Primeira parte do teste final de Criptografia Aplicada

23 de janeiro de 2023 **10h00m**

1.0 **1:** Comparando os algoritmos de cifra do DES (*Data Encryption Standard*) e do AES (*Data Encryption Standard*) verificamos que o AES apenas usa funções invertíveis nos processo de cifra e decifra, enquanto o DES combina funções invertíveis e não-invertíveis para decifrar o que se cifra. Explique como no DES é feita esta combinação de funções (lembre-se do primeiro projeto prático).

1.0 **2:** Vários algoritmos de síntese (*digest*), como o MD5, SHA-1 e SHA2, usam uma metodologia de processamento de volumes arbitrários de dados conhecida como Merkle-Damgård, onde é usada uma aproximação de compressão iterativa. Explique:

a) Como funciona esta aproximação.

b) Imagine que dispõe de uma máquina com diversos processadores capazes de executar em paralelo sobre o mesmo volume de informação (e.g. um GPU). Acha que uma máquina dessas é capaz de acelerar o cálculo de uma síntese através da paralelização de operações?

1.0 **3:** Numa comunicação segura é normal combinar duas técnicas de proteção: cifra dos conteúdos (para obter confidencialidade) e redundância não forjável (para obter controlo de integridade). A redundância não forjável pode ser calculada de várias formas, como é o caso de um MAC (*Message Authentication Code*) ou de uma assinatura digital.

a) Indique qual considera ser a diferença técnica mais relevante entre essas duas formas de gerar um controlo de integridade não forjável.

b) Indique, justificadamente, uma vantagem de cada uma das técnicas em relação à outra.

1.0 **4:** Os modos de cifra definem formas de aplicar um algoritmo de cifra a um volume arbitrário de dados. Porém, cada modo de cifra possui vantagens e desvantagens face a um conjunto de requisitos operacionais. Imagine que tem um repositório gigantesco de conteúdos cifrados com AES (*Advanced Encrypton Standard*), por uma questão de confidencialidade (e.g. registos de videovigilância), aos quais pode precisar de aceder de forma ágil para observar uma filmagem realizada num dado momento. Indique, justificando:

a) Que requisitos devem ser considerados na escolha do modo de cifra.

b) Dos modos de cifra que aprendeu, indique qual acha que será a pior escolha?

1.0 **5:** Considere o conceito de alinhamento com excipiente (*padding*). Explique:

a) Em que casos é necessário usar?

b) Como funciona o processo de alinhamento denominado PKCS #7 (ou #5)?

1.0 **6:** O protocolo Diffie-Hellman pode ser implementado usando aritmética modular. Explique como e indique qual é o problema matemático que o torna "seguro".

1.0 **7:** O sistema criptográfico RSA pode ser usado para cifrar uma mensagem. Explique porque é que o exponente público não pode ser um número par.

1.0 **8:** 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 como. Qual é o problema matemático que o torna criptograficamente "seguro"?

1.0 **9:** Num sistema RSA em que o expoente usado para cifrar uma mensagem é sempre 3 e em que não se usa *padding* aleatório, enviar a mesma mensagem m para três destinatários diferentes, com chaves públicas $(n_1, 3)$, $(n_2, 3)$ e $n_3, 3)$, é altamente desaconselhado, já que se as três mensagens cifradas, $m^3 \bmod n_1$, $m^3 \bmod n_2$ e $m^3 \bmod n_3$, forem intercetadas é possível recuperar a mensagem original. Explique como.

1.0 **10:** Explique como se pode multiplicar eficientemente um ponto de uma curva elíptica por um número inteiro negativo.

Segunda parte do teste final de Criptografia Aplicada

23 de janeiro de 2023 **10h00m**

1.0 **11:** Um elemento fundamental de uma assinatura digital é o instante temporal em que foi gerada. Como se consegue garantir que o seu valor é confiável, ou seja, que a assinatura não foi produzida num instante diferente do indicado na mesma?

1.0 **12:** *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 **13:** Qual é a relevância que dispositivos criptográficos, como o Cartão de Cidadão, têm no que diz respeito à qualidade de uma assinatura digital?

1.0 **14:** Imagine que tem de validar uma assinatura colocada num documento. Indique, de forma sucinta, os todos os passos que terá de executar (assuma, que a assinatura contém todos os elementos necessários que normalmente são necessários para essa validação, como cadeias de certificação).

1.0 **15:** Um certificado de chave pública X.509 v3 é constituído por uma parte obrigatória e por um conjunto arbitrário de extensões.

a) Como são identificadas estas extensões?

b) Uma extensão pode ser crítica ou não-crítica. Explique as implicações desta classificação.

1.0 **16:** 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 **17:** 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 **18:** 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?

1.0 **19:** A aritmética modular é usada extensivamente em aplicações criptográficas. O que é que a torna tão útil?

1.0 **20:** Para que é que serve uma cifra homomórfica?

11. TSA este vai validar quando a

assinatura foi feita.

12. 1. As assinaturas tornam-se vulneráveis
2. Atraso na atualização da ct e logo esta assinatura poderá ser invalida por um 1º verificação

13. Os dispositivos de hardware, como o CC impedem o export da priv key e esta é usada internamente e só se pode usar a pub lg. as ass são mais seguras e confiáveis visto que a priv key nunca pode ser roubada. Também estes geram chaves seguras e robustas. A chave priv tem tem um pin.

14.
- usar a chave pub do autor e validar com o CA
- Desencriptar o ak ch → tirar info da função síntese
- fazer hash do doc
- comparar as duas

15.
a) usando o ASN.1 oid para identificar se é crítico ou não
b) Se o ct da fonte for rec é vl
Se for ct for novo não é vl
Se for a ct for nova é válido

16.
para t = m
S é o segundo com b bits

cada possui gera um valor de bits B

e fez $u_m = S \oplus v_1 \oplus \dots \oplus v_{m-1}$

depois todos precisam de dar o seu

um para retornar o S.

para $t < n$

eq do share t cada um e cont

bem el sobre o o gree... um pires

12.

$$v = (m_0 + k^e) \bmod N$$

$$m_0' = m_0 + (v)^d$$

13.

$$M^2 = a \bmod p$$

19

mcm ma's pq / ± mtz

20.