Estudo dirigido sobre o capítulo 8 (parte 1) – segurança de redes

INSTITUTO FEDERAL
RIO GRANDE DO SUL

1. Liste algumas categorias mais predominantes e prejudiciais dos ataques na Internet.

- Ataques *malware*, recusa de serviço, analisador de pacotes, disfarce da fonte e modificação e exclusão de mensagem

2. Liste as propriedades desejáveis da comunicação segura.

- Confidencialidade
- Autenticação do ponto final
- Integridade de mensagem
- Segurança operacional

3. Descreva confidencialidade.

- Somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida
- A mensagem deve estar cifrada de alguma maneira para impedir que uma mensagem interceptada seja entendida por um interceptador
- Esse aspecto de confidencialidade é, provavelmente, o significado mais comumente percebido na expressão comunicação segura

4. Descreva a propriedade autenticação do ponto final.

- O remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na comunicação – confirmar que a outra parte realmente é quem alega ser
- Quando entidades comunicantes trocam mensagens por um meio pelo qual não podem ver a outra parte, a autenticação não é tão simples assim

5. Descreva a propriedade integridade de mensagem.

- As partes comunicantes também querem assegurar que o conteúdo de sua comunicação não seja alterado, por acidente ou por má intenção, durante a transmissão
- Extensões das técnicas de soma de verificação que encontramos em protocolos de transporte e de enlace confiáveis podem ser utilizadas para proporcionar integridade à mensagem

6. Descreva a propriedade segurança operacional.

- Quase todas as organizações possuem redes conectadas à Internet pública
- Essas redes podem ser comprometidas potencialmente por atacantes que ganham acesso a essas redes por meio da Internet pública
- Os atacantes podem tentar colocar *worms* nos hospedeiros na rede, adquirir segredos corporativos, mapear as configurações da rede interna e lançar ataques DoS
- Mecanismos operacionais, como *firewalls* e sistemas de detecção de invasão, são usados para deter ataques contra redes de organizações

7. Quais são as ações possíveis de um intruso passivo?

- Monitorar – identificar e gravar as mensagens de controle e de dados no canal
- Modificar, inserir ou eliminar mensagens ou conteúdos de mensagens

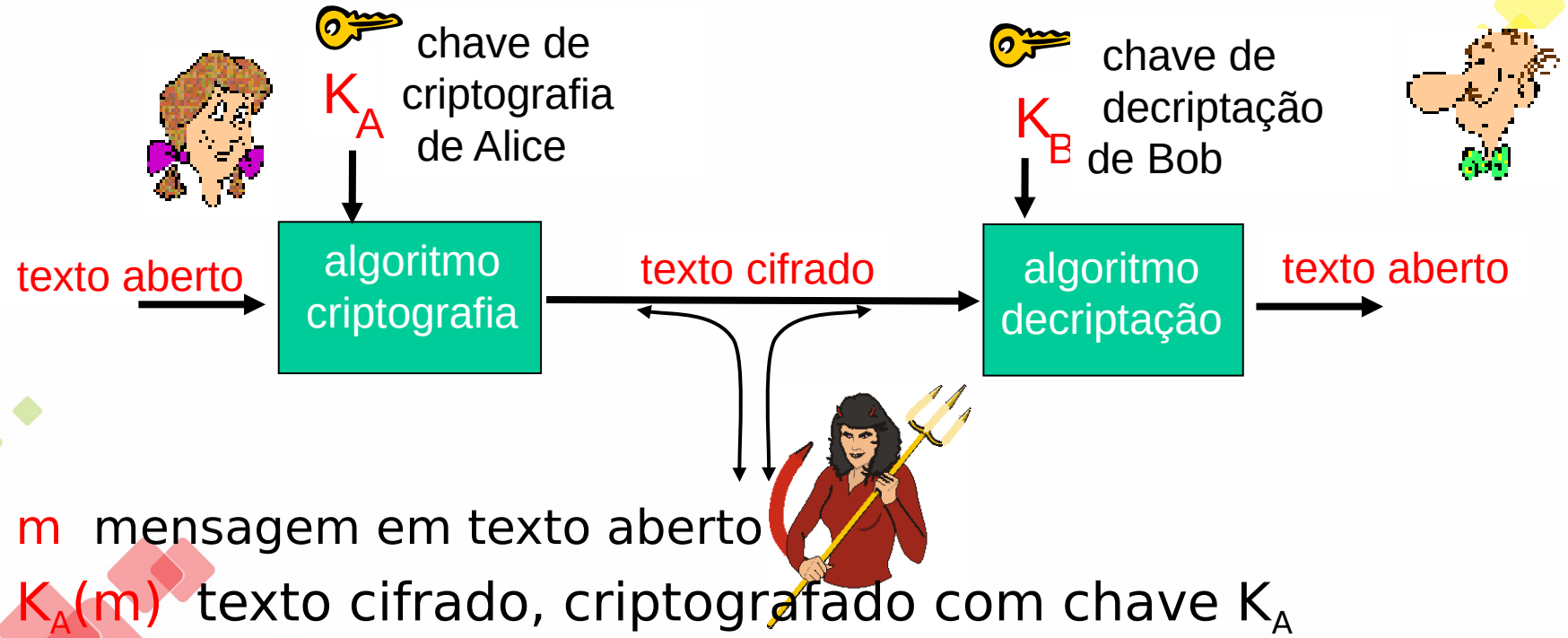
8. Explique sucintamente os componentes mais importantes da terminologia usada em criptografia.

