Funções Hash

- A função Hash é uma função não-inversível que aceita uma mensagem M de tamanho variável e produz uma saída de tamanho fixo
- A saída da função é chamada código Hash ou de sumário (digest) da mensagem (message digest)
  - h = H(M)
- Apesar de semelhante ao MAC, a função HASH não necessita de uma chave e o resultado é função somente da mensagem
- A função Hash fornece a capacidade de detecção de erro, pois a mudança em um um único bit da mensagem altera completamente o código hash
- Normalmente o código hash é adicionado à mensagem na origem. No destino o código hash é recalculado e caso seja igual ao enviado a mensagem é considerada autêntica.
- Como a função hash é pública, normalmente é necessário proteger o código hash através da cifragem do mesmo

Funções Hash Requisitos

- O objetivo de uma função hash é produzir algo semelhante a uma impressão digital de um arquivo, mensagem ou qualquer outro bloco de dados
- A fim de ser utilizada no processo de autenticação de mensagens a função H deve possuir as seguintes propriedades:
  - Pode ser aplicada a uma mensagem M de qualquer tamanho
  - Produz uma saída h de tamanho fixo
  - Deve ser computacionalmente fácil o cálculo de h = H(M)
  - É computacionalmente inviável calcular x, tal que, H(x) = h
    - propriedade conhecida unidirecional (característica de uma função injetora)
  - Dado o valor x, é computacionalmente inviável calcular y, tal que, sendo y ≠ x, H(y) = H(x)
    - propriedade conhecida como resistência fraca à colisão
  - É computacionalmente inviável encontrar um par (x,y) tal que, sendo y ≠ x, H(x) = H(y)
    - propriedade conhecida resistência forte à colisão

Funções Hash
Criptoanálise

- Ataque de força bruta
  - A resistência da função a este tipo de ataque depende unicamente do tamanho do código hash produzido
  - Caso o código tenha 64 bits, com 2^{64} tentativas é possível calcular o código hash
  - Para um código hash de n bits no geral tem-se que:

Propriedade	Tentativas
Unidirecional	2^n
Resistência fraca à colisão	2^n
Resistência forte à colisão	$2^{n/2}$

Funções Hash Criptoanálise

- Ataque de Aniversário
  - Existe porém um ataque chamado ataque de Aniversário, que é baseado no paradoxo do aniversário
    - Paradoxo do Aniversário: “Se 23 ou mais pessoas estão em uma sala, então a chance de que pelo menos duas façam aniversário na mesma data é de 50%”
- Ataque
  - Inicialmente o oponente possui uma mensagem válida com n bits
  - A partir desta mensagem válida o oponente produz $2^{n/2}$ mensagens válidas
  - Em seguida o oponente produz $2^{n/2}$ mensagens fraudulentas de seu interesse
  - Se os dois conjuntos forem comparados a probabilidade de encontrar um par que produz o mesmo código hash é maior que 50%
  - O código hash da mensagem válida é calculado. Porém o mesmo é concatenado a uma mensagem fraudulenta que no destino produzirá o mesmo código hash
- Quanto maior o código hash, menos o mesmo é susceptível a ataques

Funções Hash Algoritmos

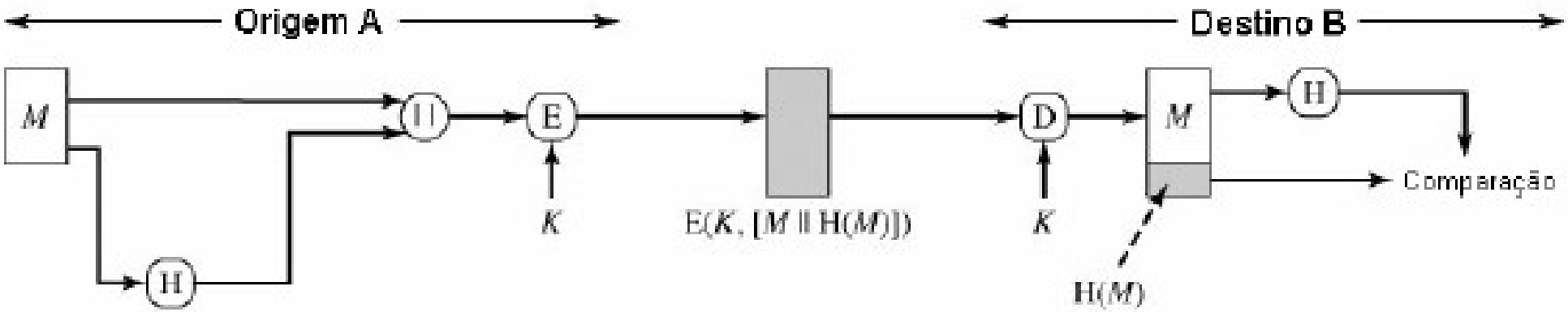
- Existem vários algoritmos para a criação de código hash, os mais bem aceitos atualmente são:

