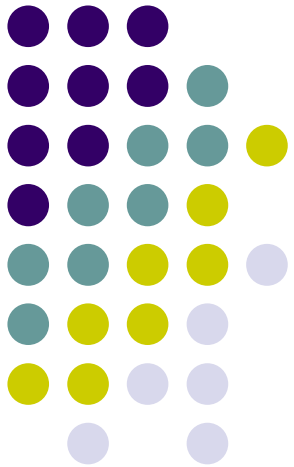
Universidade Federal de São Paulo – UNIFESP

Segurança Computacional

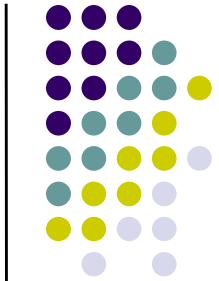
Aula 05: Autenticação



Prof.
Valério Rosset

Autenticação

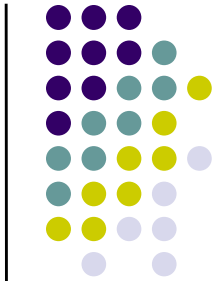
Definição



- A autenticação é o processo onde se identifica se uma informação é autêntica.
- Pode ser usada, por exemplo, para verificar a identidade de um usuário em um sistema computacional ou ainda se uma mensagem enviada por um usuário é legítima e íntegra.
- Geralmente a autenticação utiliza métodos criptográficos para determinar a legitimidade e integridade de informações.

Autenticação

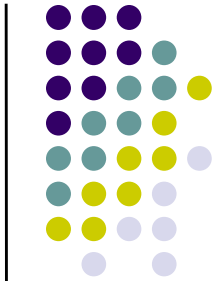
Métodos – Autenticação de usuário



- Os métodos de autenticação de usuário são baseados nos princípios do conhecimento e posse.
  - A autenticação por conhecimento tem por base a necessidade de um usuário conhecer alguma coisa, por exemplo, uma senha (password).
  - A autenticação por posse tem por base identificar um usuário através de uma coisa que ele possua, por exemplo, um cartão de identificação (token ou smartcard), um certificado digital ou dados biométricos.