- A mensagem de Alice em sua forma original é conhecida como **texto aberto** ou texto claro
- Alice criptografa sua mensagem em texto aberto usando um **algoritmo de criptografia**, de modo que a mensagem criptografada, conhecida como **texto cifrado**, pareça ininteligível para qualquer intruso
- Uma **chave** K_A é uma cadeia de números ou de caracteres que serve como entrada para o **algoritmo de criptografia**. O algoritmo de criptografia pega essa chave e o texto aberto da mensagem, m, como entrada e produz o texto cifrado como saída
- Bob fornecerá uma **chave** K_B ao **algoritmo de decriptação**, que pega o texto cifrado e a chave de Bob como entrada e produz o texto original como saída

8. Explique sucintamente os componentes mais importantes da terminologia usada em criptografia.

- em sistemas de chaves simétricas, as chaves de Bob e Alice são idênticas e secretas
- Em sistemas de chaves públicas, é usado um par de chaves. Uma das chaves é conhecida por Bob e por Alice (na verdade, é conhecida pelo mundo inteiro)
- A outra chave é conhecida apenas por Bob ou por Alice (mas não por ambos)

8. Explique sucintamente os componentes mais importantes da terminologia usada em criptografia.



m mensagem em texto aberto

$K_A(m)$ texto cifrado, criptografado com chave K_A

$m = K_B(K_A(m))$

9. Descreva a cifra de César.

- A cifra de César funciona tomando cada letra da mensagem do texto aberto e substituindo-a pela k-ésima letra sucessiva do alfabeto (permitindo a rotatividade, isto é, a letra z seria seguida novamente da letra a)
- Por exemplo, se k=3, então a letra a do texto aberto fica sendo d no texto cifrado; b se transforma em e, e assim por diante
- No caso, o valor de k serve como chave

10.Descreva a cifra monoalfabética.

- Em vez de substituir as letras seguindo um padrão regular, qualquer letra pode ser substituída por qualquer outra, contanto que cada letra tenha uma única letra substituta e vice-versa

10.Descreva a cifra monoalfabética.

texto aberto: abcdefghijklmnopqrstuvwxyz

texto cifrado: mnbvcxzasdfghjklpoiuytrewq

11. O que é abordagem de força bruta e análise estatística no contexto da cifra monoalfabética?

- A abordagem de força bruta iria testar todas as possíveis chaves do algoritmo
- A análise estatística se vale de alguma informação importante sobre o texto aberto, por exemplo: sabe-se que as letras e e t são as mais frequentes em textos em inglês

12. Quais são os três cenários diferentes, dependendo do tipo de informação que o intruso tem, para quebrar um código criptográfico?

- Ataque exclusivo a texto cifrado – o intruso tem acesso somente ao texto cifrado interceptado
- Ataque com texto aberto conhecido – quando o intruso conhece alguns dos pares (texto aberto, texto cifrado)
- Ataque com texto aberto escolhido – o intruso pode escolher a mensagem em texto aberto e obter seu texto cifrado correspondente

13. Descreva a cifra polialfabética.

- Usa várias cifras monoalfabéticas com uma cifra mono para codificar uma letra em uma posição específica no texto aberto da mensagem
- Há um modelo de repetição para as cifras monoalfabéticas como em C_1,C_2,C_2,C_1 e C_2

14. Como funciona uma cifra de bloco?

- Na cifra de bloco, a mensagem é processada em blocos de k bits
- Cada bloco é criptografado de maneira independente
- Para criptografar um bloco, a cifra utiliza um mapeamento um para um para mapear o bloco de k bits de texto aberto para um bloco de k bits de texto cifrado

14. Como funciona uma cifra de bloco?

Exemplo com k = 3:

entrada	saída
000	110
001	111
010	101
011	100

entrada	saída
100	011
101	010
110	000
111	001

Qual é o texto cifrado para 010110001111 ?

