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"?

Segunda parte do exame da época normal de Criptografia Aplicada

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

1.0 **11:** A distribuição de chaves públicas é atualmente feita maioritariamente através de certificados públicos X.509. Explique:

a) Qual é a principal função de um certificado de uma chave pública?

b) Por que razão um certificado tem de ser assinado digitalmente?

1.0 **12:** Considere o conceito de revogação de um certificado de chave pública X.509. Explique:

a) Em que consiste?

b) Quem é que é responsável por comunicar a mesma?

c) Como é que essa comunicação pode ser realizada?

1.0 **13:** Um certificado de chave pública X.509 pode ser uma raiz de uma cadeia de certificação. Explique:

a) O que é uma cadeia de certificação?

b) O que faz com que um certificado seja raiz de uma cadeia de certificação?

1.0 **14:** *Long Term Validation* (LTV) é uma expressão que é usada para referir a capacidade de uma assinatura digital ser verificável de forma confiável muitos anos depois de ter sido produzida. Qual é o principal problema que a passagem do tempo cria na validação de assinaturas, e que levou à criação dos mecanismos que permitem a LTV (não os descreva!)?

1.0 **15:** O não-repúdio é uma característica que normalmente é desejável relativamente às assinaturas digitais de documentos. Explique:

a) Em que consiste o não-repúdio?

b) Qual é a relevância que dispositivos como os smartcards, como o Cartão de Cidadão, têm para assegurar esta característica?

1.0 **16:** Como é que é feita a adição de pontos numa curva elíptica?

1.0 **17:** Explique como se pode multiplicar eficientemente um ponto de uma curva elíptica por um número inteiro negativo.

1.0 **18:** Explique como se pode partilhar um segredo entre n entidades, $n \geq 2$, em que apenas t entidades, $2 \leq t \leq n$, são necessárias para revelar o segredo. Considere os casos $t < n$ e $t = n$.

1.0 **19:** A técnica *one-of-two oblivious transfer* permite que uma entidade extraia um item de informação (de um conjunto de dois itens) de uma outra entidade sem que esta consiga saber qual dos itens foi extraído. Explique como pode adaptar essa técnica para extrair um de n, com $n > 2$. A técnica é escalável, isto é, a sua utilização para n grande é prática?

1.0 **20:** Os resíduos quadráticos são indiretamente usados em protocolos de prova de identidade que não revelam informação (*zero knowledge proofs*). Qual é o problema matemático que os torna atrativos neste contexto?