Segurança da Informação

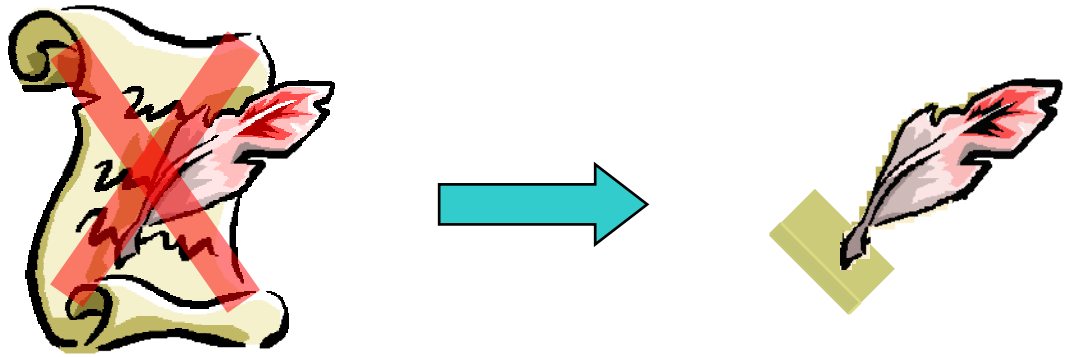
Resumos Criptográficos
(Funções de Hash – Introdução)

Funções de Hash

- AKA *resumos criptográficos*.
- Redundâncias anexadas a mensagens com o propósito de detectar alterações.
- Dependem exclusivamente da mensagem (sem chave):

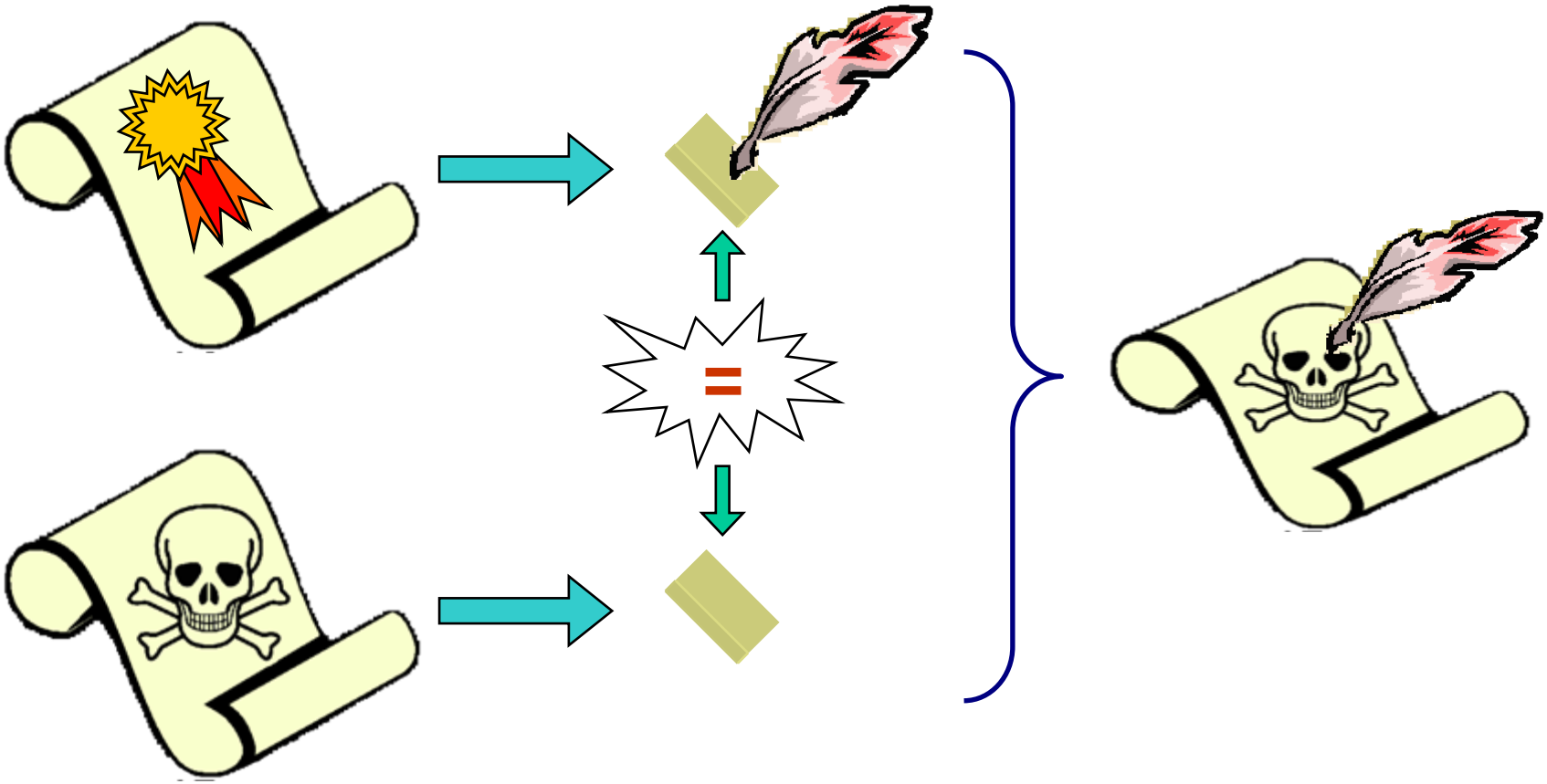
Resumos Criptográficos

- Assinaturas digitais *não* são aplicadas ao *conteúdo* de documentos eletrônicos, mas a *resumos* do conteúdo.
- Motivo: algoritmos de assinatura são muito mais *lentos* que funções de resumo (*hash*).



- Problemas?

Resumos Criptográficos



Propriedades Fundamentais

- (*Resistência a primeira inversão*) Dado um resumo R, é *inviável* encontrar uma mensagem M tal que $R = H(M)$.

- (*Resistência a segunda inversão*) Dado um resumo R e uma mensagem M_1 tal que $R = H(M_1)$, é *inviável* encontrar uma outra mensagem $M_2 \neq M_1$ tal que $R = H(M_2)$.

- (*Resistência a colisões*) É *inviável* encontrar duas mensagens M_1 e M_2 tais que $H(M_1) = H(M_2)$.

Propriedades Fundamentais