Algortimo	Tamanho Mensagem (bits)	Tamanho da Palavra (bits)	Tamanho Código Hash (bits)	Segurança (bits) - $2^{n/2}$
SHA-1	$< 2^{64}$	32	160	80
SHA-224	$< 2^{64}$	32	224	112
SHA-256	$< 2^{64}$	32	256	128
SHA-384	$< 2^{128}$	64	384	192
SHA-512	$< 2^{128}$	64	512	256
WHIRLPOOL	$<2^{512}$	64	512	256

- A família SHA (Secure Hash Algorithms) é um padrão proposto pelo NIST conhecido como Secure Hash Signature Standard (SHS) (FIPS PUB 180-2)
- A função WHIRLPOOL foi proposta por Vicent Rijmen e Paulo S. L. M. Barreto e foi recomendada pelo projeto NESSIE e é adotada pela ISO/IEC 10118-3:2004 (Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions)

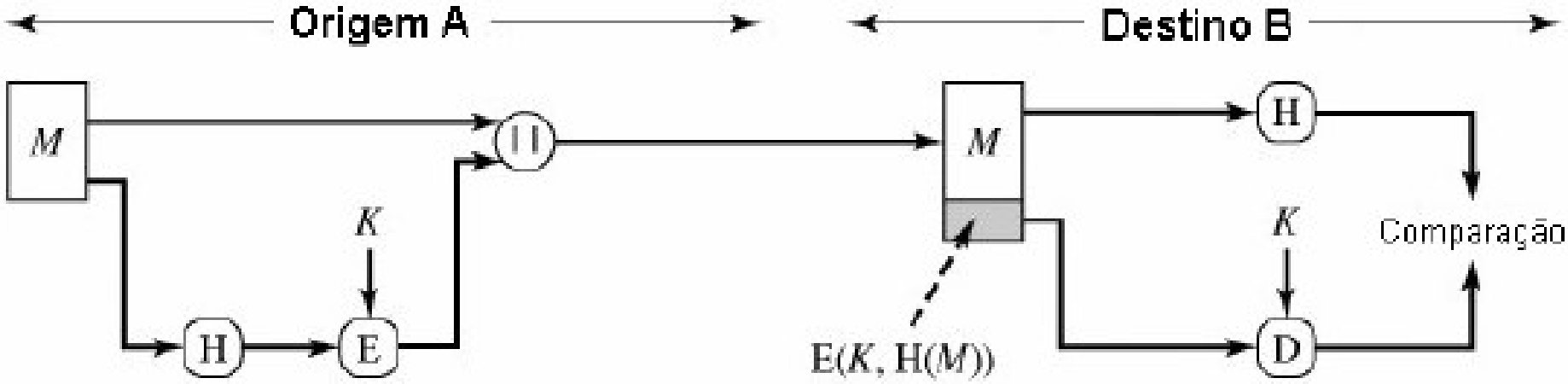
Funções Hash Funcionalidades

- Autenticação e Confidencialidade
  - Mensagem concatenada com o código hash é cifrada utilizando algoritmo simétrico
  - Como somente A e B possuem a chave mensagem é autêntica
  - Integridade é verificada com o código hash



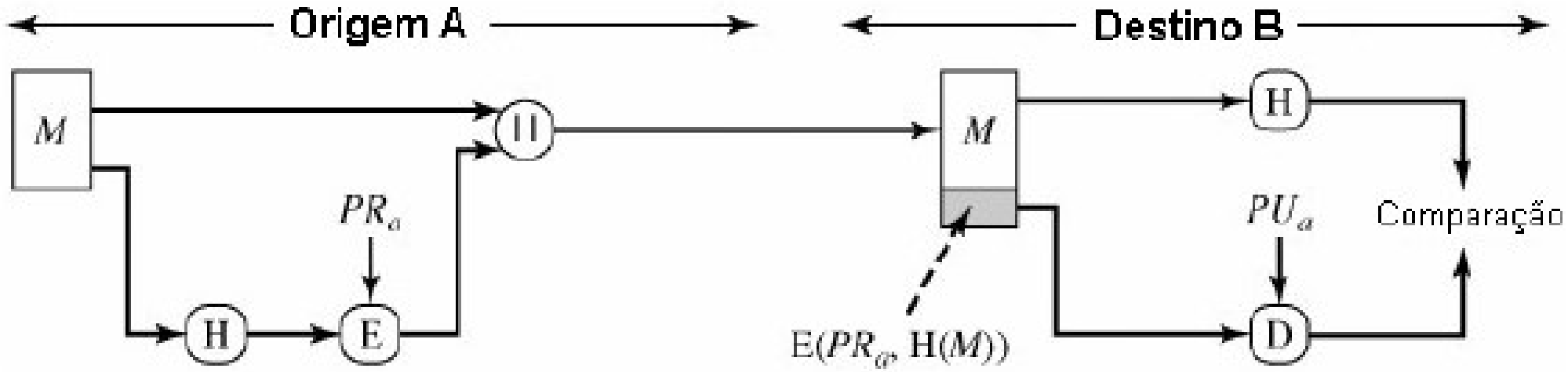
Funções Hash Funcionalidades

- Autenticação
  - Mensagem concatenada com o código hash
  - Porém somente a função Hash é cifrada utilizando um algoritmo simétrico
  - Como somente A e B possuem a chave mensagem é autêntica
  - Integridade é verificada com o código hash
  - Reduz a necessidade de processamento, porém não oferece confidencialidade
  - Na realidade E[K,H(M)] equivale ao MAC



