UNIVERSIDADE PORTUCALENSE

# Autenticação de mensagens

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Comparação
## convencionais vs digitais

Diferenças entre assinaturas convencionais e digitais

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Comparação
## convencionais vs digitais

# Inclusão

- Uma assinatura convencional **está incluída no documento**; é parte do documento.
- Quando assinamos um documento digitalmente, enviamos a assinatura como um **documento separado**.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Comparação
## convencionais vs digitais

# Validação

- Para uma assinatura convencional, quando o destinatário recebe um documento, ele **compara a assinatura** do documento **com a assinatura em arquivo**.
- Para uma assinatura digital, o destinatário recebe a mensagem e a assinatura. O destinatário precisa **aplicar uma técnica de verificação** para a combinação da mensagem e a assinatura para verificar a autenticidade.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Comparação
## convencionais vs digitais

# Relação

- Para uma assinatura convencional, normalmente há uma relação um-para-muitos entre uma assinatura e documentos.
- Para uma assinatura digital, há uma relação um para um entre uma assinatura e uma mensagem.

UNIVERSIDADE PORTUCALENSE

# Comparação
## convencionais vs digitais

# Duplicação

- Na assinatura convencional, uma cópia do documento assinado pode distinguir-se do arquivo original.
- Na assinatura digital, não há nenhum tal distinção a menos que haja um fator de tempo sobre o documento.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# O que é autenticação?

(de mensagens)

- Um procedimento para verificar que as mensagens recebidas provêm de uma fonte e  não foram alteradas.
  - Assinatura digital é uma das técnicas que podem ser utilizadas incluindo medidas de repúdio quer pela origem quer pelo destino.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Ataques à autenticação

- Ataques possíveis
  1. Divulgação
  2. Análise de tráfego
  3. Masquerade
  4. Modificação de conteúdos
  5. Modificação da sequência
  6. Modificação do tempo
  7. Repúdio: repúdio de origem e destino

UNIVERSIDADE PORTUCALENSE

# Funções de autenticação

- 3 tipos de operações criptográficas relacionadas com a autenticação:
  - Encriptação de mensagens
  - Código de autenticação da mensagem (MAC – Message Authentication Code)
  - Função de hash

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

# Encriptação convencional

- A encriptação convencional fornece uma forma fraca de autenticação
- Se Bob poder recuperar uma mensagem cifrada com uma chave compartilhada entre Alice e Bob, Bob sabe que Alice enviou esta mensagem.
- Se a mensagem for alterada, Bob não conseguirá ler a mensagem.

# Técnicas de autenticação
(mensagens)

- As duas técnicas mais comuns de criptografia para autenticação de mensagem são:

- Código de autenticação da mensagem Message authentication code (MAC)
- Função de hash segura

UNIVERSIDADE PORTUCALENSE

# Técnicas de autenticação
(mensagens)

- Message authentication code (MAC): Uma função da mensagem e uma chave secreta que produz um valor de comprimento fixo que serve como o autenticador

- Função de Hash: Uma função que mapeia uma mensagem de qualquer tamanho em um valor de hash de comprimento fixo, que serve como o autenticador

UNIVERSIDADE PORTUCALENSE

# Código de autenticação de mensagens (MACs)

- MAC envolve o uso de uma chave secreta para gerar um pequeno bloco de tamanho fixo de dados.
- MAC é conhecido como uma soma de verificação criptográfica:

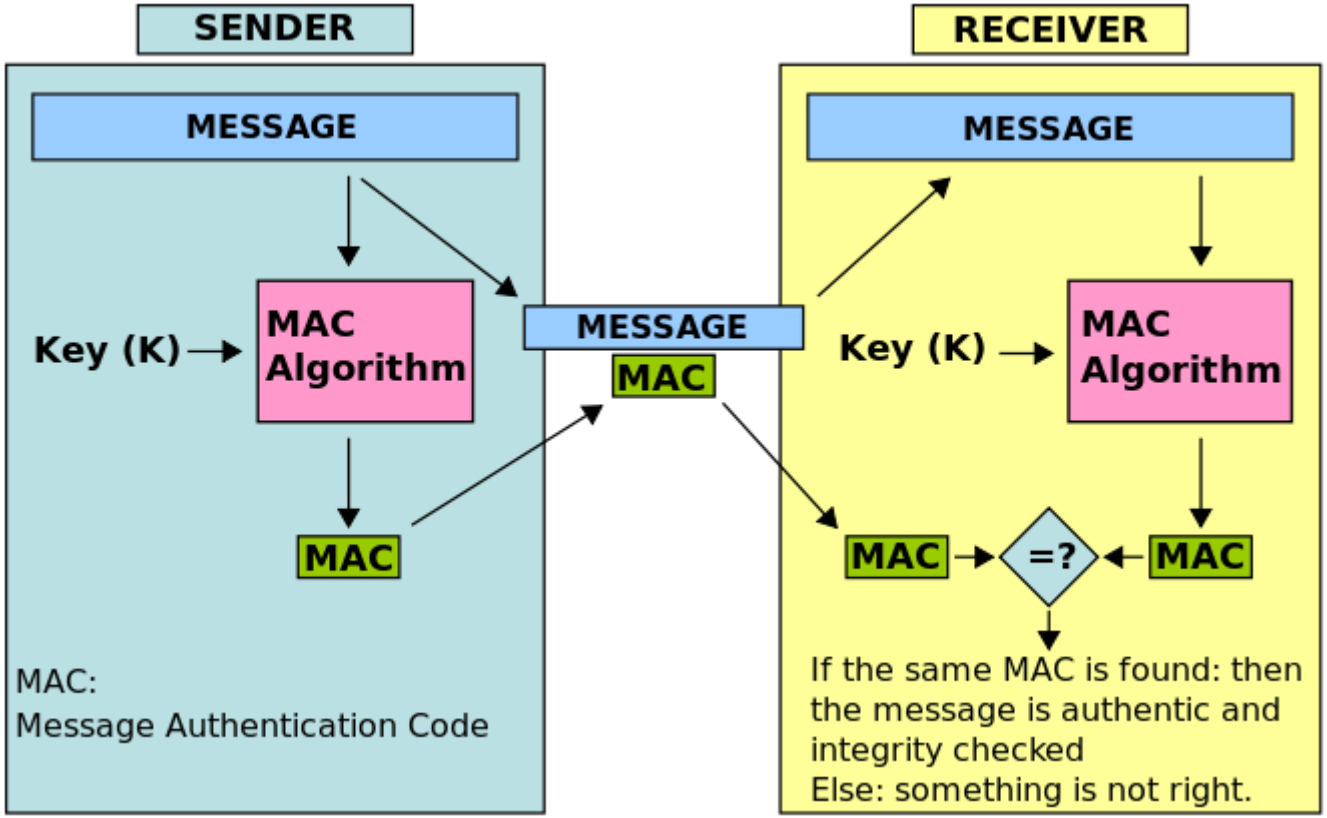
$$MAC = C_K(M)$$

onde:

  - M é uma mensagem de comprimento variável
  - K é uma chave secreta partilhada entre a origem e o destino
  - $C_K$ é o autenticador de comprimento fixo

- MAC é anexada à mensagem e enviado para o recetor.

# Código de autenticação de mensagens (MACs)



UNIVERSIDADE PORTUCALENSE

# Códigos de autenticação de mensagens (MACs)

1. Alice e Bob partilham a chave secreta K1.
2. Alice calcula $MAC_1 = C_{K1}(M)$

   Alice→Bob: $\{M, MAC_1\}$
3. Bob calcula $MAC_2 = C_{K1}(M)$

   Se $MAC_2 = MAC_1$, a mensagem M enviada pela Alice não foi alterada

- Confidencialidade pode ser fornecida por criptografia com outra chave compartilhada.

