Criptografia Aplicada

LESI / LMCC

Exame da 2a Chamada – 27 de Janeiro 2007

Questão 1 Um fabricante de alarmes para automóveis contratou-o para resolver o seguinte problema: uma seguradora apenas aceita alarmes para os quais seja garantido criptograficamente que apenas é possível utilizar um único controlo remoto para activar/desactivar o alarme. O fabricante acha que a melhor maneira de resolver o problema é cifrar as comunicações entre cada controlador e o respectivo sistema utilizando AES em modo CBC, ou a cifra RC4.

1. Descreva as características dos sistemas sugeridos pelo fabricante.
2. Comente as sugestões do fabricante. Concorda com a sua opinião? A sua resposta dependeria do esquema de cifra a utilizar?
3. O que recomendaria ao fabricante? Esboce um sistema alternativo com base nas primitivas criptográficas que estudou.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2a Chamada – 27 de Janeiro 2007

Questão 2 Um sistema de base de dados implementa um mecanismo de controlo de acessos com base em assinaturas digitais RSA. Dado o carácter sensível da informação armazenada na BD, os pedidos e as respectivas respostas são também cifrados com as chaves públicas para que os utilizadores não controlem os acessos uns dos outros. São propostas duas soluções para as trocas de informação entre um utilizador A, com par de chaves $(\texttt{Pub}_\texttt{A}, \texttt{Priv}_\texttt{A})$, e a BD, com par de chaves $(\texttt{Pub}_\texttt{BD}, \texttt{Priv}_\texttt{BD})$:

- O utilizador envia

  $$E_{\texttt{RSA}}(\mathit{pedido}, \texttt{Pub}_\texttt{BD}), S_{\texttt{RSA}}(E_{\texttt{RSA}}(\mathit{pedido}, \texttt{Pub}_\texttt{BD}), \texttt{Priv}_\texttt{A})$$

  ou seja, o pedido cifrado e uma assinatura deste criptograma.

- O utilizador envia

  $$E_{\texttt{RSA}}(\mathit{pedido}, S_{\texttt{RSA}}(\mathit{pedido}, \texttt{Priv}_\texttt{A}), \texttt{Pub}_\texttt{BD})$$

  ou seja, o pedido e a sua assinatura cifrados num único criptograma.

Em ambos os casos a BD responde com $E_{\texttt{RSA}}(\mathit{dados}, \texttt{Pub}_\texttt{A})$.

1. Considere que o algoritmo RSA é utilizado com padding determinístico. Uma destas utilizações tem diversas vulnerabilidades. Identifique-as.

2. Retire conclusões gerais sobre a combinação de primitivas de assinatura digital com cifras.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2a Chamada – 27 de Janeiro 2007

Questão 3 A utilização de cifras por blocos implica geralmente a introdução de *padding*.

1. A aplicação criteriosa deste tipo de técnica pode permitir também detectar quebras de integridade. Justifique.

2. Os ataques por Code-Book são um problema para um dos modos de utilização de cifras por blocos que estudou na aulas de CA. Descreva esse modo de funcionamento e explique como a utilização de *padding* pode proteger contra este tipo de ataques.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2a Chamada – 27 de Janeiro 2007

Questão 4 Recorde o que estudou sobre certificados X.509.

1. Existe algum inconveniente por se publicar a chave privada de um certificado que acaba de expirar? Justifique a sua resposta distingindo os cenários onde o certificado é utilizado para assinaturas digitais e para cifras.

2. Pode uma CA emitir um certificado com uma validade superior à validade do seu próprio certificado? Justifique, indicando qual o impacto na utilização desse(s) certificado(s).

3. Admita que um certificado intermédio de uma cadeia de certificação foi incluído numa CRL num dado instante (e.g. 00:00-27/01/2007GMT). Qual o estado de validade dos certificados previamente emitidos por essa CA? Fará sentido inclui-los também numa CRL? Justifique a sua resposta.

Nome:_____ **Número:**_____ **Curso:**_____

Criptografia Aplicada

LESI / LMCC

Exame da 2a Chamada – 27 de Janeiro 2007

Questão 5 Considere o sistema PGP (Pretty Good Privacy).

1. Descreva o processo de troca de uma mensagem cifrada entre dois utilizadores. Que denominação genérica se dá a essa técnica?

2. Explique porque é que todos os certificados PGP são auto-assinados, fazendo um paralelo com o X.509.

Nome:_____ **Número:**_____ **Curso:**_____