Equações Criptológicas

Convenções básicas:

E – Operação de encriptar
D – Operação de decifrar
{,[,(,),],} – usados nesta ordem para separar as operações
|| - Concatenado com
$K_{pub(A)}$ – Chave pública de A
$K_{priv(A)}$ – Chave privada de A
K_{sec} – Chave secreta
K_S – Chave de sessão
K_A – Chave Master de A
M – Mensagem em texto claro
X – Criptograma
HASH – função de hash

Exemplos:

A → B - $E\ [K_{pub(B)}\ (K_{sec}\ )]\ ||\ E\{K_{priv(A)}\ [HASH\ (M)]\}\ ||\ E[K_{sec}(M)]$
Leitura:
A envia a B a chave secreta (simétrica) encriptada com a chave pública de B. Concatenado a isso é enviado o HASH da mensagem sigilosa, encriptada com a chave privada de A. É concatenado também o criptograma criado pela encriptação da mensagem original com a chave secreta escolhida por A.

B $D\ \{\ K_{priv(B)}\ [K_{pub(B)}\ (K_{sec}\ )\ \}\ \rightarrow\ K_{sec}$
$D\ \{\ K_{sec}\ [K_{sec}(M)]\}\ \rightarrow\ M$
$D\ \{\ K_{pub(A)}\ \{K_{priv(A)}\ [HASH\ (M)]\}\}\ \rightarrow\ HASH\ (M)$
$HASH\ (M)\ \leftrightarrow\ HASH\ (M)$

Leitura: B decifra com a sua chave privada o criptograma criado pela encriptação da chave secreta com a chave pública de B, obtendo-a. Com a chave secreta, obtém a mensagem sigilosa, decifrando o criptograma correspondente. Por fim, verifica a autenticidade da mensagem, decifrando o HASH da mensagem encriptado com a chave privada de A, através da chave pública de A, e comparando em seguida com o HASH calculado em cima da mensagem recebida.

Agora, interprete as equações:

a) CA → A - $E[K_{priv(CA)}\ (K_{pub(B)}\ )]$
b) A → B - $E\{K_{priv(A)}\ [HASH(M)]\}\ ||\ M$
c) A → B - $E[\ K_{priv(CA)}\ (K_{pub(A)}\ )\ ]$

Respostas:

a) A Autoridade Certificadora, responsável pela guarda e autenticidade de certificados digitais que contém as chaves públicas dos usuários, envia criptografado com a sua própria chave privada a chave pública de um outro usuário.
b) O usuário A envia para B encriptado com a sua própria chave privada o hash da mensagem M, concatenado com a própria mensagem. Ao receber, B calcula o hash de M e compara com o recebido, após decriptografado com a chave pública de B, com a intenção de comprovar sua autenticidade.
c) A envia para B a sua própria chave pública, encriptada com a chave da autoridade certificadora.

Documento revisado em 12 de abril de 2011