SEGURANÇA DA INFORMAÇÃO

Códigos de autenticação de mensagens e funções Hash

ROTEIRO

- O que é autenticação de mensagens?
- Requisitos da segurança de mensagens
- Funções de autenticação de mensagens
- Por que autenticação de mensagens?
- Código de autenticação de mensagens

O QUE É AUTENTICAÇÃO DE MENSAGENS?

A **autenticação de mensagem** é um mecanismo ou serviço usado para verificar a integridade de uma mensagem.

A autenticação de mensagem garante que os dados recebidos sejam exatamente como enviados (ou seja, não contenham modificação, inserção, exclusão ou reprodução) e que a suposta identidade do remetente seja válida.

REQUISITOS DA SEGURANÇA DE MENSAGENS

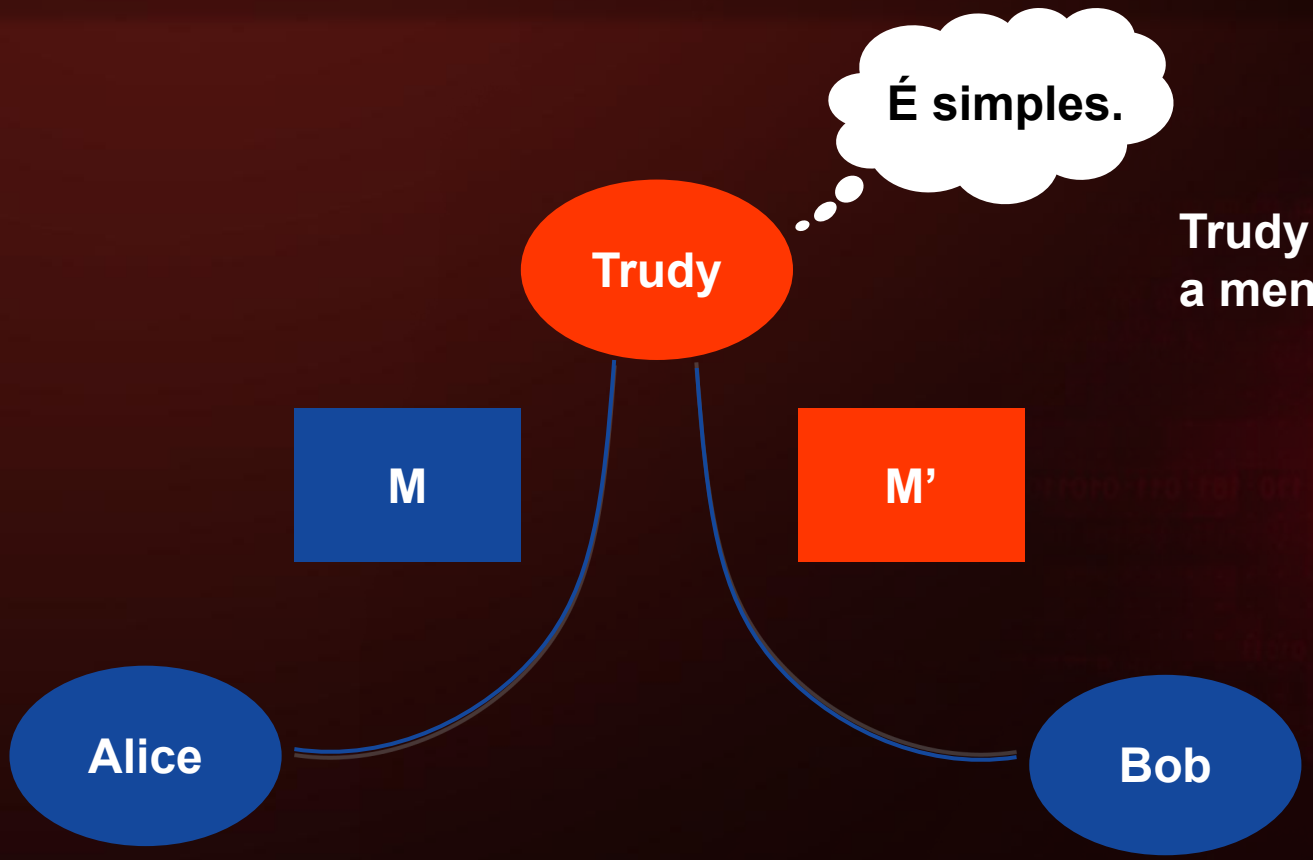
- ✔ Divulgação
- ✔ Análise de tráfego
- ✔ Modificação de conteúdo
- ✔ Modificação de sequência
- ✔ Modificação de tempo
- ✔ Repúdio da fonte
- ✔ Repúdio de destino

