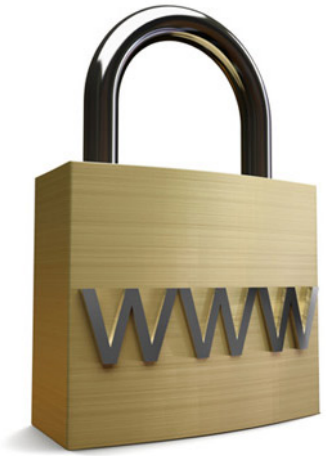
Inatel
Instituto Nacional de Telecomunicações

www.inatel.br

Segurança em Redes de Telecomunicações

SEGURANÇA DE REDES

Prof. Dr. Guilherme Pedro Aquino
guilhermeaquino@inatel.br

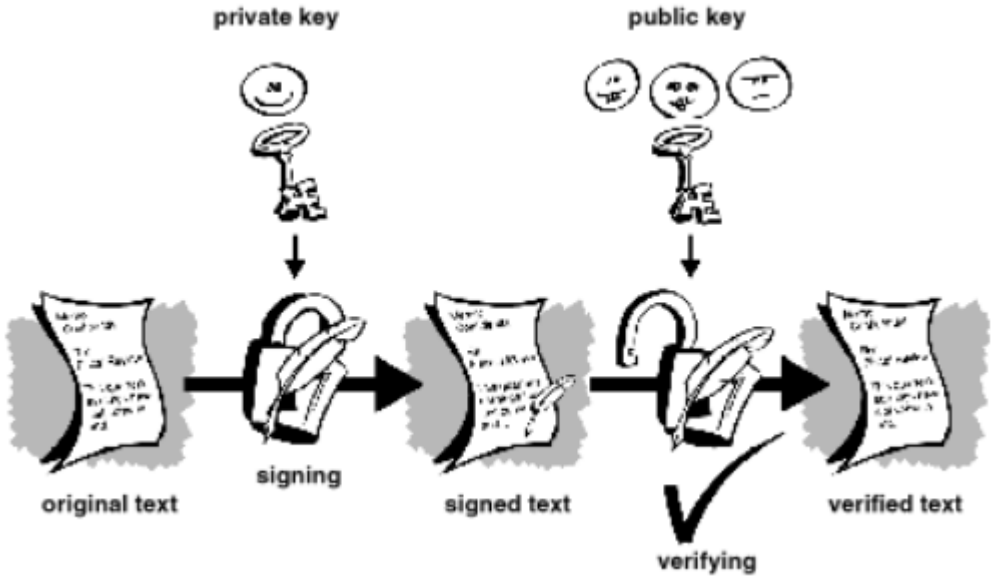


INATEL
Av. João de Camargo, 510
Santa Rita do Sapucai - MG
Tel: (35) 3471-9200

Assinatura Digital

- A autenticação de mensagem protege duas pessoas contra uma terceira. Porém ela não protege as duas partes uma da outra.

- A figura abaixo ilustra o uso do criptossistema de chave pública para prover autenticação. A autenticação é feita através da assinatura digital.



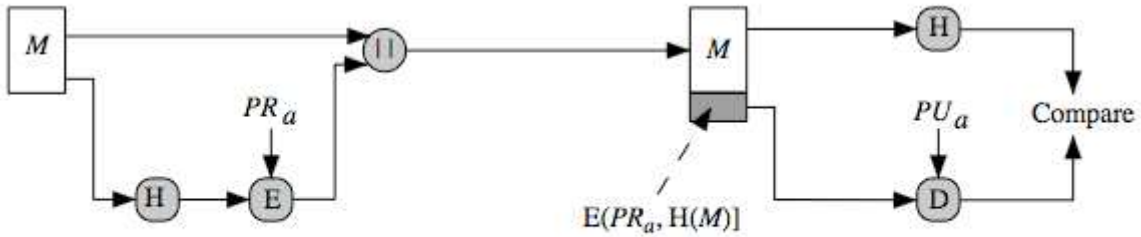
Criptografia e Assinatura Digital

- É possível oferecer confidencialidade e autenticidade com o uso duplo do esquema de chave pública:

$$Z = E(PU_b, E(PR_a, X))$$
$$X = D(PU_a, D(PR_b, Z)).$$

Criptografia e Assinatura Digital.

- Técnica para assinatura digital.
  - A assinatura digital pode ser feita criptografando a mensagem inteira com a chave privada do emissor, ou criptografando um código hash da mensagem com a chave privada do emissor.
  - A segunda opção é mais rápida em termos computacionais.



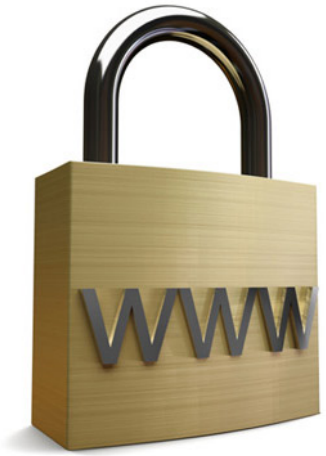
(a) RSA Approach

Inatel

Instituto Nacional de Telecomunicações

www.inatel.br

OBRIGADO.



INATEL Competence Center
Av. João de Camargo, 510
Santa Rita do Sapucai - MG
Tel: (35) 3471-9330