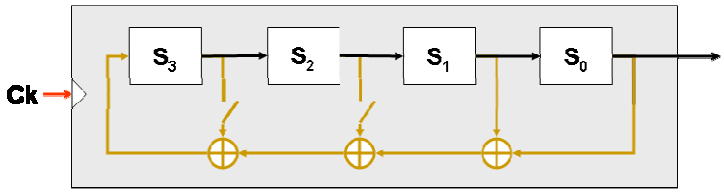
Segurança
1º Semestre, 2010/11

1º Teste
25 de Outubro de 2011

- Todas as perguntas têm a mesma cotação.
- A duração total do teste é de 1h30 (10 perguntas).

1. Considere os ataques por esmagamento da pilha (*stack smashing attack*) usando C.
   a. Explique com pormenor como atuam.
   b. Indique como podem ser detetados com canários.

2. Considere o LFSR da figura abaixo.
   a. Escolha um valor inicial não nulo e determine o período da sequência gerada pelo LFSR para esse valor inicial concreto.
   b. Indique, justificando, se o polinómio de realimentação usado é ou não primitivo.



3. O modo de cifra CTR (*Counter*) permite a concretização de uma cifra contínua com capacidade de acesso aleatório uniforme. Explique:
   a. Em que consiste esta característica?
   b. Como é que o modo CTR consegue ter essa característica?

4. As funções de síntese (*digest*) devem dificultar a descoberta de um segundo texto que produza a mesma síntese de outro texto. Explique, de forma pormenorizada, a relevância deste requisito para a segurança das assinaturas digitais.

5. Um MAC (*Message Authentication Code*) é um meio de autenticação de mensagens. Explique:
   a. Que semelhanças possui, ou não possui, com as assinaturas digitais?
   b. Como pode ser concretizado apenas com uma função de cifra em modo CBC (*Cipher Block Chaining*)?

6. A segurança da cifra RSA depende da dificuldade de cálculo de logaritmos discretos de números de grande dimensão. Explique porquê, recorrendo às expressões matemáticas que descrevem a operação do RSA.

7. As assinaturas digitais são normalmente acompanhadas por um ou mais certificados de chave pública. Indique:
   a. Que certificados são esses?
   b. Por que razão eles são enviados junto com a assinatura?

8. Considere o conceito de certificado de chave pública X.509. Explique:
   a. Para que servem estes certificados?
   b. Quem produz estes certificados?

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

10. Considere o problema da revogação de um certificado de chave pública. Explique:
    a. O que é uma lista de certificados revogados (*Certificate Revocation List*, CRL)?
    b. Quem a deve usar?