Primeira parte do exame final de Criptografia Aplicada

7 de fevereiro de 2022 **11h00m – 13h00m**

1.0 **1:** Explique como se pode usar o modo de cifra CTR (Counter) para criar uma cifra contínua ou de fluxo (stream) a partir de uma cifra por blocos.

1.0 **2:** As cifras por blocos são muitas vezes realizadas usando transformações repetitivas com base em sub-chaves (key schedules). Explique:

a) O que são e como se calculam estas subchaves?

b) Quais são as 4 transformações elementares do AES que são repetidas múltiplas vezes, uma das quais envolvendo uma subchave?

1.0 **3:** Imagine que se quer proteger de um potencial atacante que usa uma máquina com processamento paralelo, como uma unidade de processamento gráfico (GPU). Estas unidades são particularmente rápidas quando executam exatamente as mesmas instruções sobre dados diferentes. Assumindo que o atacante tem de experimentar várias chaves e decifrar as mensagens-alvo completamente de forma a verificar se escolheu a chave certa, que modo de cifra escolheria? Justifique a sua resposta.

1.0 **4:** Em que casos se justifica usar um MAC (Message Authentication Code) em vez de uma assinatura digital para a autenticação de mensagens?

1.0 **5:** As funções de síntese têm de ter 3 propriedades fundamentais. Indique:

a) Quais são essas propriedades?

b) Qual delas é crítica para as assinaturas digitais (com apêndice)?

1.0 **6:** Explique resumidamente o protocolo de Diffie-Hellman (usando aritmética modular) e indique para que é que serve. Qual é o problema matemático que o torna criptograficamente "seguro"?

1.0 **7:** O protocolo Diffie-Hellman também pode ser implementado usando curvas elípticas. Explique como. Aproveita a ocasião para explicar muito resumidamente que operações aritméticas podem ser feitas sobre pontos pertencentes a uma curva elíptica.

1.0 **8:** O sistema criptográfico RSA requer exponenciações usando aritmética modular. Explique como é que essas exponenciações podem ser feitas de uma forma eficiente. Em particular, explique por que é que o expoente 65537 é muito usado nas chaves públicas RSA.

1.0 **9:** O sistema criptográfico RSA 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 como. Que precauções devem ser tomadas?

1.0 **10:** Um utilizador inexperiente construiu uma chave RSA com um expoente público de apenas 3. Se a mensagem a cifrar tiver um valor numérico pequeno, que problemas é que um exponente pequeno como este pode causar? Como é que se podem resolver esses problemas (sem alterar o expoente)?

Segundo teste de Criptografia Aplicada
Segunda parte do exame final de Criptografia Aplicada

7 de fevereiro de 2022 **9h00m – 11h00m**

1.0 **1:** A criptografia assimétrica pode ser usada para comunicação segura ou para a autenticação de mensagens. Em qualquer dos casos, é fundamental o conhecimento por terceiros da chave pública de um interlocutor. Neste contexto, explique a importância fulcral que têm os certificados de chave pública no âmbito da assinatura de documentos.

1.0 **2:** A validação de um certificado de chave pública envolve diversos passos, sendo um deles a verificação do seu período de validade. Indique, justificando:

a) Como se estabelece esse período de validade?

b) Qual a relação que terá de ser verificada entre esse período de validade e uma assinatura realizada com a respetiva chave privada?

1.0 **3:** Como é que é normalmente indicada a identidade de uma entidade que produz uma assinatura de um documento? Explique porquê.

1.0 **4:** As assinaturas digitais de documentos são tipicamente realizadas usando RSA e assinaturas com apêndice. Neste último caso, explique:

a) Por que razão são calculadas com uma função de síntese (digest function)?

b) Como é que o validador da assinatura sabe qual é a função que foi usada?

1.0 **5:** Qual é a relevância das TSA (Time Stamping Authorities) no âmbito das assinaturas digitais de documentos?

1.0 **6:** Explique como se pode partilhar um segredo entre n entidades, em que todas as entidades são necessárias para revelar o segredo.

1.0 **7:** Explique como se pode partilhar um segredo em que 3 de 5 entidades são necessárias para revelar o segredo.

1.0 **8:** 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.

1.0 **9:** Os resíduos quadráticos são indiretamente usados em protocolos de prova de identidade que não revelam informação (*zero knowledge*). Qual é o problema matemático que os torna atrativos neste contexto?

1.0 **10:** Indique uma vantagem e uma desvantagem que um sistema de distribuição de chaves quântico tem em relação a um sistema mais tradicional.

2 parte

saber se estes são de confiança, e são do proprietário que este o diz ser. Logo existe certificados pelos root CA para estabelecer esta confiança, garantindo que a chave pub é do mesmo.

2.
a) Pede de cópia de chave pub em q este é válido e uma data de expiração delimitada pela root CA

b) Se na assinatura a data do doc não estiver entre os datas este não é confiável.

3.
Para se saber a atividade se soubermos a chave pub este tem um certificado ligado com a inf de sua atividade validade.

4.
a) Síntese é usada pois produzem valores mais pequenos
b) Certificados

5. Protocolos de mudança de tempo no computador e dando maior confiança nos dados das assinaturas

6. o Segredo S com k bits é todo ficam um vaso com k bits s_n

$s_n = S \oplus s_1 \oplus \dots \oplus s_{n-1}$

agr é necessário todos o s_n para saber S

$S = s_1 \oplus \dots \oplus s_n$

7. Se cada um tiver um plano em 3-dim
Apenas 3 pontos para descobrir o ponto

ou
com Polinómios

$(m_1, A(m_1))$

e depois com Lagrange ou Newtons interpolation

cria-se polinomios que se não intersetam num ponto o grau do polinomio determina o numero de pessoas para descobrir o S sv. de neste caso 3.

8. Alice sorteia um m_1 e é pela chave x_0 e x_1

Bob passa num valor k verde a x_0 ou x_1 e no valor pub da Alice e encripta u e dá a Alice este com este valor cria dois valores descriptando com a sua chave juntando o seu m_0 ou m_1 e a prova $m_0 + k$ ou $m_1 + k$ mas não sabe qual é e sabe pois no escolheu e tirou o seu k para ter o m.