  Alice→Bob: $\{M, MAC_1\}_{K2}$

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Códigos de autenticação de mensagens (MACs)

- O recetor tem certeza de que a mensagem não foi alterada.
- Se um invasor altera a mensagem, mas não altera o MAC, em seguida, cálculo do recetor do MAC será diferente do MAC recebido.
- Porque se presume que o atacante não conhece a chave secreta, o atacante não pode alterar o MAC para corresponder às alterações na mensagem.

UNIVERSIDADE PORTUCALENSE

# Códigos de autenticação de mensagens (MACs)

- O recetor tem a certeza que a mensagem é do remetente.
- Porque ninguém mais sabe a chave secreta, ninguém mais poderia preparar uma mensagem com um MAC adequado.

UNIVERSIDADE PORTUCALENSE

# Requisitos para o MACs

1. Se alguém observa M e $C_K(M)$, deve ser computacionalmente inviável construir M' tal que $C_K(M') = C_K(M)$.

2. $C_K(M)$ deve ser uniformemente distribuído de tal forma que para mensagens escolhidas aleatoriamente, M e M', a probabilidade de $C_K(M) = C_K(M')$ é $2^{-n}$, onde n é o número de bits no MAC.

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

- Uma variação do o código de autenticação de mensagem é a função de hash unidirecional. Como o código de autenticação de mensagem, uma função de hash aceita uma mensagem de tamanho variável M como entrada e produz um tamanho fixo de saída, referido como um hash do código H(M).
- Ao contrário do MAC, uma função de hash não usa uma chave mas é uma função somente da mensagem de entrada.
- O código de hash é também referido como um valor de hash ou digest da mensagem.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