15. Por que as cifras de bloco de tabela completa são difíceis de implementar?

- Devido aos tamanhos das tabelas de mapeamento
- Para k=64 e para um deteminado mapeamento, Alice e Bob precisariam manter uma tabela com 2^{64} valores de entrada, uma tarefa impraticável

16. Cite cifras de bloco conhecidas.

- **DES** (*Data Encryption Standard*)
- **3DES**
- **AES** (*Advanced Encryption Standard*)

17. Qual é o problema que pode surgir quando se usa uma cifra de blocos que criptografa independentemente cada bloco?

- Dois ou mais blocos de texto aberto podem ser idênticos
- Em relação a estes blocos idênticos, uma cifra de bloco produziria, é claro, o mesmo texto cifrado
- Um atacante poderia eventualmente adivinhar o texto aberto ao ver blocos de texto cifrado idênticos e ser capaz de decriptografar a mensagem inteira identificando os blocos de texto cifrado idênticos e usando o que sabe sobre a estrutura da mensagem em questão

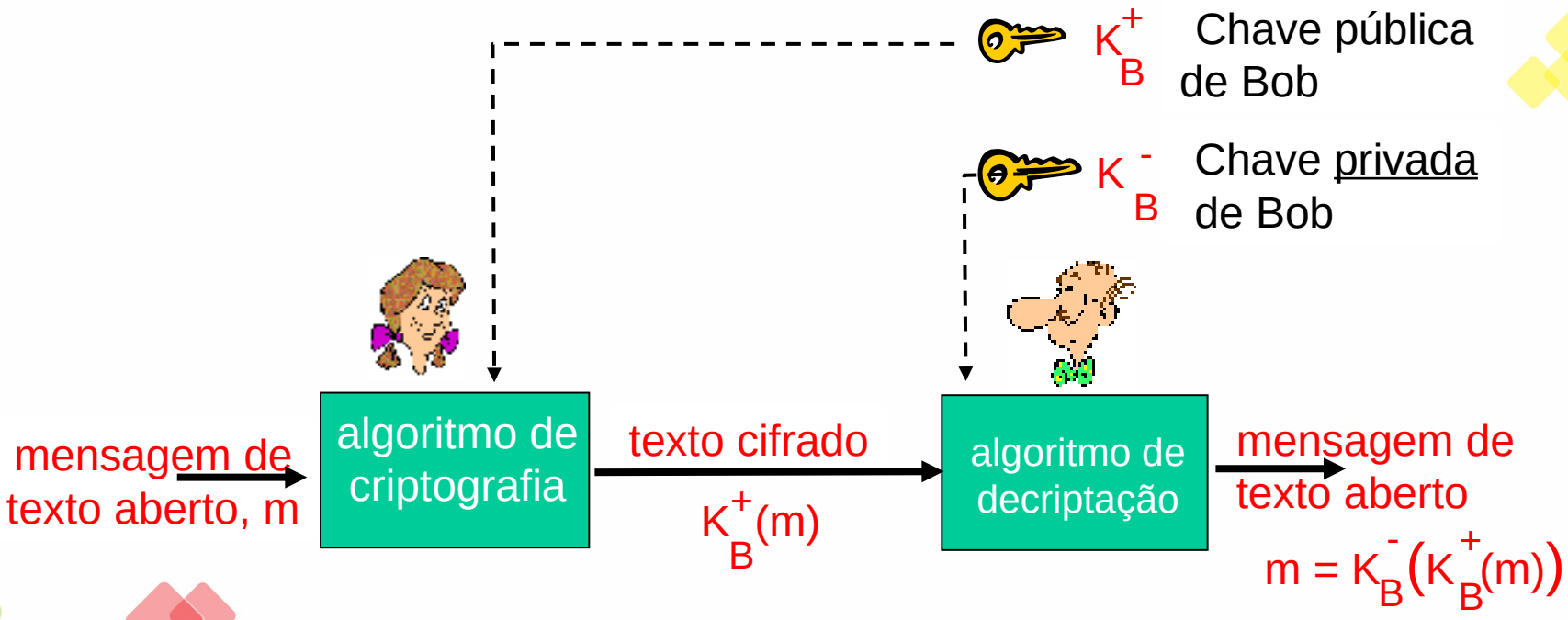
18. Explique a técnica chamada Encadeamento do Bloco de Cifra (CBC).

