Instituto **S**uperior de **E**ngenharia de **L**isboa

Licenciatura em Engenharia Informática e de Computadores

Semestre de Inverno 2016/2017

Segurança Informática

Primeira série

LI51N

Trabalho elaborado pelo Grupo 1:

Sara Sobral N.º 40602

Eduardo António N.º 40686

1. **Qual a motivação para os esquemas MAC (Message Authentication Code), dado que os esquemas de cifra simétrica já fornecem confidencialidade?**

Nos esquemas MAC "Todos podem verificar, apenas o emissor autorizado pode assinar (gerar a marca)".

A motivação para os esquemas MAC é o facto de garantirem Integridade e Autenticidade ao invés da cifra simétrica.

2. **No contexto das funções de hash, o que é a propriedade da resistência ao cálculo da segunda pré-imagem (falsificação seletiva)? Forneça um exemplo de utilização onde esta propriedade é usada.**

A propriedade da resistência ao cálculo da segunda pré-imagem diz que dadas duas mensagens não podem der semelhanças no hash.

Por exemplo com SHA-1 ficamos com :

Hash("O Eduardo é muito awesome!") = 68b8291eb95e9e77a44a8fd87265b6bc027bce52;

Hash("A Sara é muito awesome!") = 75f3f2554a34604b9f04c7d22bd21153e4a5a79f;

Como podemos ver não se encontra qualquer semelhança logo é respeitada a propriedade da resistência ao cálculo da segunda pré-imagem.

3. **Quando o espaço de mensagens a cifrar é muito pequeno (e.g. PINs de 4 dígitos), é fundamental que o esquema assimétrico de cifra utilizado tenha a função E não determinística. Justifique.**

Sim pois se a mensagem é pequena não é seguro que apos a encriptação seja sempre igual pois será mais fácil a sua desencriptação por ambientes externos.

4. **Com o objetivo de eliminar o problema do modo ECB quanto à passagem de padrões do texto em claro para o texto cifrado, foi definido o seguinte modo de operação:**

• m = m1, . . . , mL a divisão da mensagem m nos blocos mi .

• R é um numero aleatório.

• c0 = R, ci = E(k)(mi ⊕ R), para i = 1, . . . , L, onde ⊕ denota a operação de ou-exclusivo bit a bit e E uma primitiva de cifra em bloco.

Este modo de operação cumpre o objetivo?

Não, pois a operação de ou-exclusivo vai ser feita nos blocos usando o mesmo R logo dois blocos iguais, ficariam igualmente cifrados. Logo duas mensagens iguais ficariam igualmente cifrados.

5. **Na biblioteca JCA, porque razão a classe MAC não precisa de ter um método verify, semelhante ao existente na classe Signature?**

O método verify usa a chave publica para verificar a assinatura, sendo o MAC um esquema simétrico não requer assinatura.

6. **Considere a infraestrutura de certificados X.509.**

6.1. Foi atribuído à Alice o certificado C_{Alice} e a respetiva chave privada. Justifique se a Alice consegue ou não alterar o campo com a data de validade do certificado, mantendo a sua validade?

Não, pois a sua edição só é permitida à entidade que emite o certificado.

6.2. Quais as consequências se uma aplicação consumidora de certificados ignorar a extensão basic constraints?

Ficheiros de extensão basic constraints são usados para restringir as autoridades de certificação que à partida não são confiáveis.

Se estes ficheiros forem ignorados as regras colocadas na autoridade de certificação que permite restringir os certificados emitidos pela CA com base nos critérios previstos no pedido não são aplicadas.

6.3. Considere que o servidor S usa a CA0 para a emissão dos seus certificados. Em que situações o ataque a uma autoridade de certificação diferente de CA_0 pode criar as condições para ataques de Man In The Middle entre clientes e S.

Se for realizado a um ataque a um certificado intermedio, gerado por CA0, roubando-lhe a chave privada é possível forjar mensagens e certificados de um S' pensando que se trata do S, ou seja, existe *man in the middle* entre S e os clientes.

6.4. Qual a diferença entre um ficheiro .pfx e um ficheiro .cer?

Certificados (.cer) são ficheiros usados para guardar certificados X.509.Normalmente são usados para certificações SSL para verificar e identificar a segurança de servidores. Um ficheiro destes contem informação acerca do criador do certificado assim como a chave pública e privada do certificado.

Personal Exchange Format (.pfx) são ficheiros PKCS12 que contem uma grande variedade de informação criptográfica como certificados, certificados de autoridade de raiz, certificados intermédios e chaves privadas. São protegidos por palavra-passe para manter as chaves privadas privadas e preservar a integridade dos certificados de raiz.

7. Realize uma aplicação de consola para proteger JSON Web Tokens (JWT) usando a biblioteca JCA. A proteção consiste no uso de cifra/decifra autenticada, com transporte de chaves usando criptografa assimétrica, tal como exemplificado na secção 3.3 do RFC 7516.

- **Realize e teste um componente para cifrar e decifrar strings arbitrarias usando o algoritmo AES em modo GCM [1, 2].**

Classe: AesSecretKey.java

- **Realize e teste um componente para cifrar e decifrar uma chave AES usando o algoritmo RSA.**

Classe: RsaKey.java

- **Realize e teste um componente para obter a chave publica de um certificado X.509 validado e uma chave privada de um keystore.**

Classes: GetPublicKey.java e GetPrivateKeu.java

- **Use os componentes anteriores para realizar e testar o sistema pretendido.**

Classe: Program.java

Testes: CodeTests.java, cada classe tem um método teste nesta classe com o seu nome.