# Segurança
# 1º Semestre, 2008/09

## 1º Teste
## 11 de Novembro de 2008

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

1. No âmbito dos sistemas computacionais:
   a. Explique a relação que existe entre vulnerabilidades e riscos.
   b. Quais as vantagens e desvantagens de eliminar riscos em vez de eliminar vulnerabilidades.
2. Considere o sistema de protecção de endereços de retorno com canários do StackGuard e a protecção de memória de um *stack* proibindo execução. Explique a complementaridade entre estes dois mecanismos de protecção.
3. Os modos de cifra com realimentação (e.g. CBC) não são apropriados para cifrar conteúdos de ficheiros em sistemas de ficheiros seguros. Mas os modos de cifra sem realimentação (e.g. ECB) também não são só por si apropriados. Explique porquê em ambos os casos.
4. Compare os modos de cifra por blocos CBC e OFB quanto aos seguintes aspectos:
   a. Paralelização (considere separadamente cifras e decifras).
   b. Pré-processamento (para aumentar a eficiência).
5. O modo de cifra PCBC (*Propagating Cipher Block Chaining*) chegou a ser usado porque supostamente permitiria uma melhor propagação de erros resultantes de criptogramas errados. O PCBC é semelhante ao CBC mas tem uma realimentação adicional na cifra e decifra:
   $C_i = E(P_i \oplus P_{i-1} \oplus C_{i-1})$
   $P_i = D(C_i) \oplus P_{i-1} \oplus C_{i-1}$.
   No entanto, se se trocarem dois blocos consecutivos do criptograma ($C'_i = C_{i+1}$ e $C'_{i+1} = C_i$), a decifra do bloco seguinte $C'_{i+2} = C_{i+2}$ já não evidencia qualquer erro. Demonstre esse facto matematicamente.
6. Um MAC (*Message Authentication Code*) pode ser calculado de várias maneiras a partir de uma mensagem e de uma chave secreta partilhada. Indique:
   a. Uma que faça uso apenas de de operações de cifra e somas módulo 2 (XOR).
   b. Uma que faça uso apenas de funções de resumo.
7. Considere as operações de compressão e cifra. Indique, justificadamente, as vantagens e desvantagens relativas da sua aplicação pela ordem indicada ou pela ordem inversa.
8. A cifra de conteúdos armazenados pode ser feita grosso modo a três níveis: aplicacional, sistema de ficheiros e dispositivo. Discuta vantagens e desvantagens de actuar a cada um deste níveis em relação aos seguintes aspectos:
   a. Transparência das operações de cifra e decifra para o utente.
   b. Transparência das operações de cifra e decifra para aplicações.
   c. Noção (ou *feedback*) que o utente tem do que está ou não está cifrado.
9. Considere os sistemas de ficheiros seguros CFS e EFS. Compare, justificando, os dois quanto aos seguintes aspectos:
   a. Protecção de conteúdos de ficheiros em trânsito entre clientes e servidores.
   b. Capacidade de partilha de ficheiros cifrados entre diferentes utilizadores.
10. Uma das principais funcionalidades de um *smart card* é a concretização de assinaturas digitais ou de autenticação com criptografia assimétrica. Explique:
    a. Porque razão tal acontece.
    b. Que características deverá ter o *smart card* para que tais operações sejam isentas de risco.