Segurança
1º Semestre, 2012/13

1º Teste
7 de Novembro de 2012

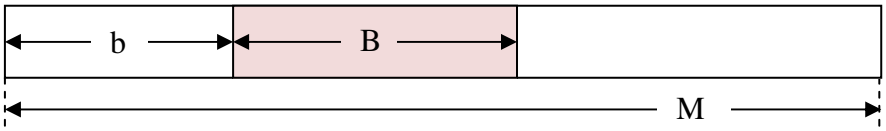
- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 1h30.

1. Considere os ataques por esmagamento da pilha (*stack smashing attack*) usando C.
   a. Explique qual é a vulnerabilidade que exploram.
   b. Indique por que razão não são possíveis com Java.

2. Um ataque de injeção de procuras SQL (*SQL injection attack*) explora um de terminado tipo de vulnerabilidade. Explique:
   a. Em que consiste essa vulnerabilidade.
   b. Como se pode eliminar essa vulnerabilidade.

3. Uma cifra contínua não deve ser usada com a mesma configuração inicial (VI e chave) para cifrar mensagens diferentes. Explique porquê.

4. Considere o modo de cifra CTR (*Counter Mode*). Explique:
   a. Como funciona.



   b. Como faria para decifrar B octetos de uma mensagem M, a partir do deslocamento b, com uma cifra n-bit CTR?

5. Indique as propriedades que distinguem as funções de síntese (*digest*) de outras funções de dispersão (*hashing*).

6. Um MAC (*Message Authentication Code*) pode ser calculado com uma cifra por blocos em modo CBC da mensagem (método conhecido como DES-MAC). Explique:
   a. Por que razão não se pode considerar que uma qualquer mensagem cifrada com uma cifra por blocos em modo CBC tem implicitamente um MAC?
   b. Como se poderia modificar trivialmente a mensagem para resolver esse problema (i.e. passar a conter implicitamente um MAC)?

7. Explique por que razão as cifras assimétricas, tal como a RSA, são realizadas sobre valores que incluem (i) o conteúdo que se quer efetivamente cifrar, (ii) uma marca constante e (iii) um valor aleatório.

8. Explique por que razão a validação de assinaturas digitais implica a existência de certificados de chave pública.

9. Considere a gestão de chaves públicas. Explique:
   a. O que é uma cadeia de certificação?
   b. Em que consiste exatamente uma raiz confiável de uma cadeia de certificação?

10. Considere o problema da revogação de um certificado de chave pública. Explique:
    a. A diferença entre uma CRL (*Certificate Revocation List*) e uma delta-CRL.
    b. A relação entre uma CRL e o serviço OCSP (*Online Certificate Status Protocol*).