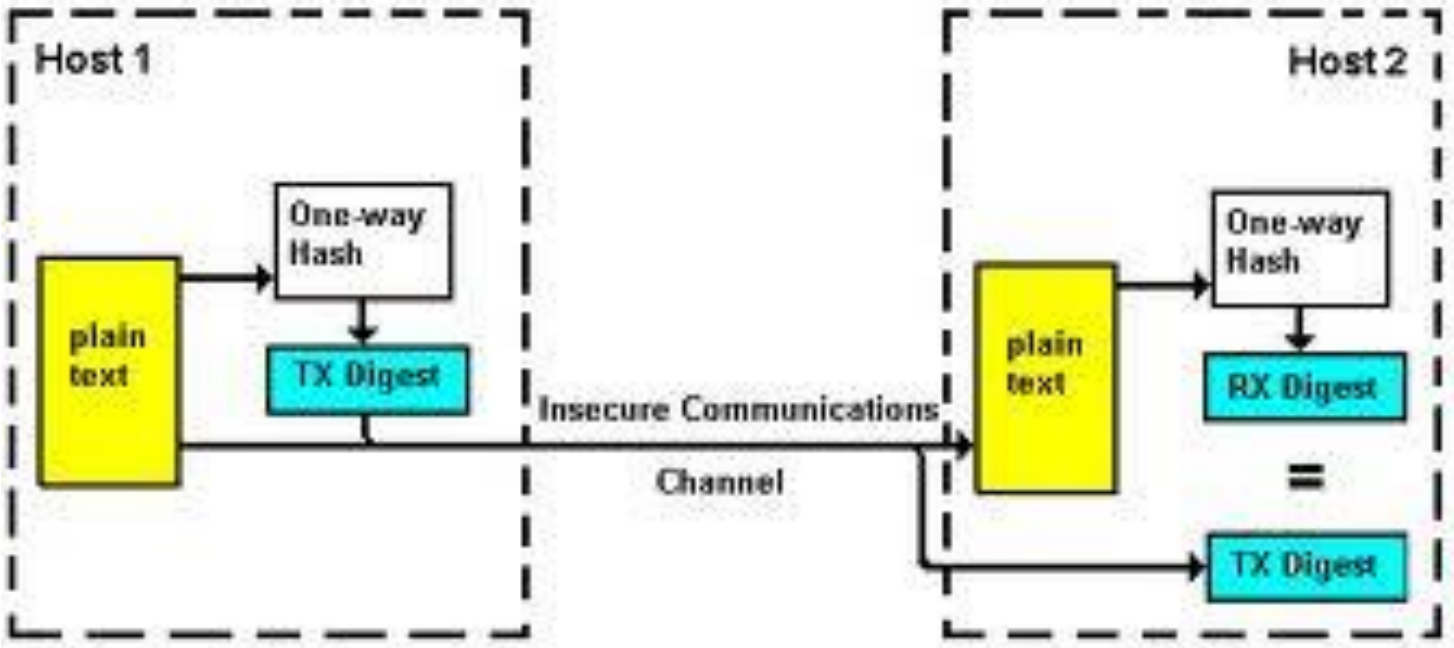
# Funções de Hash

- Uma função de hash (um sentido) aceita uma mensagem de comprimento variável M como entrada e produz um código hash de tamanho fixo H(M) como resultado (chamado Message Digest)

- O código de Hash fornece deteção de erros (uma alteração num bit da mensagem resulta numa alteração do código de hash).

UNIVERSIDADE PORTUCALENSE

# Funções de Hash




DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Requisitos para as funções de Hash

1. H pode ser aplicada a um bloco de dados de qualquer tamanho.
2. H produz um resultado com tamanho fixo.
3. É fácil de calcular H(x) para qualquer x.
4. Para qualquer h é computacionalmente inviável descobrir x onde H(x) = h (“uma mensagem ”)
5. Para qualquer x, é computacionalmente inviável encontrar y, y≠x, H(y) = H(x) (“resistência de colisão fraca”)
6. Computacionalmente inviável encontrar qualquer par (x, y) tal que H(x) = H(y) (“resistência forte colisão”)

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(utilização)

- O código de hash mais a mensagem é criptografado usando a criptografia simétrica.
- O código de hash fornece a estrutura ou a redundância necessária para alcançar a autenticação

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(utilização)

- Somente o código de hash é encriptado, usando a criptografia simétrica.

- Isto reduz a carga de processamento para aquelas aplicações que não exigem confidencialidade.

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(utilização)

- Somente o código de hash é criptografado, usando criptografia de chave pública e chave privada do remetente.
- Isso fornece autenticação. Ele também fornece uma assinatura digital, pois somente o remetente poderia ter produzido o código hash criptografado.
- É a essência da técnica de assinatura digital.

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(utilização)

- Se se desejar confidencialidade, bem como uma assinatura digital, então a mensagem mais o código de hash é encriptado por chave privada pode ser encriptado usando uma chave simétrica secreta.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(utilização)

- É possível usar uma função de hash, mas sem criptografia para autenticação de mensagem.
- A técnica pressupõe que as duas partes da comunicação compartilham um valor comum secreto S.
- **A** computa o hash com a concatenação de M e S e acrescenta o valor de hash resultante para M.
- Porque B possui S, ele pode recalcular o valor de hash para verificar.
- Porque o valor secreto propriamente dito não é enviado, um adversário não pode modificar uma mensagem intercetada e não é possível gerar uma mensagem falsa.

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(exemplo)

- Todas as funções de hash operaram utilizando os seguintes princípios gerais:
- A entrada (arquivo de mensagem, etc.) é vista como uma sequência de blocos de n-bits.
- É processado um bloco de cada vez, de um modo iterativo para produzir uma função de n-bit hash.