POR QUE AUTENTICAR MENSAGENS?

Utilizamos autenticação para:

- proteger a integridade de uma mensagem
- validar a identidade do originador
- não repúdio de origem (resolução de disputas)

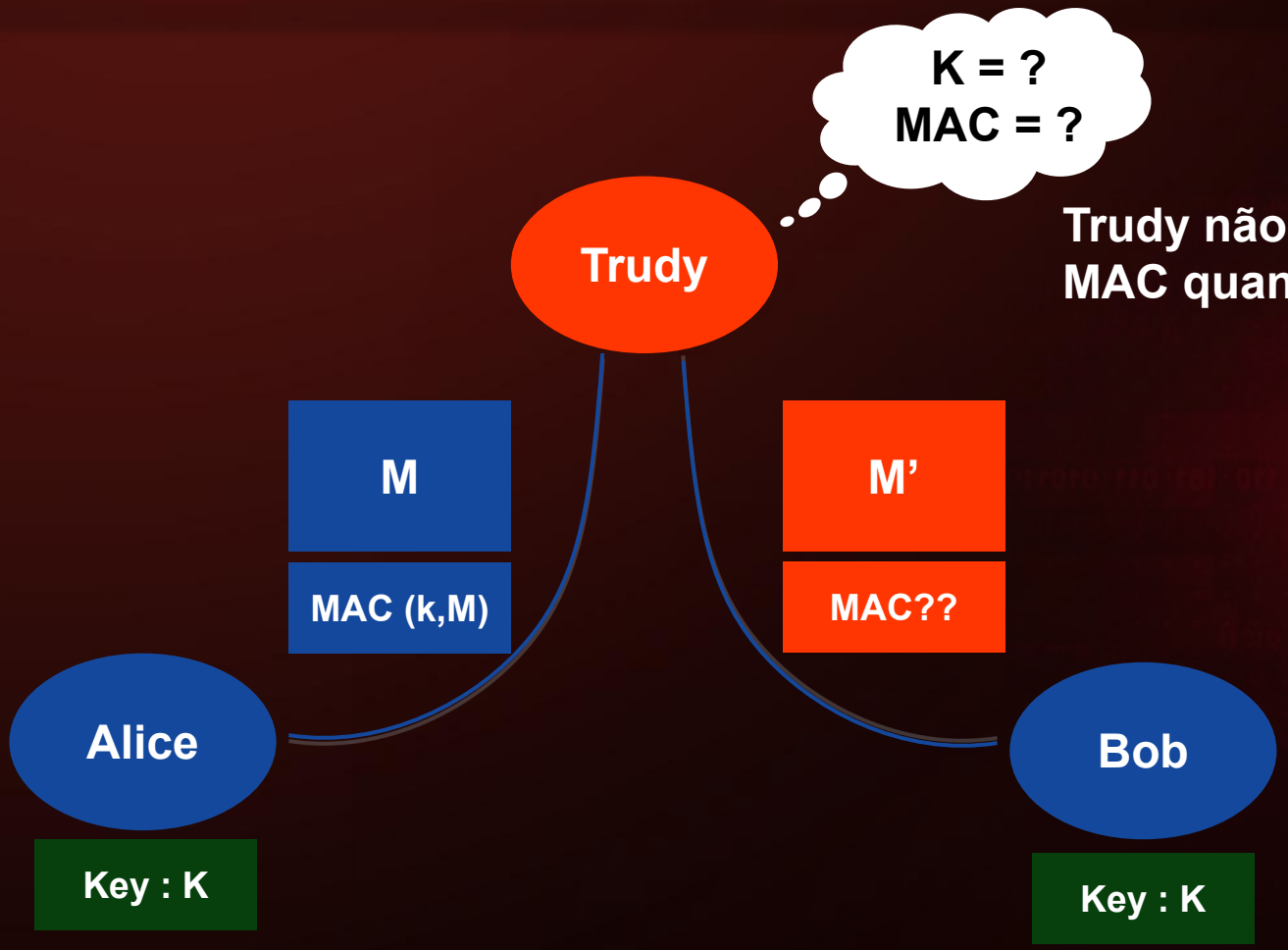
POR QUE AUTENTICAR MENSAGENS?