Autenticação

Mecanismos de Autenticação - Usuário

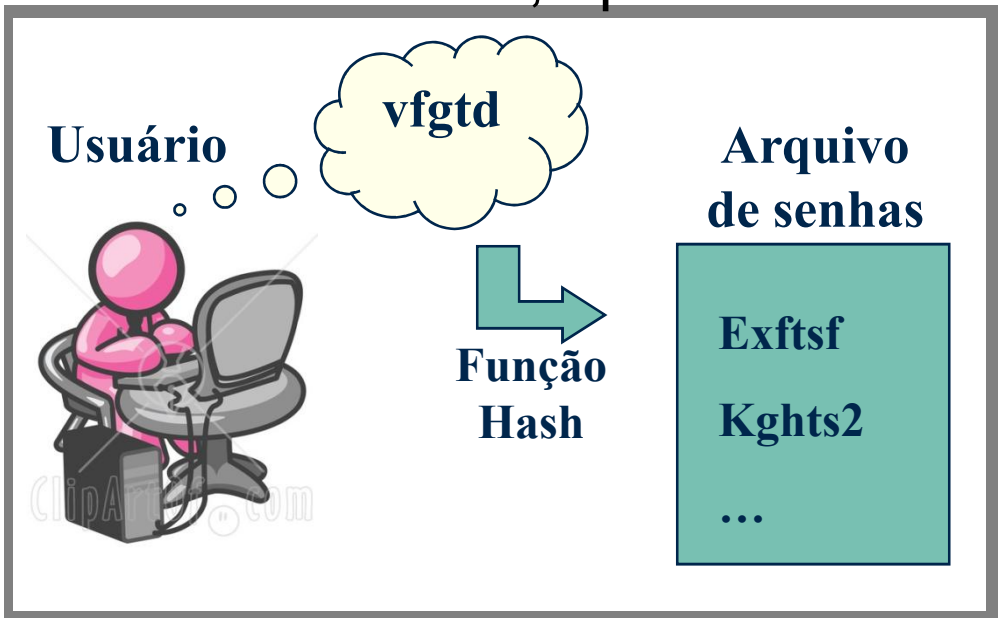


- Autenticação de usuário por senha (*password authentication*)
  - Exemplo simples de mecanismo *Challenge Response.*
    - Idéia:
      - Usuário tem uma senha.
      - O sistema verifica a senha para autenticar o usuário.

Autenticação

Mecanismos de Autenticação - Usuário

- ***Autenticação por senha (funcionamento):***
  - Usuário cria uma senha.
  - Senha do usuário é armazenada como h(senha).
  - Nenhuma senha é armazenada em disco, apenas o hash.

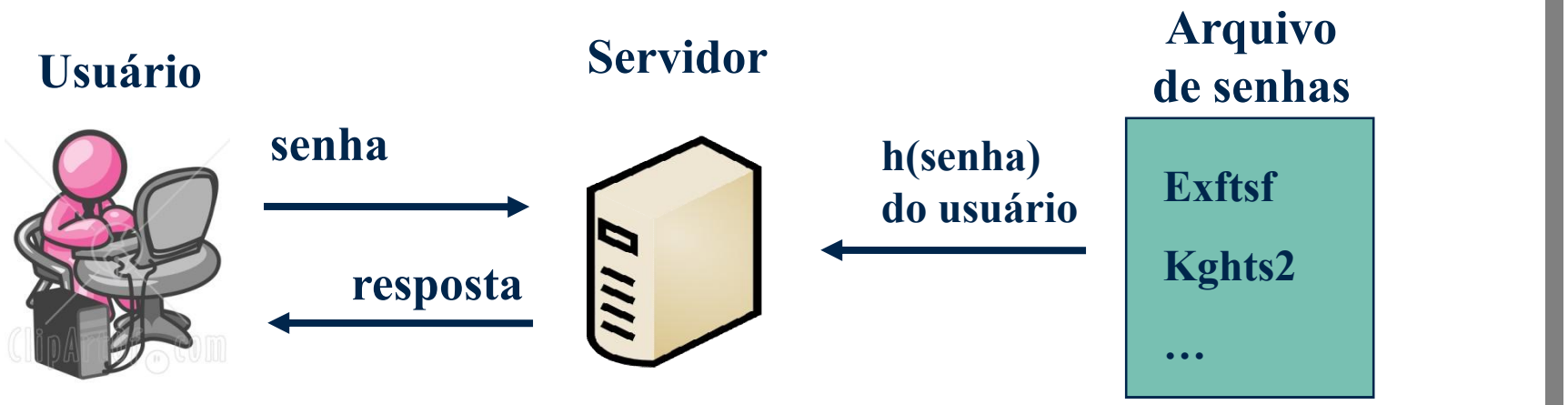


- **Dada uma h(senha), é muito difícil adivinhar a senha.**
- **Melhor Algoritmo seria pelo método o de tentativa e erro (Força Bruta).**

Autenticação

Mecanismos de Autenticação

- ***Autenticação por senha (funcionamento):***
  - Quando o usuário entra com a senha
    - **O Servidor computa a h(senha)**
    - **Compara com o valor armazenado no arquivo de senhas**