UNIVERSIDADE PORTUCALENSE

# Funções de Hash

(exemplo)

- Uma das mais simples funções de hash é o (XOR) bit-a-bit ou exclusivo de cada bloco. Isto pode ser expresso como se segue:
  - $C_i = b_{i1} + b_{i2} + ... + b_{im}$
  - onde
  - $C_i$ = i eximo bit do código de hash
  - m = número de blocos de n-bits de entrada
  - $b_{ij}$ = bit I no bloco j
  - + = operação de XOR

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

# Funções de Hash

(exemplo)

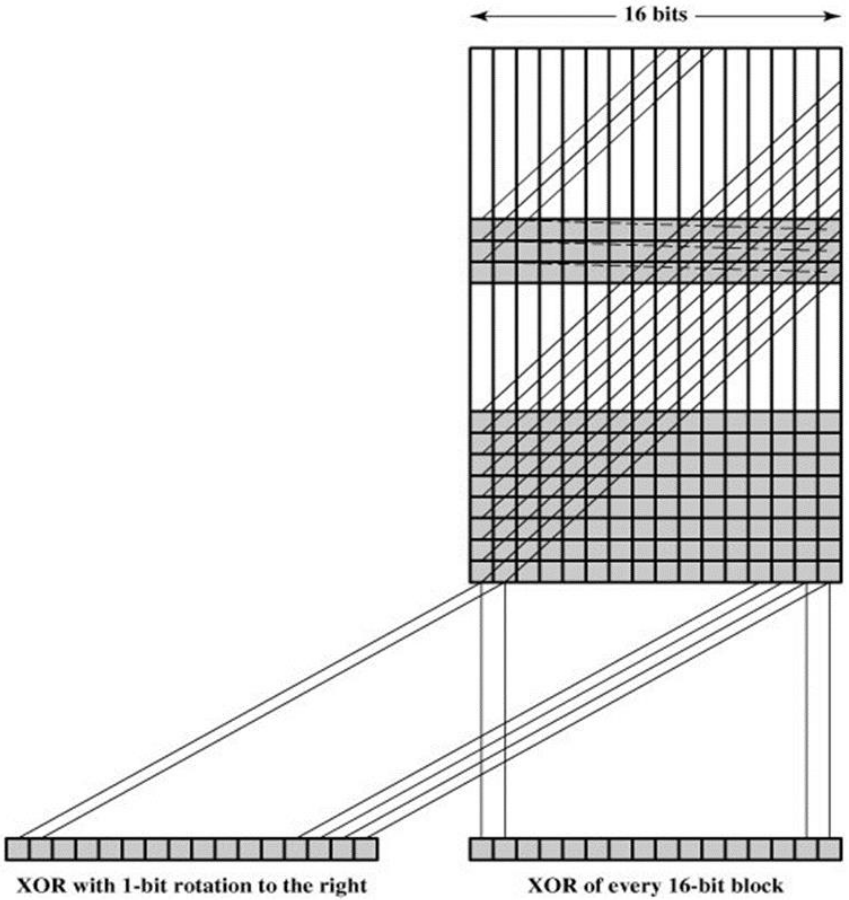
| X | Y | O |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |



XOR

# Funções de Hash

(exemplo)



UNIVERSIDADE PORTUCALENSE

# Segurança de e-mail

- Confidencialidade
  - proteção contra a divulgação
- Autenticação
  - De quem envia a mensagem
- Integridade da mensagem
  - Proteção contra a modificação
- Não-repúdio de origem
  - proteção da negação por remetente

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

# Pretty Good Privacy (PGP)

- Amplamente utilizado
- Desenvolvido por Phil Zimmermann
- Selecionados os melhores algoritmos de encriptação
- Utilizado em vários Sistemas operativos
- Originalmente livre (existe versão comercial)

