UNIVERSIDADE PORTUCALENSE

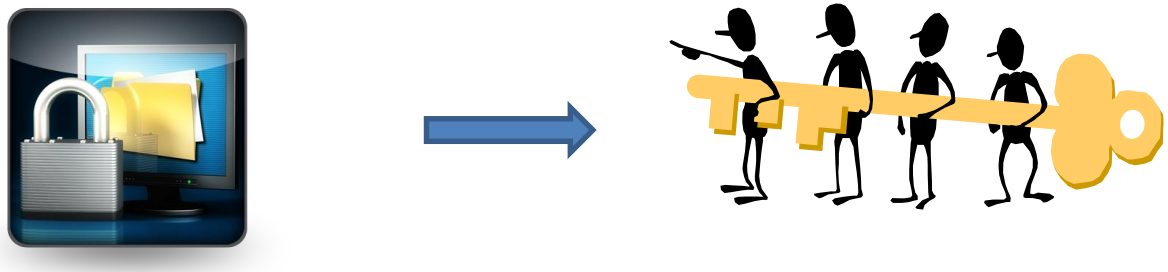
Criptografia

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA e SEGURANÇA DE REDES

- Nas redes locais ou Internet é muito fácil enganar uma pessoa com quem se comunica; resolver este problema é muito importante para efetuar uma comunicação confiável.



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA e SEGURANÇA DE REDES

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA e SEGURANÇA DE REDES

Objetivo

Garantir que uma mensagem ou informação só será lida e compreendida pelos destinatários autorizados

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA

Princípios

- A criptografia é sobre a troca de mensagens
- A chave do sucesso é que todas as partes envolvidas numa troca confiem que o sistema irá protegê-los de ameaças e transmitir com precisão a sua mensagem
- CONFIANÇA é essencial
- Algoritmos devem ser públicos e verificáveis
- Temos de ser capazes de estimar o risco de compromisso
- A solução deve ser prático para os utilizadores e impraticável para um invasor quebrar

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA

Princípios

- Criptografia é sempre baseada em algoritmos em que é muito mais fácil de calcular o frente (normal) do que no sentido inverso (ataque).
- O problema do invasor nunca é mais difícil do que tentar todas as chaves possíveis
- Quanto mais material, o atacante tem mais fácil a sua tarefa se torna

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA

Algoritmos: Diffie – Hellman

Alice	*Concordam em* p,g	*Bernardo*
Escolhe um valor aleatório A		Escolhe um valor aleatório B
	$T_A = g^A \bmod p$ →	
	← $T_B = g^B \bmod p$	
Calcula $(T_B)^A$		Calcula $(T_A)^B$

A chave secreta é: $g^{AB} \bmod p$

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA

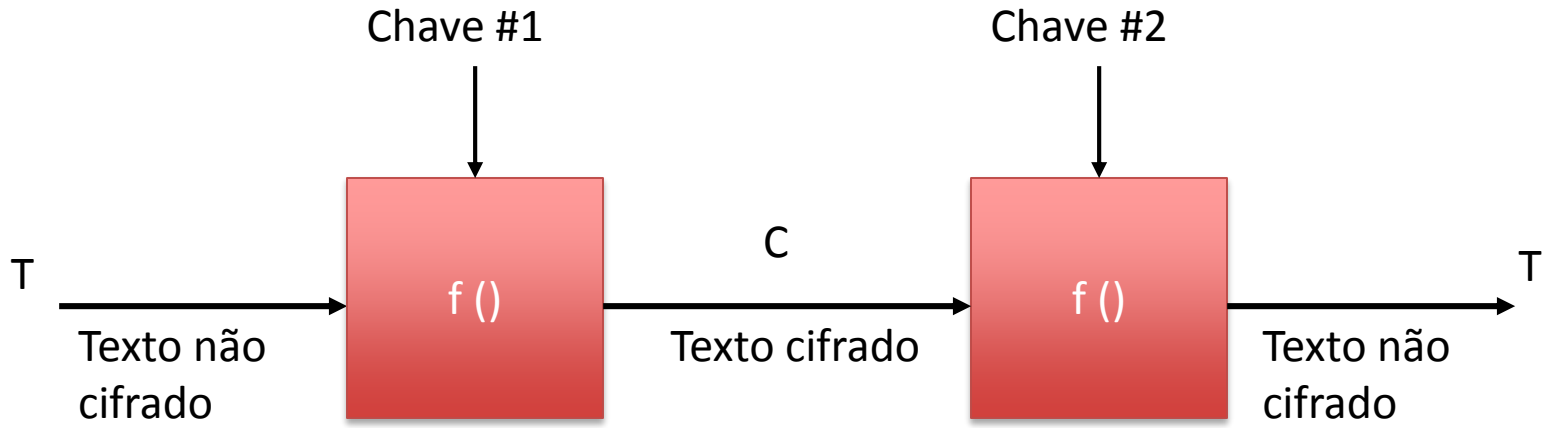
Algoritmos: Diffie – Hellman (problemas)