Trudy pode modificar a mensagem

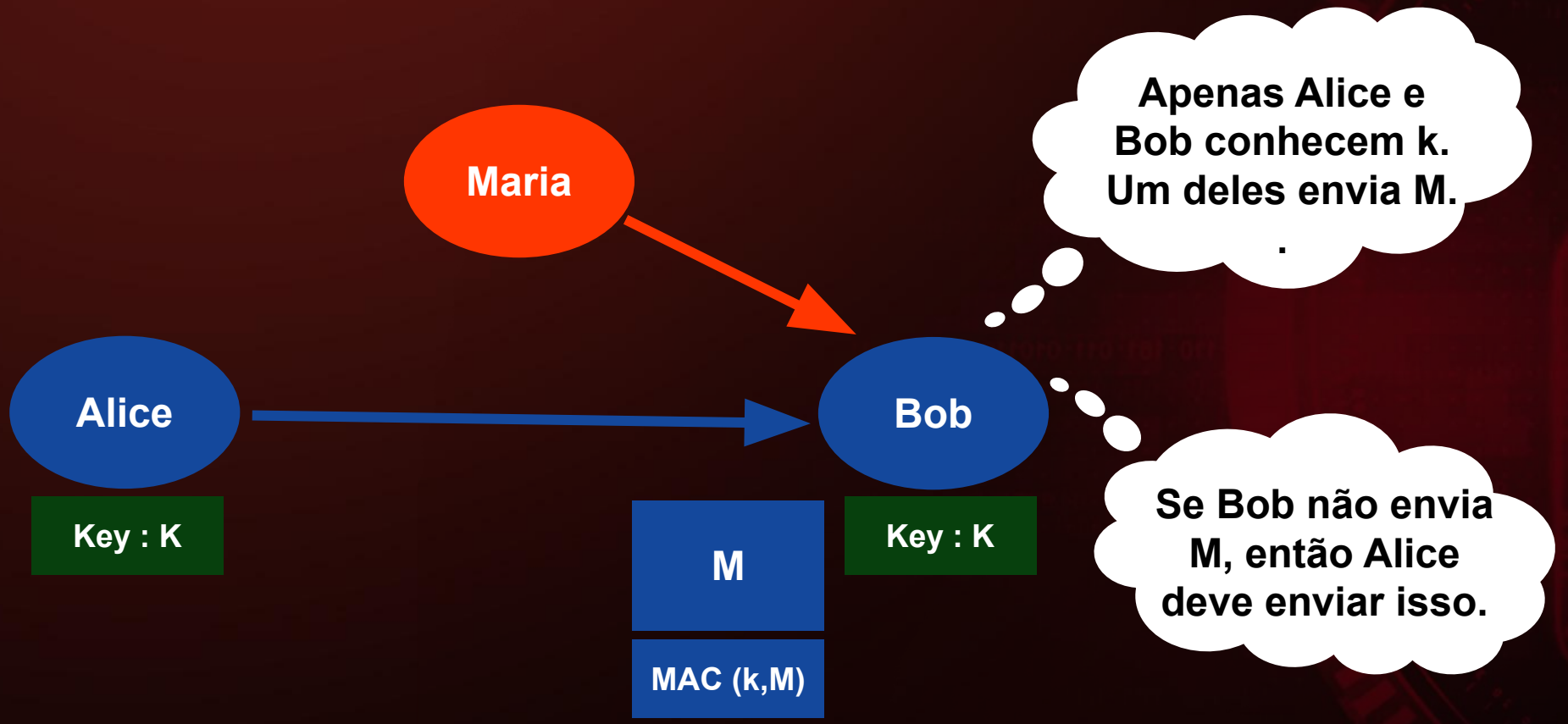
Chave compartilhada K para gerar a mensagem autenticada

