^y mod p**), ela **não pode descobrir x** nem **y**.

  Nenhum algoritmo é conhecido para computar o **módulo de logaritmo discreto** de um **número primo muito grande.**