Segurança
1º Semestre, 2010/11

1º Teste
9 de Novembro de 2010

- Todas as perguntas têm a mesma cotação.
- A duração total é de 1 hora e 30 minutos

1. Considere o conceito de ataque por esmagamento da pilha (*stack smashing attack*):
    a. Explique qual é a vulnerabilidade da linguagem C que é explorada para a sua execução.
    b. Indique duas formas de detectar a sua ocorrência durante a execução de uma aplicação.
2. Explique o modelo geral de funcionamento de uma cifra contínua, incluindo operações de cifra e decifra, e complemente a sua explicação com um diagrama.
3. O CFS (*Cryptographic File System*) usa uma combinação de modos de cifra, nomeadamente ECB (*Electronic Code Book*) e OFB (*Output Feedback*). Explique porquê.
4. Explique por que razão o modo de cifra CTR (*Counter Mode*) tem acesso aleatório uniforme, o modo de cifra OFB (*Output Feedback*) normalmente não o possui e o modo de cifra CFB (*Cipher Feedback*) só o possui na decifra.
5. Explique o modelo geral de aplicação de uma cifra assimétrica (e.g. RSA) à comunicação segura (confidencial) entre duas entidades.
6. Considerando as 3 propriedades que as boas funções de síntese devem possuir, duas delas são críticas para a sua exploração na geração e validação de assinaturas digitais. Indique:
    a. Quais são essas duas propriedades?
    b. Porque são críticas?
7. Considere o conceito de MAC (*Message Authentication Code*):
    a. Qual o fim a que se destina um MAC?
    b. Indique duas formas alternativas de o calcular.
8. Considere o conceito de hierarquias de certificação. Explique:
    a. Em que consistem?
    b. Qual é a relevância, nas mesmas, dos certificados raiz auto-assinados?
9. Explique qual é a mais-valia da utilização do Cartão de Cidadão para a implantação de uma infra-estrutura de geração e validação de assinaturas digitais qualificadas realizadas por cidadão Portugueses?
10. Considere o conceito de tempo de vida de um par de chaves assimétricas. Indique:
    a. Que mecanismos existem para controlar este tempo de vida?
    b. Descreva de modo sumário as políticas que podem governar cada um dos mecanismos.