- Não é um método de encriptação
- Têm que se continuar a utilizar um método de encriptação
- Sujeito ao ataque “man in the middle”
  (Alice pensa que está a falar com o Bernardo mas realmente está a falar com a Teresa)

UNIVERSIDADE PORTUCALENSE

CRIPTOGRAFIA

Algoritmos: RSA (Ronald Rivest, Adi Shamir e Leonard Adleman)



Chave #1 Pode ser uma chave pública ou privada.
Chave #2 É a chave correspondente privada ou pública.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

CRIPTOGRAFIA

UNIVERSIDADE PORTUCALENSE

Algoritmos: RSA (Ronald Rivest, Adi Shamir e Leonard Adleman)

- Rivest, Shamir and **A**delman (1978)
- Posso enviar mensagens que só você pode ler
- Posso verificar que você e só você enviou uma mensagem
- Posso usar uma autoridade confiável para distribuir minha chave pública
  - A autoridade confiável é para seu benefício!

CRIPTOGRAFIA

UNIVERSIDADE PORTUCALENSE

Algoritmos: RSA (Ronald Rivest, Adi Shamir e Leonard Adleman)

- Utiliza a mesma operação para encriptar e desencriptar uma mensagem
- Para encriptar utilizamos a chave “a” e para desencriptar utilizamos a chave “b”
- *a* e *b* são inversas relativamente ao algoritmo escolhido

UNIVERSIDADE PORTUCALENSE

Vantagens e desvantagens da criptografia de chave pública

- Vantagens:
  - Aumento da conveniência e segurança;
  - Fornece assinaturas digitais que não podem ser repudiadas;
- Desvantagens:
  - Mais lento do que o método de chave secreta, mas pode ser usado em conjunto com a chave secreta para o tornar mais eficaz;
  - Pode ser vulnerável à personificação se hackeado.

CRIPTOGRAFIA

MDx (4,5,6) - Message digests

UNIVERSIDADE PORTUCALENSE

- Um “message digest” resumo de mensagem é um algoritmo não-reversível, que reduz uma mensagem a um “hash” resumo de comprimento-fixo;
- Uma alteração no original implica uma mudança no resumo;
- A probabilidade de um sumário novo ser igual ao antigo é de *1*/(tamanho da mensagem)

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

Criptografia de chave privada

UNIVERSIDADE PORTUCALENSE

- A criptografia tradicional de chave privada/secreta/única utiliza uma chave só
- Partilhada pelo emissor e recetor
- Se a chave é divulgada as comunicações ficam comprometidas
- Simétrico, as duas partes são iguais
- Não protege o recetor do remetente forjar uma mensagem e reivindicar que é enviada pelo remetente

Criptografia de chave pública

UNIVERSIDADE PORTUCALENSE

- Utiliza duas chaves (uma chave pública e uma chave privada)
- Assimétrico uma vez que as duas partes não são iguais
- Complementa em vez de substituir a criptografia de chaves privadas

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Criptografia de chave pública

UNIVERSIDADE PORTUCALENSE

- Desenvolvida para resolver dois problemas:
  - **Distribuição de chaves** – como conseguir ter comunicações seguras sem ter que confiar em terceiros
  - **Assinaturas digitais** – como verificar se uma mensagem chega intacta e de um remetente que afirma a ter enviada
- Descoberta devida a Diffie & Hellman da Universidade de Stanford em 1976