PROTEGER A INTEGRIDADE COM MAC

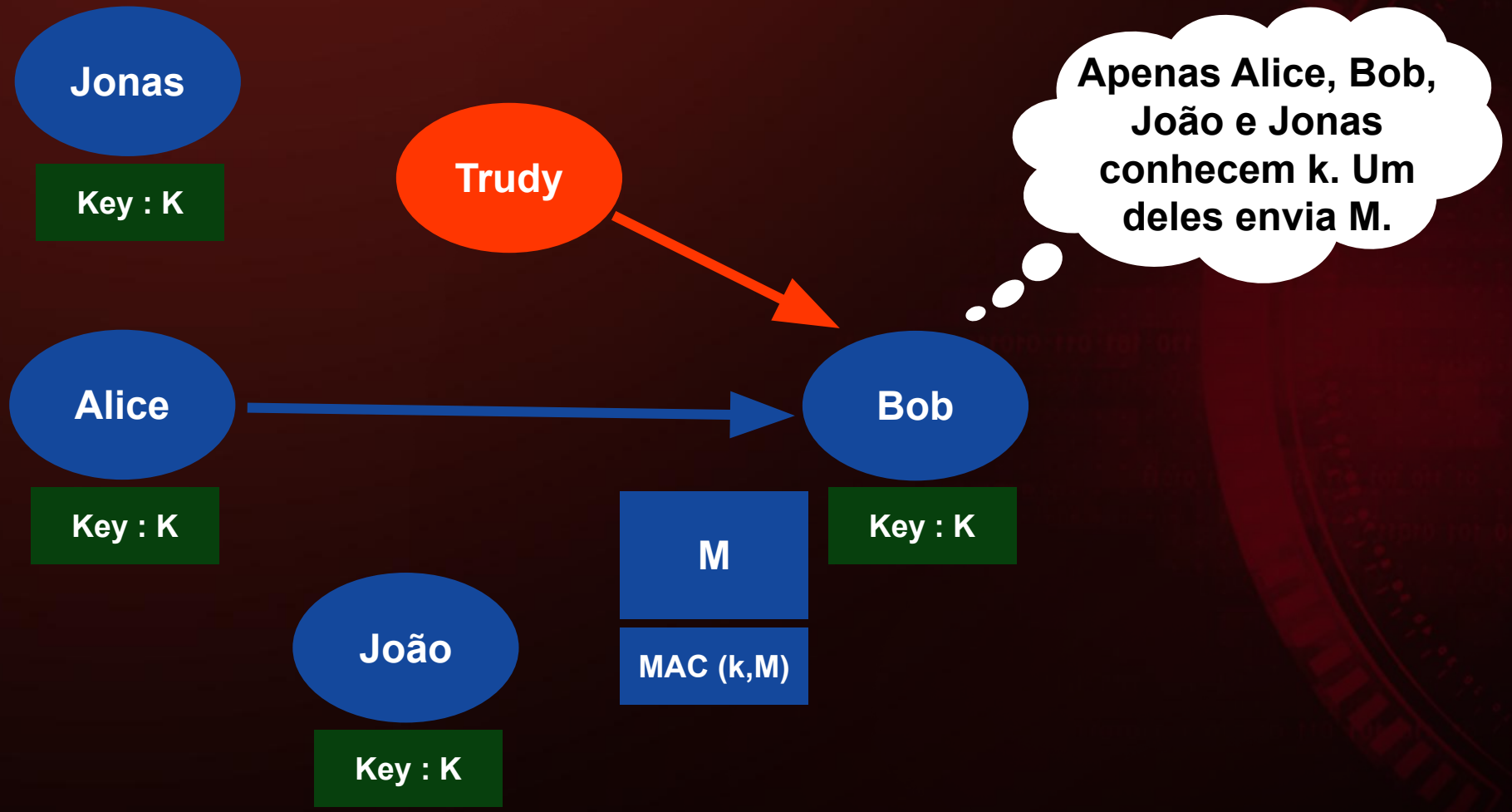


Chave compartilhada K para gerar a mensagem autenticada

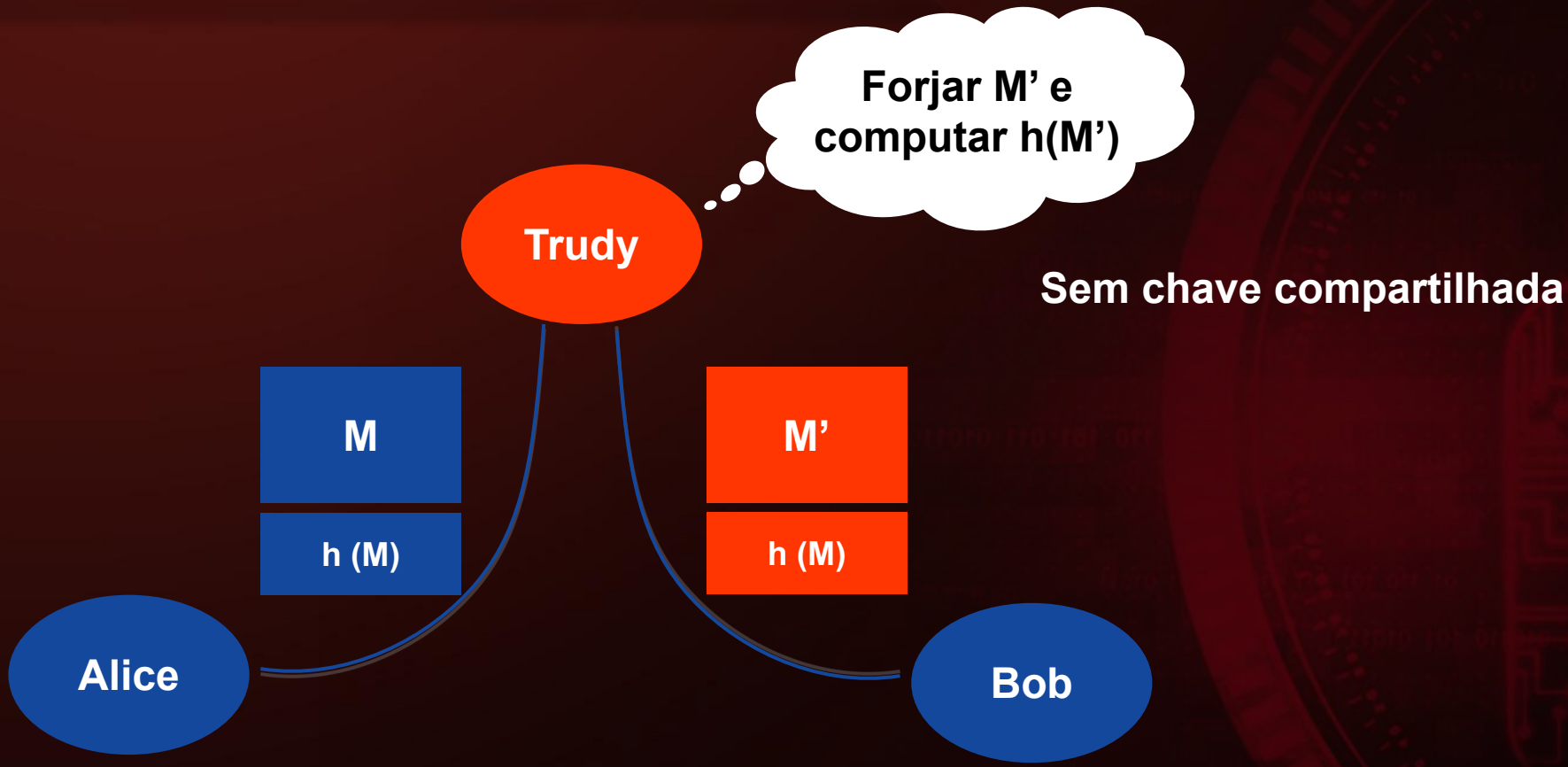
AUTENTICAÇÃO DE MENSAGENS



AUTENTICAÇÃO DE MENSAGENS



INTEGRIDADE COM HASH



Não podemos enviar o hash com a mensagem para servir de autenticação de mensagem, pois Trudy pode alterar a mensagem e recalcular o hash.

O uso de hash precisa de um procedimento mais apropriado para garantir a integridade

FUNÇÕES DE AUTENTICAÇÃO DE MENSAGENS

Funções Hash

Uma família de hash é uma tupla (X, Y, K, H), onde:

- ✔ X é um conjunto de mensagens possíveis
- ✔ Y é um conjunto finito de possíveis resumos de mensagens
- ✔ K é o espaço-chave
- ✔ Para cada $K \in \mathcal{K}$, existe uma função hash $h_K \in \mathcal{H}$. Cada $h_K: X \rightarrow Y$