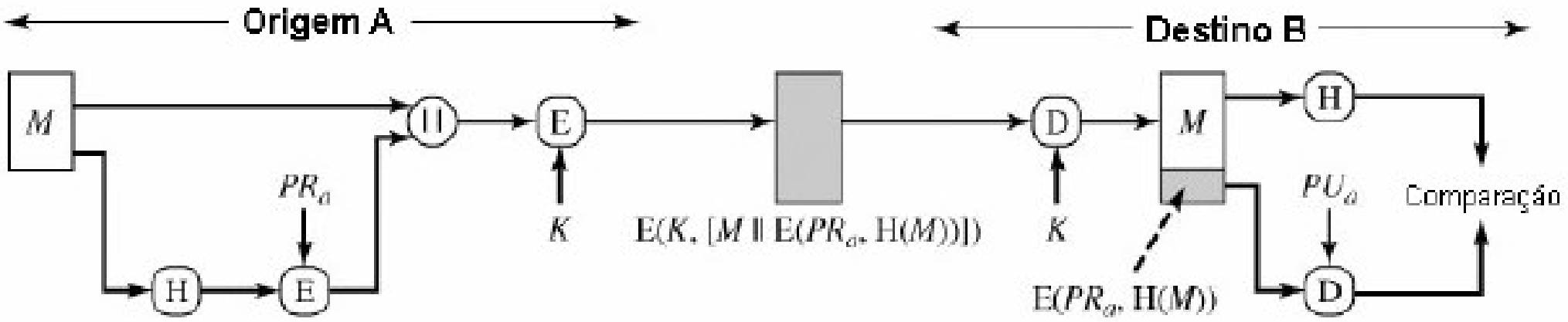
Funções Hash Funcionalidades

- Autenticação e Assinatura Digital
  - Somente o código hash é cifrado utilizando um algoritmo de chave pública
  - Fornece também uma assinatura digital, pois somente A poderia ter produzido o código hash cifrado
  - É a base para a técnica de assinatura digital
  - Reduz a necessidade de processamento, porém não oferece confidencialidade



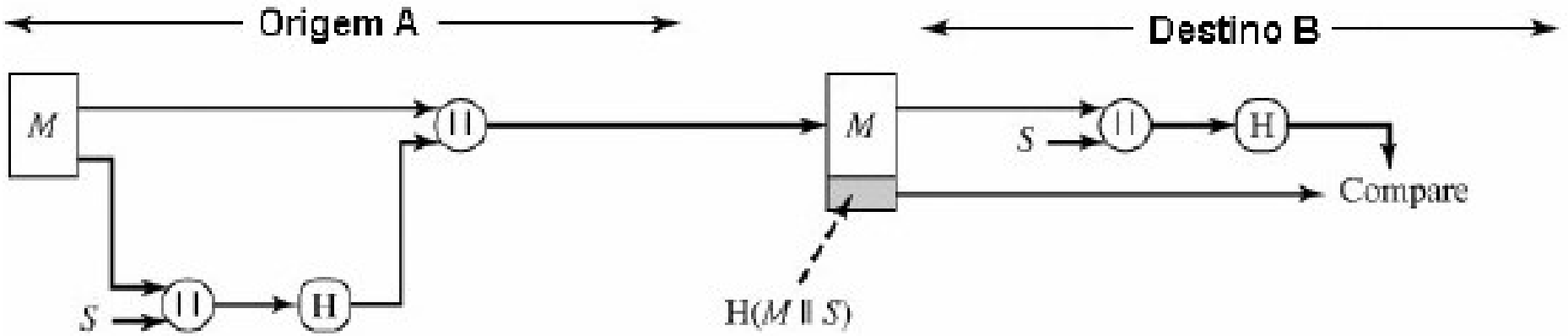
Funções Hash Funcionalidades

- Autenticação, Assinatura Digital e confidencialidade
  - Além do código hash, toda a mensagem é cifrada utilizando um algoritmo de chave pública
  - Fornece também uma assinatura digital, pois somente A poderia ter produzido o código hash cifrado



Funções Hash Funcionalidades

- Autenticação
  - Neste caso não utilizada cifragem
  - É necessário que ambas as partes conheçam um valor secreto S
  - Na origem é realizado um hash do valor resultante da concatenação de M com o valor S
  - Como B conhece o valor S é possível calcular o hash no destino e comparar com o hash recebido



Funções Hash Funcionalidades

- Autenticação e Confidencialidade
  - É necessário que ambas as partes conheçam um valor secreto S
  - Na origem é realizado um hash do valor resultante da concatenação de M com o valor S
  - O valor resultante é cifrado. Neste caso existe também a confidencialidade
  - Como B conhece o valor S é possível calcular o hash no destino e comparar com o hash recebido