- A ideia básica é enviar somente um valor aleatório junto com a primeira mensagem e, então, fazer com que o emissor e o receptor usem blocos codificados em vez do número aleatório subsequente
- Antes de criptografar a mensagem, o emissor cria uma cadeia de k bits, chamada vetor de inicialização, c(0); o emissor envia o IV ao receptor em texto aberto
- O emissor calcula m(1)+c(0) - ou-exclusivo – e codifica o resultado através do algoritmo de cifra de bloco. O emissor envia o bloco crptografado c(1) ao receptor
- Para o i-esimo bloco, o emissor cria o i-ésimo bloco de texto cifrado de $c(i)=K_s (m(i)+c(i-1))$
- ONDE M É O TEXTO ABERTO, C É O TEXTO CIFRADO, + INDICA OU-EXCLUSIVO E K_s INDICA A CRIPTOGRAFIA DA CIFRA DE BLOCO

19. Como se dá a utilização de criptografia de chaves públicas?

- Bob tem duas chaves – uma chave pública, que está à disposição do mundo todo, e uma chave privada, que apenas Bob conhece
- Para se comunicar com Bob, Alice busca primeiramente a chave pública de Bob
- Em seguida, ela criptografa sua mensagem usando a chave pública de Bob e um algoritmo criptográfico conhecido
- Bob recebe a mensagem criptografada de Alice e usa sua chave privada e um algoritmo de decriptação conhecido para decifrar a mensagem de Alice

19. Como se dá a utilização de criptografia de chaves públicas?



20. Qual é o algoritmo que se tornou quase um sinônimo de criptografia de chave pública?

- Embora existam muitos algoritmos e chaves que tratam dessas preocupações, o algoritmo RSA (cujo nomo se deve a seus inventores, Ron Rivest, Adi Shamir e Leonard Adleman) tornou-se quase um sinônimo de criptografia de chave pública

21. O que é uma chave de sessão?

- A exponenciação exigida pelo RSA é um processo que consome tempo considerável
- Como resultado, o RSA é frequentemente usado na prática em combinação com a criptografia de chave simétrica
- Alice escolhe uma chave que será utilizada para codificar os dados; essa chave às vezes é denominada chave de sessão
- Alice deve informar a Bob essa chave de sessão, já que essa é a chave simétrica compartilhada que eles usarão com uma cifra de chave simétrica (exemplo: DES ou AES)
- Alice criptografa o valor da chave de sessão usando a chave pública RSA de Bob
- Bob recebe a chave de sessão codificada com RSA e a decifra para obter a chave de sessão
- Ele agora conhece a chave que Alice usará para transferir dados cifrados em DES

22. O que é necessário para se autenticar uma mensagem?

- A mensagem foi, realmente, enviada por Alice
- A mensagem não foi alterada a caminho de Bob

23. O que é uma função de hash e qual é a sua propriedade adicional?

- A função de hash recebe uma entrada, m, e computa uma cadeia de tamanho fixo H(m) conhecida como hash
- A soma de verificação da Internet e os CRCs satisfazem esta definição
- Uma função de hash criptográfica deve apresentar a seguinte propriedade adicional:
- Em termos de processamento, é impraticável encontrar duas mensagens diferentes x e y tal que H(x)=H(y)

24. Descreva rapidamente dois algoritmos de hash.

- O algoritmo de hash MD5 de Ron Rivest é amplamente usado hoje
- Ele processa um resumo de mensagem de 128 bits por meio de um processo de quatro etapas
- O segundo principal algoritmo de hash em uso atualmente é o SHA-1 (*secure hash algorithm*)
- Esse algoritmo se baseia em princípios similares aos usados no projeto do MD4, o predecessor do MD5
- O uso do SHA-1, um padrão federal norte-americano, é exigido sempre que aplicações de âmbito federal precisarem de um algoritmo de resumo de mensagem seguro
- Ele produz um resumo de mensagem de 160 bits. O resultado mais longo torna o SHA-1 mais seguro

25. Como se pode garantir a integridade de uma mensagem?

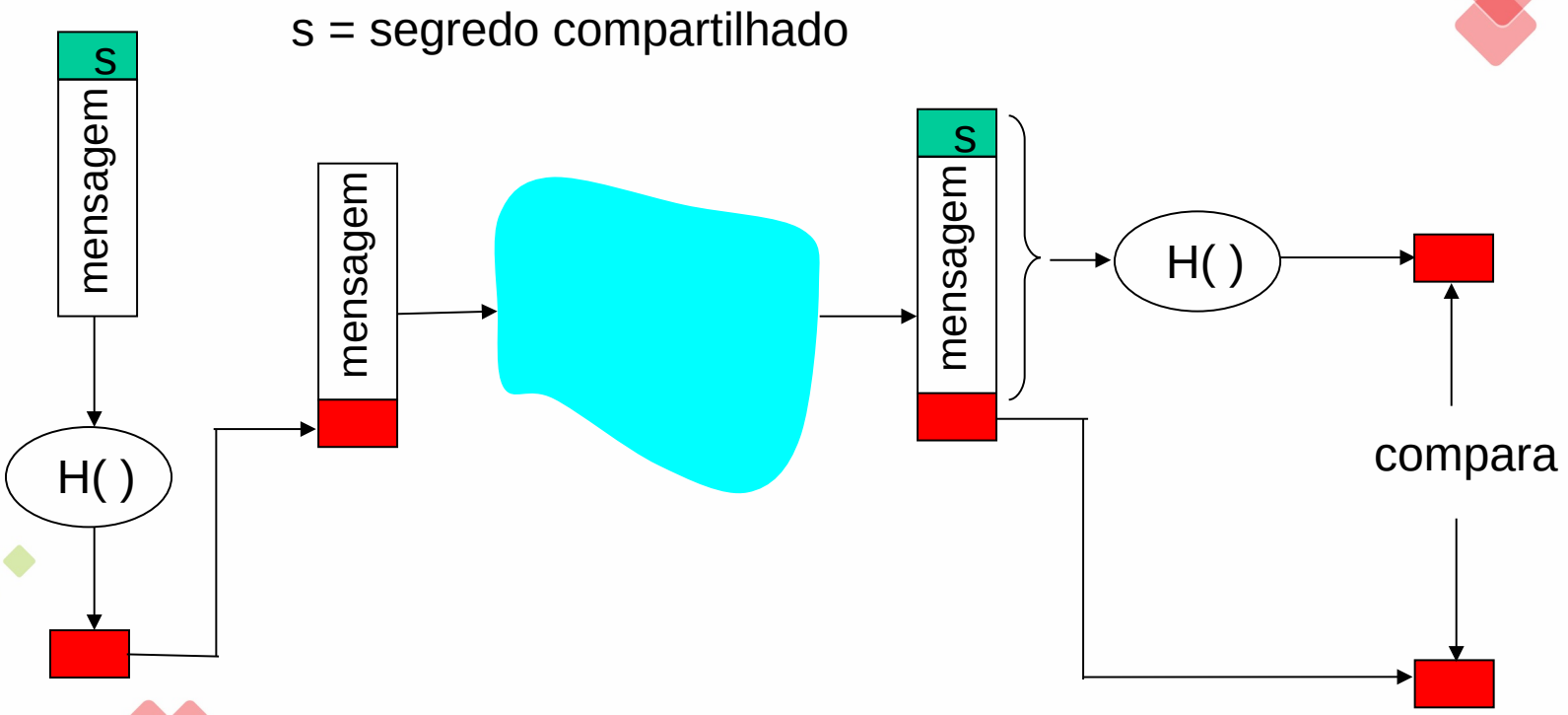
Alice e Bob precisarão de um segredo compartilhado s, que não é nada mais do que uma cadeia de bits denominada chave de autenticação

1. Alice cria a mensagem m, concatena s com m para criar m+s, e calcula o hash H(m+s), que é denominado o código de autenticação da mensagem - MAC

2. Alice então anexa o MAC à mensagem m, criando uma mensagem estendida (m,H(m+s)), e a envia a Bob

3. Bob recebe uma mensagem estendida (m,h) e conhecendo s, calcula o MAC H(m+s). Se H(m+s)=h, Bob conclui que está tudo certo

25. Como se pode garantir a integridade de uma mensagem?



26. O que é uma chave de autenticação?

- A chave de autenticação é o segredo compartilhado s

27. Quais são as finalidades de uma assinatura digital?

- No mundo digital, frequentemente se quer indicar o dono ou o criador de um documento ou deixar claro que alguém concorda com o conteúdo de um documento
- A assinatura digital é uma técnica criptográfica usada para cumprir essas finalidades no mundo digital

28. A assinatura digital deve ser verificável e não falsificável. O que isso significa?

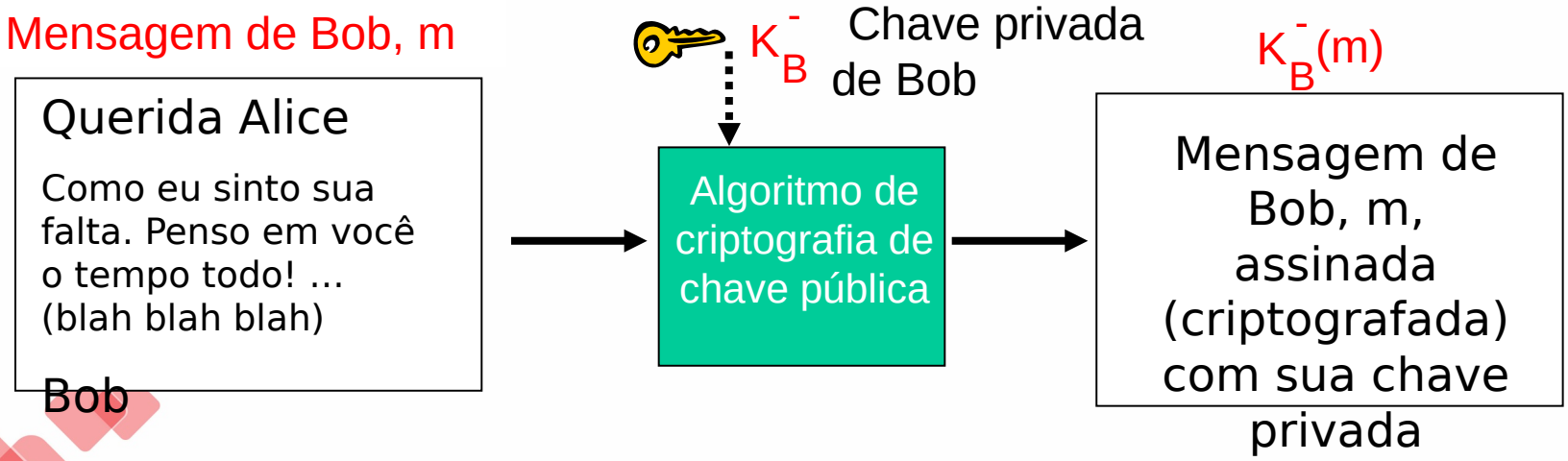
- Deve ser possível provar que um documento assinado por um indivíduo foi na verdade assinado por ele (a assinatura tem de ser verificável)
- E que somente aquele indivíduo poderia ter assinado o documento (a assinatura não pode ser falsificada)

29. Por que apenas os MACs não são suficientes para uma assinatura digital?

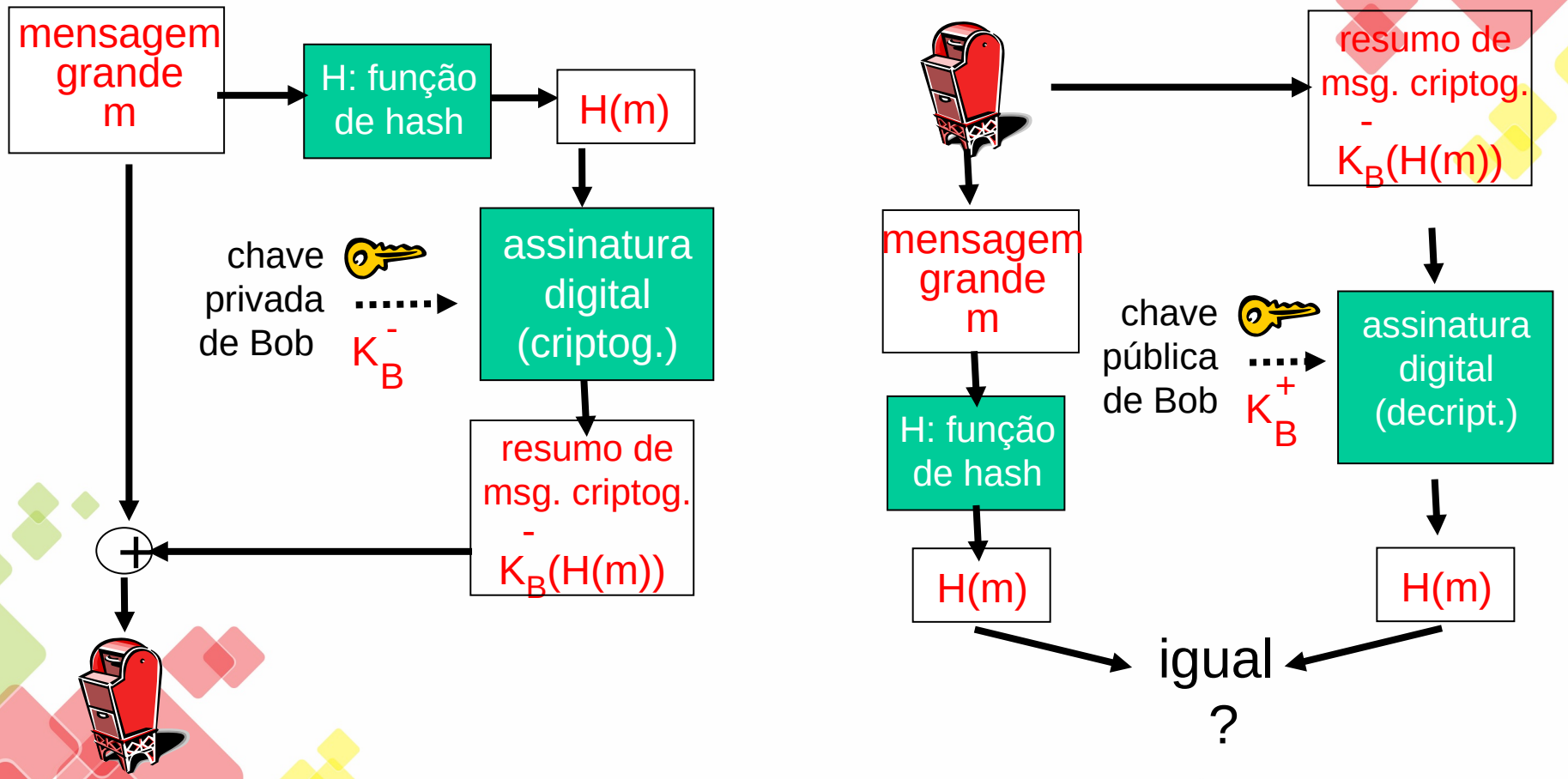
- Quando Bob assina uma mensagem, ele deve colocar algo nela que seja único para ele
- Bob poderia adicionar um MAC à assinatura, sendo o MAC criado ao adicionar sua chave (única para ele) à mensagem e, depois, formar o hash
- Mas para Alice verificar a assinatura, ela deve também ter uma cópia da chave, que não seria única para Bob
- Portanto, os MACs não se incluem nesse processo

