SSH

- SSH(Secure Shell) é um padrão para comunicação e acesso remoto a máquinas Linux de forma segura, ou seja, utilizando criptografia.
- Ele permite administrar máquinas remotamente, executando inclusive aplicativos gráficos e permite transferir arquivos de várias formas diferentes.

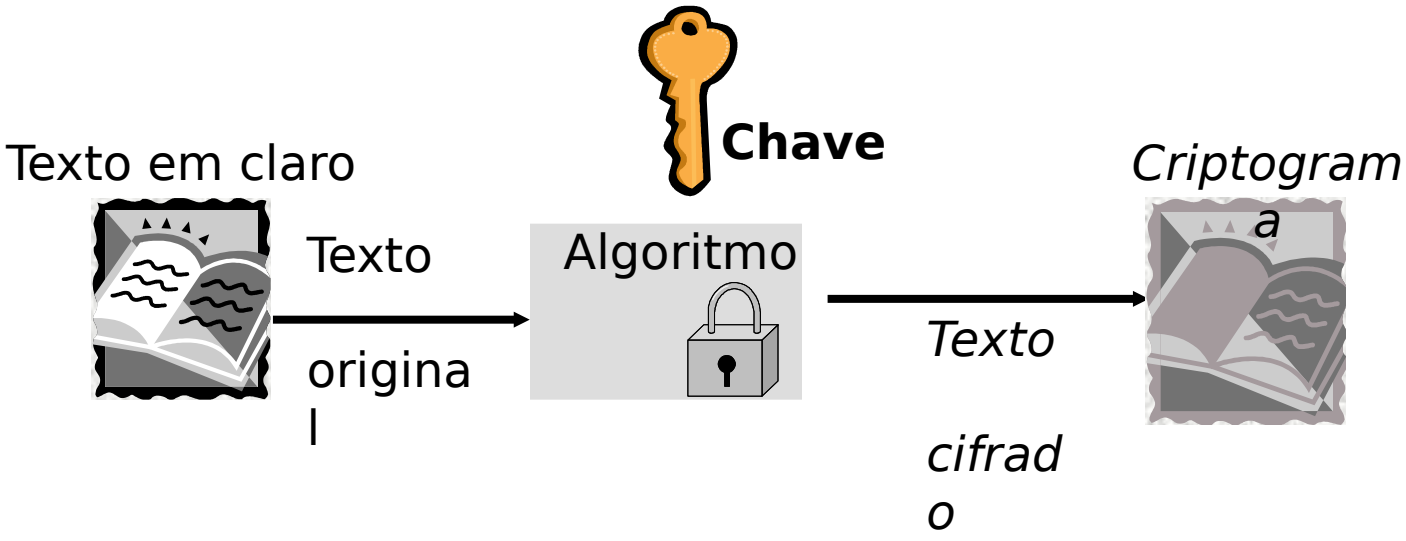
SSH

- *Criado pela empresa SSH Communications Security em 1995, com implementação livre (OpenSSH)*
- *Plataforma POSIX (Unix, Linux, etc)*
- *http://www.ssh.fi*

SSH

- *Arquitetura cliente e servidor - TCP/IP*
- *Autenticação segura*
- *Transferência segura de arquivos*
- *Encapsula outros protocolos*

SSH



- *A troca de mensagens é criptografada (supre o telnet)*
- *Chave pública e privada (assimétricas)*

SSH

- Proteção contra IP spoofing (quando um computador se finge de outro)
- Proteção contra DNS spoofing (ataque de sobreposição de servidores DNS), usando chave pública
- Troca de chaves usando algorítmo RSA (atualizadas de tempo em tempo)

SSH

- O SSH é dividido em dois módulos.
  - **sshd** é o módulo servidor
  - **ssh** é o módulo cliente

- A configuração do servidor, independentemente da distribuição usada, vai no arquivo "**/etc/ssh/sshd_config**", enquanto a configuração do cliente vai no "**/etc/ssh/ssh_config**".

Configuração

- **Para se logar em um servidor SSH, utilizar o comando**
  - ssh ip_servidor

Configuração

- **Para se logar como um usuário específico ao invés do usuário padrão use o comando:**

ssh usuário@servidor

ou então

ssh -l usuário servidor

ssh -l usuário –p porta servidor