FUNÇÕES DE AUTENTICAÇÃO DE MENSAGENS

Limitações de Função de Hash

Exige um canal confiável para transmitir o hash de uma mensagem

- ✔ Qualquer um pode calcular o valor de hash de uma mensagem, pois a função de hash é pública

Como resolver isso?

- ✔ Utilizar mais de uma função hash
- ✔ Utilizar um chave

POR QUE AUTENTICAÇÃO DE MENSAGENS?

A autenticação utiliza a criptografia convencional

Desta forma, somente o remetente e o destinatário devem compartilhar uma chave

Na autenticação de mensagem sem criptografia

- ✔ Uma etiqueta de autenticação é gerada e anexada a cada mensagem

Código de autenticação de mensagem

- ✔ Calcular o MAC em função da mensagem e da chave

$$MAC = F(K, M)$$

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

Um código de autenticação de mensagem (MAC) é um algoritmo que requer o uso de uma chave secreta.

Um MAC recebe uma mensagem de comprimento variável e uma chave secreta como entrada e produz um código de autenticação.

Um destinatário de posse da chave secreta pode gerar um código de autenticação para verificar a integridade da mensagem.

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

MAC é um pequeno código de comprimento fixo gerado usando chave (K) e a mensagem (M)

✔ MAC = C (K, M)

O código gerado não é reversível.

Um MAC O MAC é anexado à mensagem como uma assinatura.

No lado do receptor é calculado um novo MAC, que é comparado com o MAC original.

MAC fornece garantia de que a mensagem é inalterada e vem do remetente.