30. Explique o processo de criação de uma assinatura digital para uma mensagem m ou seu hash, H(m).

- Bob usa sua chave privada para criptografar a mensagem m, ou, ainda melhor, para criptografar o hash H(m), que exige muito menos processamento



30. Explique o processo de criação de uma assinatura digital para uma mensagem `m` ou seu hash, `H(m)`.



31. Compare MACs com assinaturas digitais.

- Uma assinatura digital é uma técnica “mais pesada”, uma vez que ela exige uma Infraestrutura de Chave Pública (PKI), subjacente com autoridades de certificação
- O PGP – um sistema seguro de e-mail renomado – utiliza assinaturas digitais para a integridade da mensagem
- O OSPF usa MACs para a integridade da mensagem
- Os MACs são também usados pelos conhecidos protocolos de segurança da camada de transporte e da camada de rede

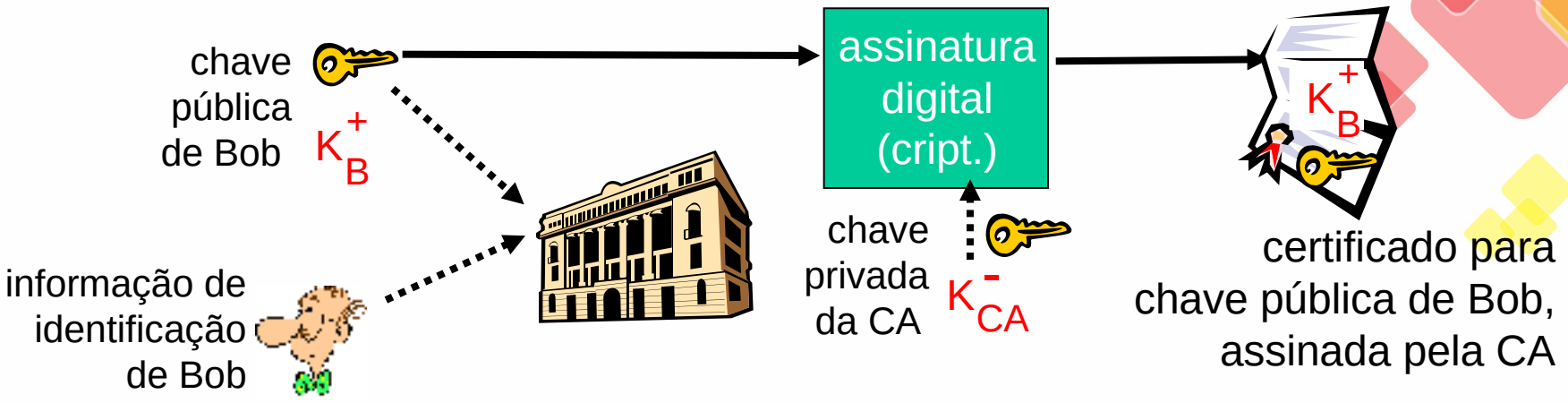
32. Dê um exemplo que demonstre a importância de verificar se uma chave pública é verdadeira.

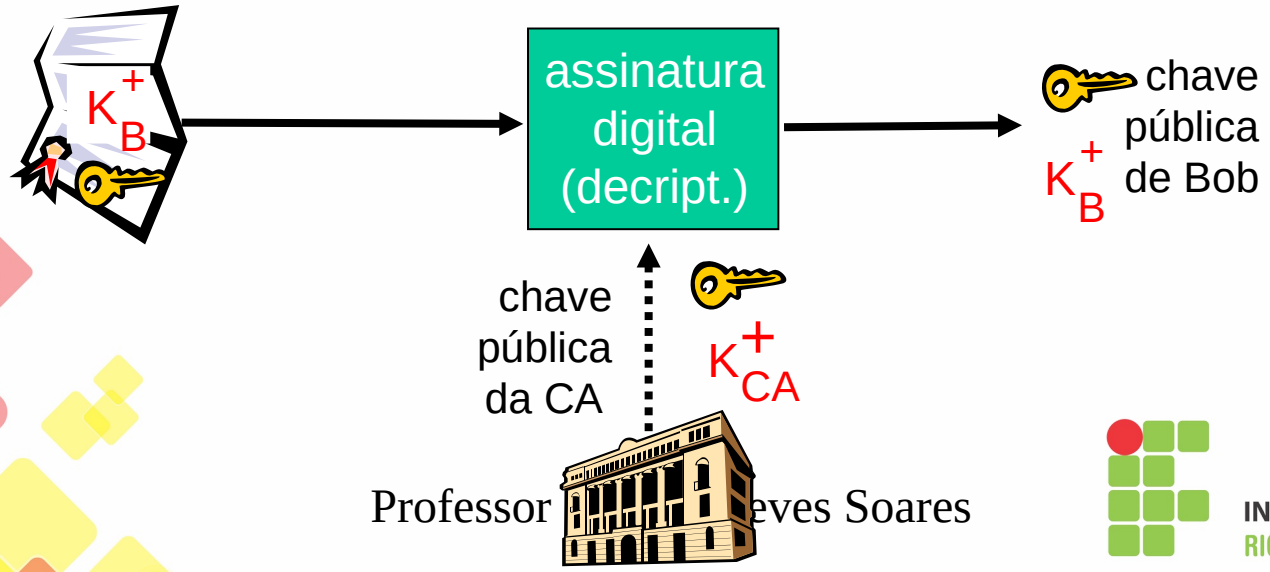
- Bob envia a Alice uma mensagem em texto aberto que contém o endereço de sua casa e o tipo de pizza que quer
- Nessa mensagem, ele inclui também uma assinatura digital (isto é, um hash assinado extraído da mensagem original em texto aberto)
- Trudy envia uma mensagem a Alice na qual diz que é Bob, fornece o endereço de Bob e pede uma pizza
- Nessa mensagem ela também inclui sua chave pública, embora Alice admita, naturalmente, que seja a de Bob
- Trudy também anexa uma assinatura digital, a qual foi criada com sua própria chave privada

33.Quais são as incumbências de uma autoridade certificadora?

- 1. Uma CA verifica se uma entidade (pessoa, roteador e assim por diante) é quem diz ser
- 2. Tão logo verifique a identidade da entidade, a CA cria um certificado que vincula a chave pública da entidade à identidade verificada
- O certificado contém a chave pública e a informação exclusiva que identifica mundialmente o proprietário da chave pública

33.Quais são as incumbências de uma autoridade certificadora?





34. Qual é a solução para o problema levantado na questão 32?

- Quando Bob faz seu pedido, ele também envia seu certificado assinado por uma CA
- Alice usa a chave pública da CA para verificar a validade do certificado de Bob e extrair a chave pública dele

35. O que é a autenticação do ponto final?

- A autenticação do ponto final é o processo de provar a identidade de uma pessoa a alguém

36. Exemplifique um ataque de reprodução.

- Trudy precisa somente analisar e gravar a mensagem estendida de Alice (com o MAC) e reproduzi-la um tempo depois
- A mensagem repetida poderia ser “Concordo em transferir um milhão de dólares da conta de Bill para a conta de Trudy”, fazendo com que um total de dois milhões de dólares sejam transferidos
- Ou a mensagem poderia ser “o enlace do roteador Alice para o roteador Charlie parou de funcionar”, que, se enviada após o enlace ter sido consertado, poderia causar configurações errôneas nas tabelas de repasse

37. O que é um nonce e como ele é usado na autenticação do ponto final?

- Um nonce é um número que o protocolo usará somente uma vez por toda a vida

1. Bob escolhe um nonce, R, e o envia a Alice. Observe que o nonce é enviado em aberto. Alice agora cria o MAC usando m, s e o nonce R. Para criar o MAC, Alice pode, por exemplo, concatenar o segredo compartilhado e o nonce com a mensagem e obter um resumo através de um hash). Alice anexa o MAC à mensagem, cria uma mensagem estendida e a envia para Bob

2. Bob calcula o MAC da mensagem (contido na mensagem estendida), um nonce R e o segredo comparilhado s. Se o MAC resultante for igual ao MAC da mensagem estendida, Bob sabe não somente que Alice criou a mensagem mas também que ela criou a mensagem após Bob ter enviado um nonce