Primeira parte do exame da época normal de Criptografia Aplicada

11 de janeiro de 2024 **14h00m – 15h30m/17h00m**

1.0 **1:** Explique qual é o princípio fundamental de funcionamento das cifras contínuas, ou de fluxo (*stream*).

1.0 **2:** Os algoritmos de síntese (*digest*), como o MD5, SHA-1, SHA2, etc., são funções de dispersão que possuem 3 propriedades que as distinguem de outras funções de dispersão. Descreva com pormenor cada uma dessas propriedades.

1.0 **3:** Imagine que comunica com um conjunto de interlocutores de forma confidencial, usando para o efeito as chaves públicas dos destinatários. Porém, a cifra com chaves públicas é normalmente bastante menos eficiente que uma cifra simétrica, pelo que normalmente é substituída por uma cifra designada por híbrida ou mista. Explique como funciona este tipo de cifra.

1.0 **4:** HMAC (*Hashed-based Message Authentication Code*) é uma forma parametrizável de cálculo de um MAC (*Message Authentication Code*). Explique:

a) O que é um MAC?

b) Para que serve um MAC?

c) Como funciona o HMAC?

1.0 **5:** Imagine que tem um conjunto de ficheiros aos quais quer aplicar, individualmente, uma cifra com a mesma chave (ou seja, cada ficheiro é cifrado individualmente, mas usa-se a mesma chave em todos) e que resolve usar o algoritmo AES (*Advanced Encrypton Standard*) em modo Counter (CTR) para cada um desses ficheiros.

a) Indique duas características desse modo de cifra que lhe são potencialmente vantajosas.

b) Indique que cuidado especial que deverá tomar relativamente à cifra desses ficheiros usando a mesma chave.

1.0 **6:** A aritmética modular é usada extensivamente em aplicações criptográficas. O que é que a torna tão útil?

1.0 **7:** Indique para que serve o teorema do resto Chinês. Que operações do sistema criptográfico RSA podem ser aceleradas usando este teorema?

1.0 **8:** O sistema criptográfico RSA pode ser usado para cifrar uma mensagem. Explique detalhadamente como. Explique também como pode depois essa mensagem ser decifrada. Qual é o problema matemático que o torna criptograficamente "seguro"?

1.0 **9:** O sistema criptográfico RSA também pode ser usado para assinar uma mensagem, isto é, para atestar, desde que sejam tomadas as precauções devidas, que uma messagem não foi forjada por outro que não o remetente. Explique detalhadamente como e quais as precauções a tomar.

1.0 **10:** Explique como implementaria o protocolo Diffie-Hellman, usando aritmética modular, para estabelecer um segredo partilhado por três partes (em vez das duas do protocolo original). Qual é o problema matemático que o torna criptograficamente "seguro"?