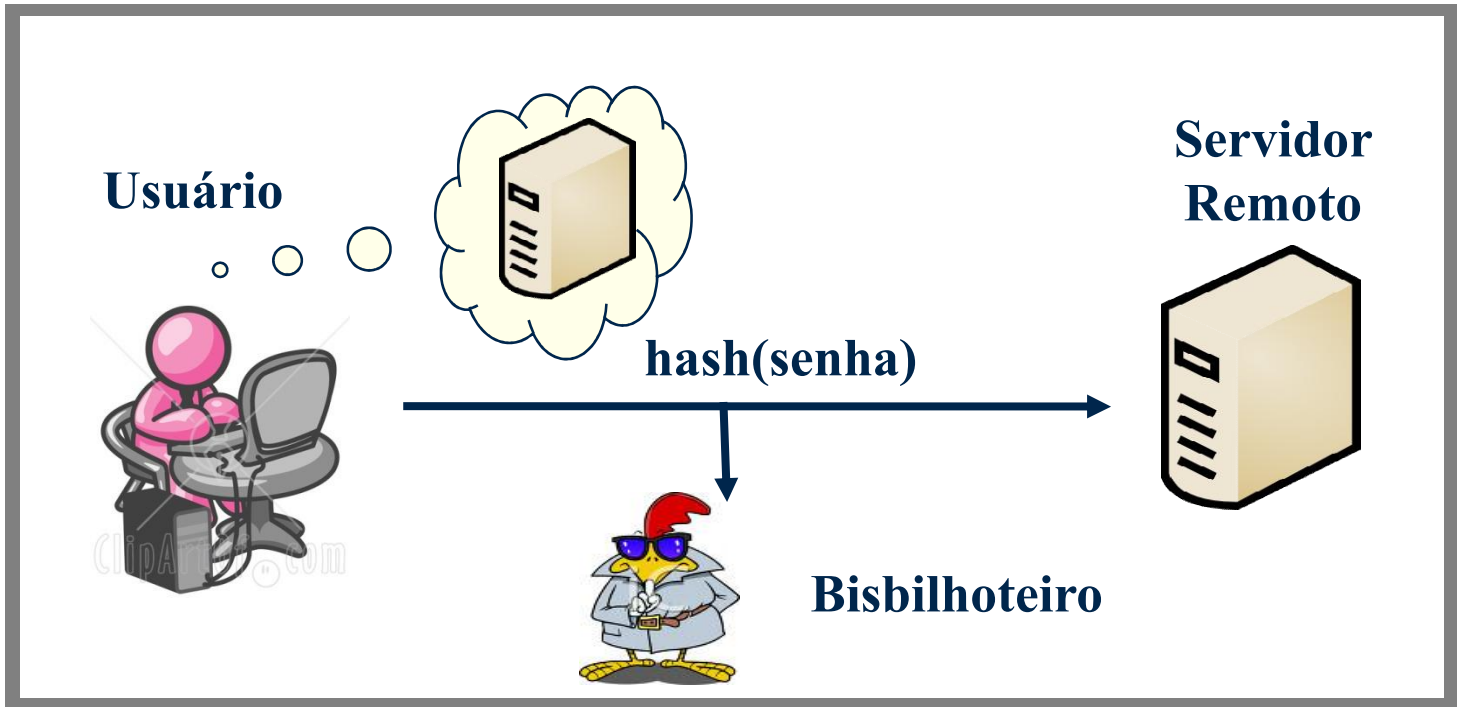
Funciona bem quando a autenticação é local

Autenticação

Mecanismos de Autenticação

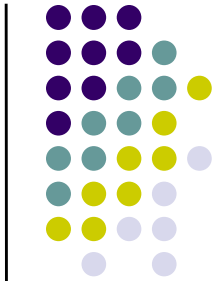
- ***Autenticação Remota por senha***

Problema: sujeita a ataques, como interceptação, *man-in-the-middle e phishing*.