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

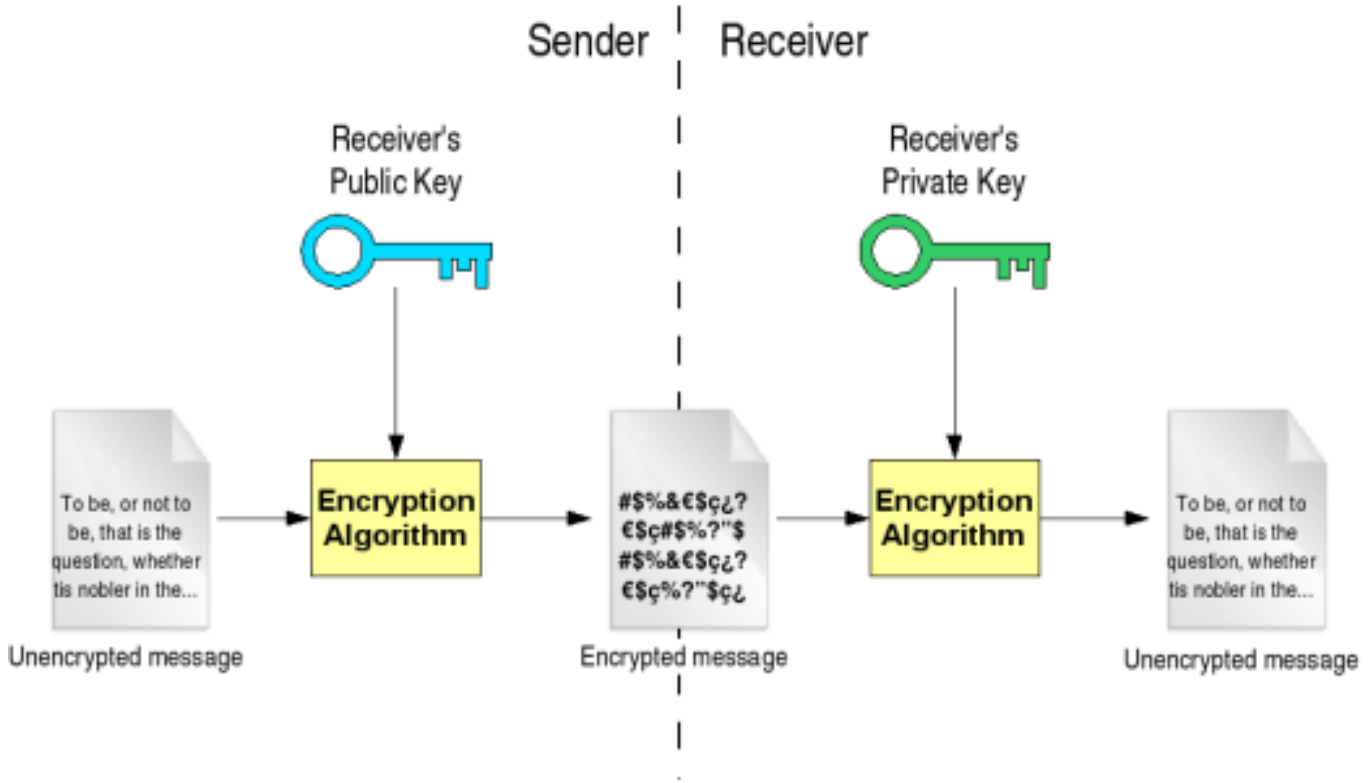
Criptografia de chave pública

UNIVERSIDADE PORTUCALENSE

- **A criptografia chave-pública (public-key)** envolve a utilização de **duas** chaves:
  - Uma chave **pública**, que pode ser conhecida por todas as pessoas e pode ser utilizada para **encriptar mensagens** e **verificar assinaturas**
  - Uma chave **privada** conhecida apenas pelo recetor e é utilizada para **desencriptar mensagens** e **criar assinaturas**
- É **assimétrica** porque:
  - Aqueles que encriptam as mensagens ou assinaturas não podem desencriptar as mensagens nem criar assinaturas.

Criptografia de chave pública

UNIVERSIDADE PORTUCALENSE



DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

Criptografia de chave pública

UNIVERSIDADE PORTUCALENSE

- Algoritmos de chave pública dependem de duas chaves onde:
  - é impraticável encontrar a chave de desencriptação sabendo apenas o algoritmo e a chave de encriptação
  - é computacionalmente fácil encriptar/desencriptar mensagens quando as chaves relevantes são conhecidas

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Software

- http://gpg4win.org/download.html

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA