**SI Trabalho 1**

1. Questão - Quais as semelhanças e as diferenças entre um esquema assimétrico de assinatura digital e um esquema MAC? Quais os critérios de decisão para selecionar um deles?

Um esquema MAC providencia segurança acerca da origem e integridade da mensagem através de autenticação da origem dos dados e é computado através de duas entradas, sendo essas entradas, a mensagem em si e uma chave criptográfica privada.

Um esquema assimétrico de assinatura digital consiste de um algoritmo gerador de chaves, um algoritmo de assinatura e um algoritmo de verificação.

As semelhanças entre os dois esquemas são que a computação de ambos é feita através de duas entradas e ambos os esquemas se caracterizam pela autenticação da origem dos dados, no entanto no esquema MAC esta autenticação é feita através de uma chave privada partilhada pelo recetor e no esquema de assinatura digital a chave utilizada na assinatura é privada e a chave utilizada na autenticação é publica, por esta razão podemos dizer que o esquema MAC é um esquema simétrico e o esquema de assinatura digital é assimétrico.

Apesar de o esquema MAC permitir que o emissor e o recetor da mensagem detetem mensagens fraudulentas inseridas pelo intruso ou atacante, este mesmo esquema não permite uma terceira entidade saber se a mensagem origina mesmo de determinado emissor (Non repudiation), para estes casos precisamos de um esquema de assinatura digital.

Concluindo, se necessitarmos de produzir provas para uma terceira entidade conseguir verificar a origem da mensagem sem ter de lhe ser dado nada, por exemplo, num cenário de comércio eletrónico, um esquema de assinatura digital é ideal, mas no entanto noutros tipos de cenários em que esta prova não seja necessária, é mais eficiente utilizar um esquema MAC, pois não necessita de estabelecer uma chave publica que seja confiada por ambas as partes.

1. Questão - Considere a função de hash H(m) definida por:
   1. Seja Ep(k)(b) uma primitiva de cifra em bloco que usa chaves k de n bits e blocos b de n bits
   2. Seja m = m1, m2, . . . , mL a divisão da mensagem em blocos de n bits. Assuma que a dimensão das mensagens é sempre múltipla de n.
   3. Seja yi = Ep(mi−1)(mi), para i = 2,...,L, com y1 = m1.
   4. O valor de hash é H(m)=yL.

Explique porque motivo é computacionalmente fazível, dado m, obter m ̸= m tal que H(m′) = H(m).

O número de mensagens diferentes possíveis de serem enviadas é ilimitado, mas no entanto o número de hash codes possíveis de serem gerados é limitado, a isto chamamos de birthday paradox e é desta forma que podemos ter o mesmo hash para mensagens diferentes. Segunda pré-imagem

1. Questão - Apresente uma forma de atacar uma implementação de um esquema de cifra assimétrica cujo algoritmo de cifra, Ea(k)(m), seja determinístico (isto é, se x = y então Ea(k)(x) = Ea(k)(y)).

Cifrar mensagens com diferentes keys geradas aleatoriamente até chegar a uma mensagem que tenha um algoritmo de cifra igual á mensagem que pretende atacar.

1. Questão - Os sistemas A e B cifram mensagens usando, respetivamente, as primitiva DES (chaves com 56 bits úteis) e AES (chaves de 128 bits). Admitindo o uso de chaves aleatórias, porque motivo os criptogramas produzidos por A podem ser mais difíceis de criptoanalisar do que os produzidos por B?

DES caracteriza-se por cifra dupla, ou seja, apesar das chaves terem menos bits, torna-se mais difícil de criptoanalisar porque existem duas chaves a chave da primeira cifra e a chave da segunda cifra.

1. Questão - Na biblioteca Java Cryptography Architecture (JCA), como é que as engine classes (ex: Cipher, Signature, Mac) possibilitam a aplicação incremental das respetivas proteções? Qual a vantagem de aplicar proteções incrementalmente?

Cipher-Para a engine classe cipher,a mesma é inicializada com o método init e para cifrar parte da mensagem é utilizado o método update que retorna parte do criptograma,no ultimo bloco da mensagem a cifrar é utilizado o método doFinal que retorna o final do criptograma.

Signature-Para a engine classe signature,a mesma é inicializada com o método initSign ou initVerify dependendo se queremos criar ou verificar uma assinatura utilizando em ambas o método update para receber parte da mensagem,no ultimo bloco da mensagem a assinar/verificar é utilizado o método sign/verify que cria ou verifica uma assinatura na mensagem.

MAC-Tal como na engine classe cipher são utilizados os métodos init,update e dofinal para,respectivamente,inicializar,autenticar parte da mensagem,e autenticar o final da mensagem.

A grande vantagem de aplicar proteções incrementalmente é evidente quando existem grandes mensagems ou ficheiros que precisem de ser cifrados,assinados/verificados ou autenticados,em que,ao invés de ocupar-mos toda a memoria disponível,realizamos o processo pretendido subdividindo-o em várias partes.

1. Questão - Considere os certificados X.509 e as infraestruturas de chaves pública (PKI):
   1. De que forma a resistência à segunda pré-imagem de uma função de hash contribui para garantir a autenticidade da chave pública de um certificado.
   2. Considere o certificado folha C e os intermédios I1, I2, . . . , In. Alguma das chaves privadas dos certificados intermédios é usada para validar o certificado C?

6.1 Resposta:

Sendo a resistência à segunda pré imagem – tendo um valor de entrada x e *h*(*x*), ser computacionalmente infazível encontrar um outro valor de entrada , com *h*(*x*) = *h*().

A resistência á segunda pré imagem de uma função de hash verifica que dado uma mensagem m1 é muito improvável encontrar uma mensagem m2 cujo hash(m1)=hash(m2),ou seja,mensagens diferentes resultam em hash’s diferentes.Logo ao criar uma assinatura cifrada com a chave privada do certificado é possível verificar a autenticidade de uma chave publica se a mesma decifrar a assinatura.

* 1. Resposta:

No certificado X.509,a hierarquia de certificados é baseada em arvore com o certificado raiz no topo que não precisa de ser assinado e os respetivos certificados intermediários e certificados folha. Logo o certificado folha C tem de ser assinado por uma entidade de maior nível(certificado intermédio),e para isso é necessário o uso da chave privada desse mesmo certificado intermédio

Questão 7-Considere o laboratório sobre cifra simétrica dos Labs for Security Eduction (SEED) . Realize o ponto 2.4 Task 4: Padding". Na alínea 1 indique os modos que usam padding explicando as experiências efetuadas. Na alínea 2 realize a experiência com a primitiva AES em modo CBC e indique, para cada dimensão de ficheiro, os valores de padding.

Na alínea 1 era pedido para usarmos os modos de criptografia ECB,CBC,OFB,CFB e verificar quais deles utilizavam padding e quais não utilizavam,para isso,foi criado um ficheiro de texto teste ao qual aplicamos todos estes modos para o encriptar e em seguida desencriptar utilizando a instrução -nopad para que fosse visível o padding depois da desencriptação.Através da analise dos ficheiros é possível afirmar que tanto o modo ECB como o modo CBC produziram pading pois o tamanho do ficheiro aumentou e é possível verificar que no texto foram adicionados dois espaços em branco.No entanto,o modo OFB e o CFB não produziram qualquer padding pelo que o tamanho do ficheiro manteve-se igual

//EXPLICAR PORQUE!!

//PRINTS??

Na alínea 2 era pedido para criarmos 3 ficheiros com respectivamente 5,10 e 16 bytes e depois da respectiva encriptação verificamos que o tamanho dos novos ficheiros era de,respectivamente,32,32 e 48 bytes.Para verificar a existência de padding desencriptamos os ficheiros utilizando a instrução -nopad para que o padding não fosse removido na desencriptação.Os ficheiros desencriptados ficaram então com 16,16 e 32 bytes.

Por fim verificamos através do hexdump quantos bytes tinham sido acrescentados á mensagem,chegámos aos valores esperados que foram 11,6 e 16 bytes de padding para cada ficheiro,respectivamente.