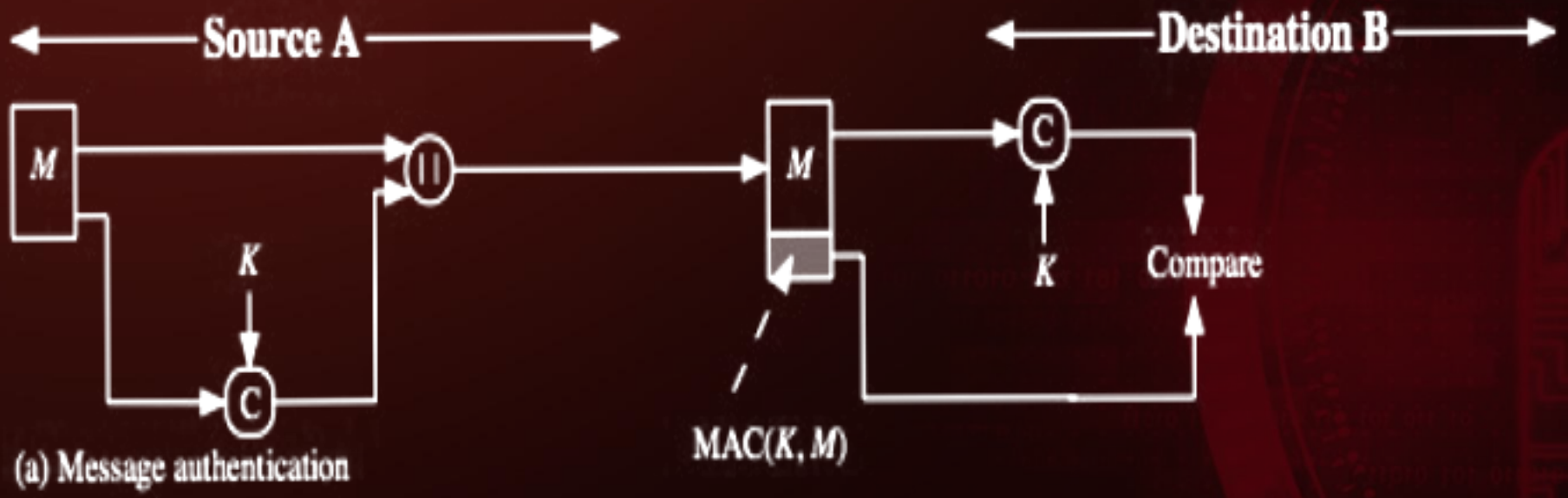
Ao contrário da função Hash, pode haver mais de um simples texto que pode gerar o mesmo MAC.

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

MAC é uma soma de verificação (checksum) criptográfica

- ✔ Condensa uma mensagem de comprimento variável M usando, uma chave secreta K para um autenticador de tamanho fixo
- ✔ É uma função de muitos para um
  - ✔ Potencialmente muitas mensagens têm o mesmo MAC
  - ✔ Porém, encontrar isso é muito muito difícil!

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS



CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

MAC e a criptografia podem prover autenticação

- ✔ **Porque muitas vezes apenas a autenticação é necessária**
  - **Muitas vezes também é necessário persistir a autenticação por mais tempo em relação à criptografia (por exemplo, para manipular um arquivo depois de autenticado em um sistema)**

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

Utilizamos um MAC baseado em hash porque essas funções são rápidas de calcular

Códigos de funções hash são amplamente divulgados

Precisamos de um hash incluindo uma chave junto com a mensagem

Originalmente o hash não tem chave e isso levou ao desenvolvimento do:

HMAC

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

HMAC

- ✔ É um código de autenticação de mensagens baseado em hash
- ✔ Desenvolvido por Mihir Bellare, Ran Canetti e Hugo Krawczyk em 1996, e especificado como padrão da Internet no RFC2104
- ✔ Utiliza a função de hash criptográfica combinada com uma chave secreta
- ✔ Utiliza qualquer função hash
  - ✔ MD5, SHA-1,Whirlpool, HMAC-MD5, HMAC-SHA1 etc.
  - ✔ Muitas delas utilizadas nos protocolos IPsec e TLS