UNIVERSIDADE PORTUCALENSE

# PGP - Autenticação

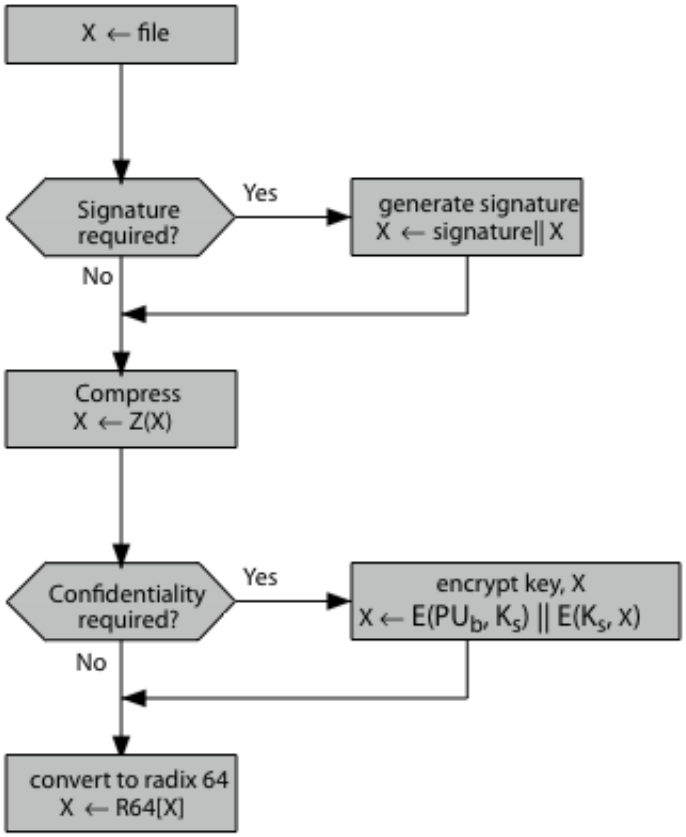
- Remetente cria mensagem
- Cria um hash SHA-1160-bit da mensagem
- RSA anexado assinado hash a mensagem
- Recetor desencripta e recupera o código hash
- Recetor verifica hash da mensagem recebida

UNIVERSIDADE PORTUCALENSE

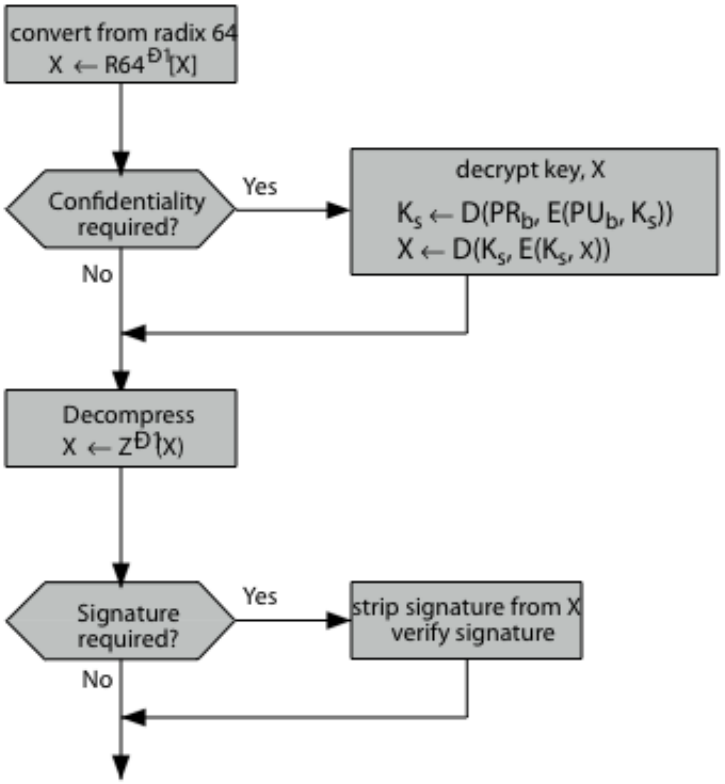
# PGP - Confidencialidade

- O Remetente gera uma chave aleatória de sessão de 128 bits
- Encripta a mensagem com a chave da sessão
- Anexa a chave da sessão encriptada com RSA
- Recetor desencripta e recupera a chave da sessão
- A chave da sessão é utilizada para desencriptar a mensagem

# PGP - Utilização




(a) Generic Transmission Diagram (from A)




(b) Generic Reception Diagram (to B)

Stallings