Criptografia Aplicada

LESI / LMCC

Exame de Recurso – Fevereiro de 2008

ATENÇÃO: Quem estiver a realizar o teste referente à primeira parte da matéria deve responder às questões assinaladas com "1"; à segunda parte com "2" e a toda a matéria com "T". Melhorias de notas devem sempre responder a toda a matéria (T).

Questão 1 – (1+T)

1. Considere a utilização de uma cifra por blocos no modo CBC em que o vector de inicialização é transmitido em claro.

   (a) Qual é o impacto, ao decifrar uma mensagem, da alteração de um *bit* em: *(i)* o vector de inicialização; *(ii)* um bloco de criptograma intermédio.

   (b) Com base na resposta à alínea anterior, discuta a adequação da solução proposta em termos de segurança (propondo alternativas se entender apropriado).

2. Em que consiste um *Message Authentication Code*? Que propriedades pretende estabelecer?

3. Uma forma de codificar um MAC consiste em fazer uso de uma função apropriada h da seguinte forma:

   $$\mathrm{MAC}(k, M) = \mathsf{h}(k \cdot \mathsf{h}(M \cdot k))$$

   onde $\cdot$ denota a concatenação. Justifique a adequação desta solução explicitando quais são as premissas e como é que se estabelecem as propriedades pretendidas.

4. As *Engines Classes* do JCA/JCE disponibilizam aos programadores "serviços" criptográficos. Forneça exemplos de 4 dessas classes, indicando a respectiva funcionalidade.

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

Criptografia Aplicada

LESI / LMCC

Exame de Recurso – Fevereiro de 2008

ATENÇÃO: Quem estiver a realizar o teste referente à primeira parte da matéria deve responder às questões assinaladas com "1"; à segunda parte com "2" e a toda a matéria com "T". Melhorias de notas devem sempre responder a toda a matéria (T).

Questão 2 – (2+T)

1. O certificados X509 são provavelmente o aspecto mais visível da utilização da criptografia nas utilizações correntes (correio electrónico, navegação web, etc.)

   (a) Que problema é que pretendem resolver?

   (b) No que é que consistem e porque é que permitem ultrapassar as dificuldades apontadas na alínea anterior?

   (c) Faz sentido um certificado ser auto-assinado? Em que circunstâncias e com que objectivos?

   (d) Descreva a utilização de certificados no envio e recepção de *emails* assinados e cifrados.

   (e) Refira outra aplicação criptográfica onde estejam envolvidos certificados X509. Descreva de forma sucinta essa aplicação e qual a utilização que faz dos certificados.

2. A qualidade dos números aleatórios é um factor determinante na segurança das técnicas criptográficas. Para confirmar esta afirmação, relembre a cifra *El-Gamal* estudada no curso: dado um primo p e um gerador g de $Z_p^\star$;

   - **Inicialização**: gera um número x $(0 < x < p)$ e faz-se $y = g^x \ [p]$. A chave privado é formado pelo triplo $\langle x, g, p\rangle$ e a chave pública pelo triplo $\langle y, g, p$.
   - **Cifrar**: gera-se um número aleatório r $(0 < r < p)$, sendo o criptograma formado pelo par $\langle c_1, c_2\rangle = \langle g^r, m * y^r\rangle$.
   - **Decifrar**: dado um criptograma $\langle c_1, c_2\rangle$, a mensagem é recuperada calculando $c_2/(c_1^x) \ [p]$.

   Mostre como um adversário poderá atacar a cifra se puder prever qual o número aleatório utilizado na operação de cifra.

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

Criptografia Aplicada

LESI / LMCC

Exame de Recurso – Fevereiro de 2008

ATENÇÃO: Quem estiver a realizar o teste referente à primeira parte da matéria deve responder às questões assinaladas com "1"; à segunda parte com "2" e a toda a matéria com "T". Melhorias de notas devem sempre responder a toda a matéria (T).

Questão 3 – (1)

1. No curso foi estudada a cifra *One Time Pad* (OTP) como um exemplo de uma cifra incondicionalmente segura.
   (a) Explique o princípio de funcionamento dessa cifra.
   (b) O que significa a afirmação "a cifra OTP é incondicionalmente segura"?
   (c) Apesar do referido na alínea anterior, a cifra OTP é reconhecidamente inapropriada em utilizações correntes da criptografia. Porquê?
2. O que é uma *função de hash criptográfica*? Que propriedades são esperadas nessas funções?
3. O que caracteriza uma cifra sequencial auto-sincronizável? Em que situações aconselharia a sua utilização?

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

Criptografia Aplicada

LESI / LMCC

Exame de Recurso – Fevereiro de 2008

ATENÇÃO: Quem estiver a realizar o teste referente à primeira parte da matéria deve responder às questões assinaladas com "1"; à segunda parte com "2" e a toda a matéria com "T". Melhorias de notas devem sempre responder a toda a matéria (T).

Questão 4 – (2)

1. Relembre a primitiva criptográfica RSA estudada no curso.

   - **Inicialização**: geram-se dois números primos p e q ($n = p \cdot q$), e um inteiro e tal que $gcd(e, \varphi(n)) = 1$. Calcula-se d tal que $e \cdot d = 1$ $[\varphi(n)]$.
   - **Cifrar**: $c = m^e$ $[n]$ (com $0 \leq m < n$).
   - **Decifrar**: $m = c^d$ $[n]$.

   (a) A segurança do RSA está intimamente relacinada com a dificuldade de se factorizarem números grandes. Explique como é que, conhecendo a factorização de n, se pode atacar o RSA.

   (b) Um problema associado à utilização directa da primitiva RSA na implementação de uma cifra assimétrica é a sua *natureza determinística*. Explique como tirar partido dessa característica num ataque à cifra e como é que técnicas como RSA-OAEP ultrapassam esse problema?

2. As *assinaturas digitais* e os *message authentication codes* foram duas das técnicas estudadas no curso. Descreva as similaridades e as diferenças que é possível estabelecer entre essas técnicas (nível das propriedades que lhes associamos).

3. O acordo de chaves é um ingrediente importante na utilização corrente da criptografia.

   (a) Descreva o protocolo de acordo de chaves *Diffie&Helman* e justifique a sua segurança perante um adversário passivo.

   (b) Como é que protocolo *Station-to-Station* ultrapassa as limitações do acordo de chaves *Diffie&Helman* perante adversários activos? Justifique.

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