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

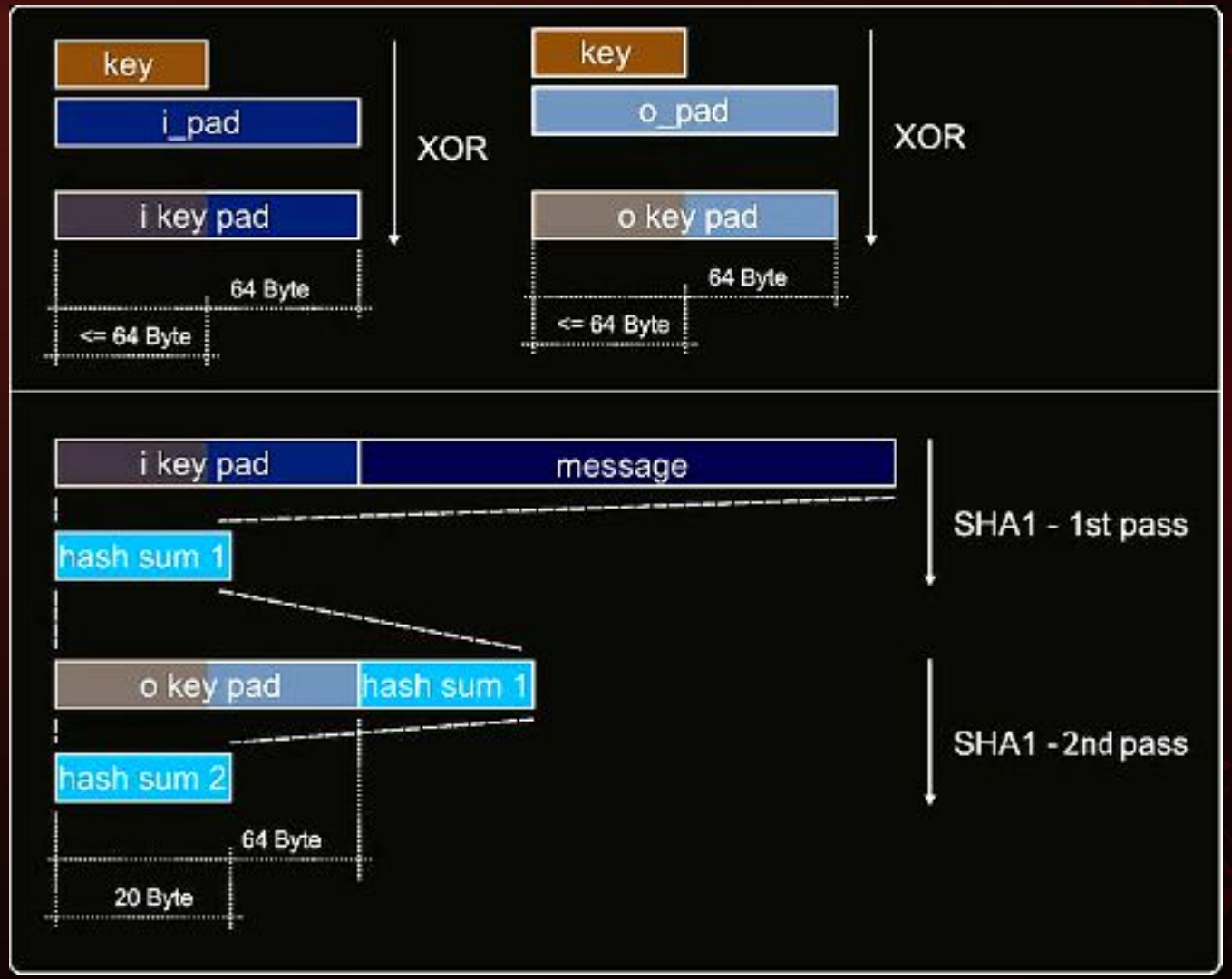
HMAC

Usa duas passagens de computação de hash

- ✔ A chave secreta é usada primeiro para derivar duas chaves - interna e externa.
- ✔ A **primeira passagem** do algoritmo produz um hash interno derivado da mensagem e da chave interna
- ✔ A **segunda passagem** produz o código HMAC final derivado do resultado do hash interno e da chave externa. Assim, o algoritmo fornece melhor imunidade contra ataques de extensão de comprimento.

CÓDIGO DE AUTENTICAÇÃO DE MENSAGENS

HMAC



CONCLUSÃO

Um Hash é usado para garantir a integridade dos dados

Um MAC garante integridade e autenticação

Um Hash recebe uma única entrada – uma mensagem e produz um resumo da mensagem

Um algoritmo MAC recebe duas entradas - uma mensagem, uma chave secreta e produz um MAC

Um algoritmo HMAC é simplesmente um tipo específico de algoritmo MAC que usa um algoritmo de hash internamente para gerar o MAC

REFERÊNCIAS

1. https://pt.wikipedia.org/wiki/HMAC#:~:text=O%20HMAC%20usa%20duas%20passagens,mensagem%20e%20da%20chave%20interna
2. Criptografia e Segurança de Redes: Princípios e Práticas - Willian Stallings

SEGURANÇA DA INFORMAÇÃO

Códigos de autenticação de mensagens e funções Hash