UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE COMPUTAÇÃO

Exercício 01 - Recuperação de mensagens - Tópicos em Redes de Computadores 01

Aluno: Adriano Ricardo Ruggero
RA: 144659
Professor: Edmundo R. M. Madeira

Resumo

Para este cenário (*e-mail* com confidencialidade, autenticação e integridade da mensagem), mostrar os passos do **receptor** para obter a mensagem m

1 Exercício 01

Resposta: para que o receptor **B** possa obter a mensagem m enviada por **A** (emissor) neste cenário proposto, é necessário que ele siga os passos abaixo descritos:

- **B** recebe uma mensagem de **A**. Esta mensagem é formada pela concatenação de um ”pacote” (encriptado com uma chave simétrica, contendo a mensagem m concatenada com o *hash* da mensagem m, *hash* este que é assinado digitalmente com a chave privada de **A**) e a chave simétrica utilizada para a encriptação do pacote, encriptada com a chave pública de **B**;
- **B** utiliza sua chave privada para extrair a chave de sessão utilizada por **A** para a encriptação do ”pacote” com chaves simétricas. A chave de sessão fora previamente encriptada pelo emissor utilizando a chave pública de **B**, o que, em teoria, permite que apenas **B** (detentor da chave privada correspondente) possa decriptá-la;
- De posse da chave de sessão utilizada por **A**, **B** pode decriptar o "pacote"enviado por **A**;
- Com o "pacote” decriptado, **B** pode agora verificar a assinatura digital de A, utilizando a chave pública de **A**;
- **B** utiliza a mesma função de *hash* utilizada por **A** na mensagem m decriptada por ele, e compara o resultado com o *hash* recebido concatenado com a mensagem. Caso sejam ”iguais”, **B** saberá que não houve alteração em m.

Desta forma, a assinatura do *hash* da mensagem m garante autenticaçao do remetente, a verificação do *hash* garante integridade da mensagem e a encriptação com a chave de sessão garante confidencialidade. Como a troca da chave de sessão entre o remetente e o receptor não pode ocorrer em um canal seguro, é utilizado o sistema de chaves públicas para encriptação da chave de sessão.

Referências

[1] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach.* Addison-Wesley Publishing Company, USA, 5th edition, 2009.