Autenticação

Mecanismos de Autenticação

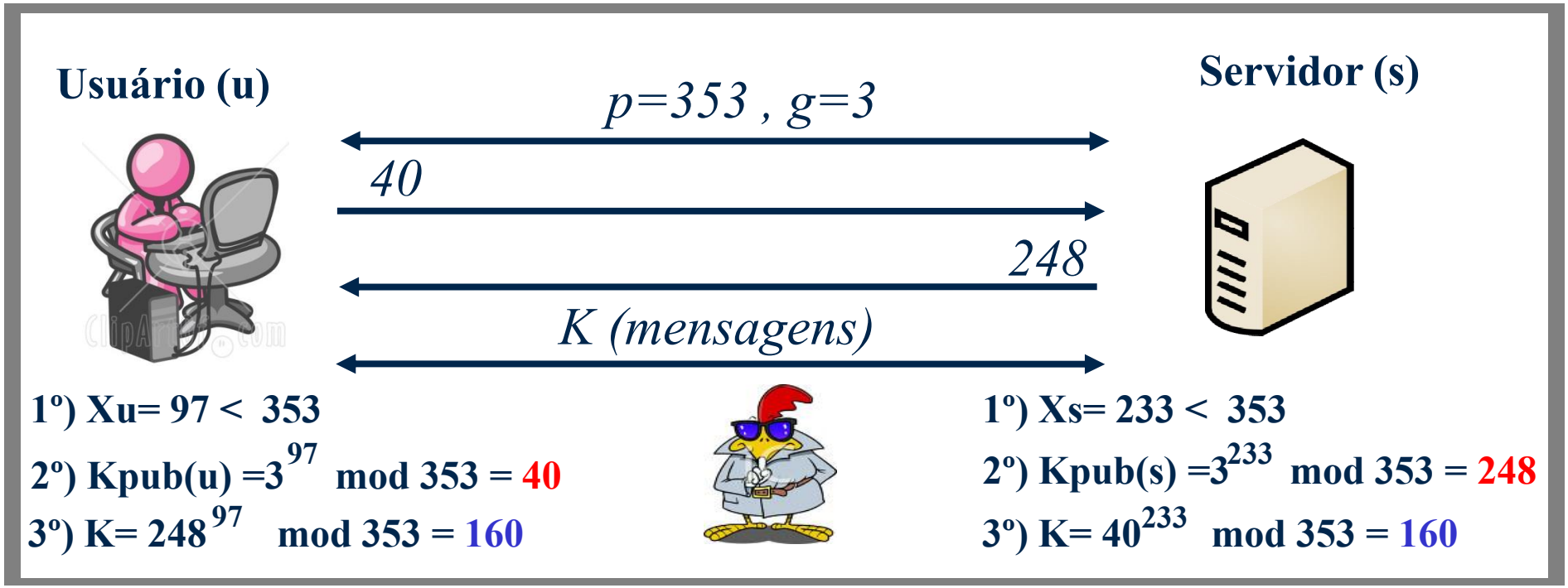


- ***Solução*** : Antes de começar uma comunicação os dois lados precisam estabelecer um canal seguro (por ex. através de SSL). Para isso utilizam um algoritmo para troca de uma chave secreta (sessão).
- Algoritmo de troca de chaves de *Diffie-Hellman*:
  - Ambos os lados acordam os valores de um número primo *p* e sua raiz primitiva *g*.
  - Cada um escolhe um primo X < g como seu segredo e Xu calculam:
    - Kpub(u) = g^{Xu} *mod p* → K = $Kpub(s)^{Xu}$ *mod p*
    - Kpub(s) = g^{Xs} *mod p* → K = $Kpub(u)^{Xs}$ *mod p*

Autenticação

Mecanismos de Autenticação

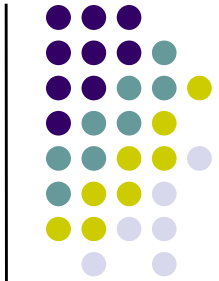
- Exemplo: Troca de Chaves Diffie-Hellman



- Problema: resolve o problema de interceptação de mensagem aberta, porém ainda é vulnerável ao ataque man-in-the-middle.

Autenticação

Mecanismos de Autenticação



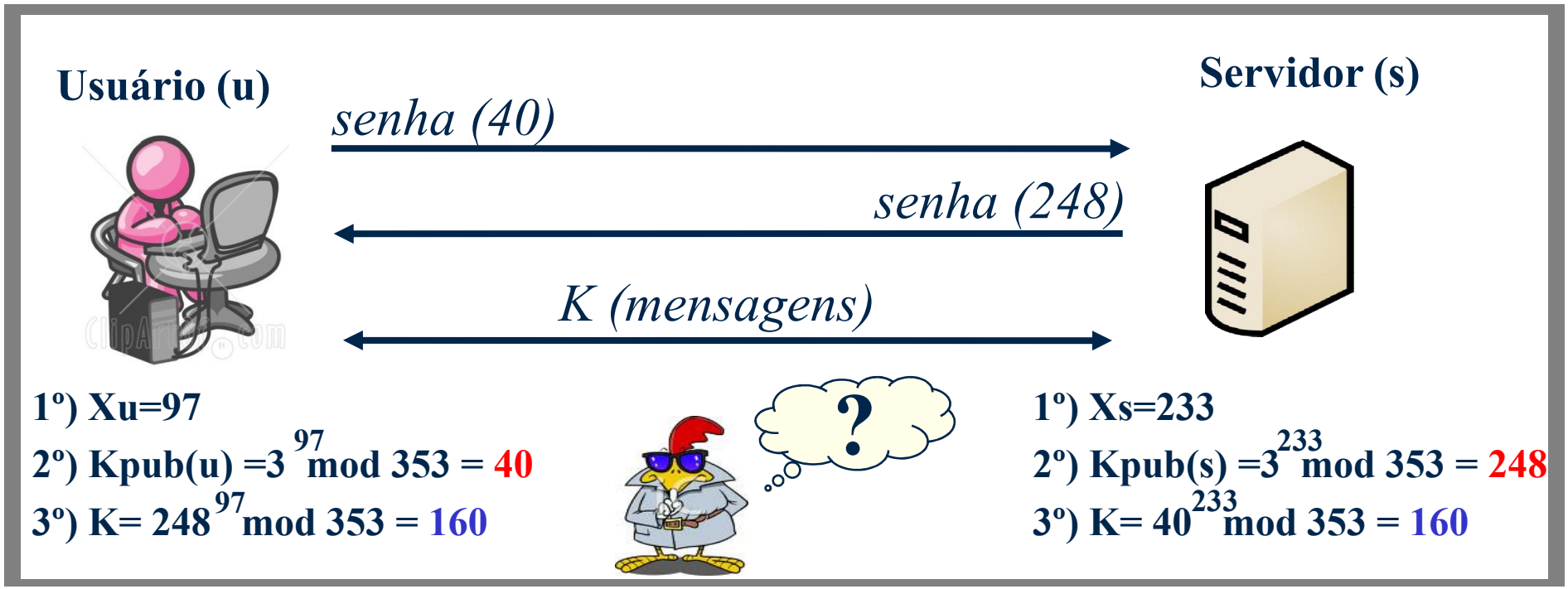
- ***Solução***
  - EKE-DH (Encription Key Exchange – Diffie-Hellman)
  - Baseia-se no algoritmo de troca de chaves de Diffie-Hellman (*vulnerável ao man-in-the-middle*).
  - A diferença está em utilizar a um elemento de conhecimento mútuo (*como a senha*) como uma chave para cifrar o resultado do cálculo da chave pública de cada participante.
  - Assim temos :

$$senha\ (g^{xu} \bmod p)$$

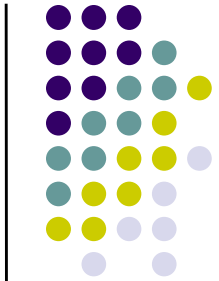
Autenticação

Mecanismos de Autenticação

- Solução Final:
  - Exemplo de EKE-DH



Atividade



Implementar a Troca de Chaves Diffie - Hellman na aplicação de CHAT Seguro.