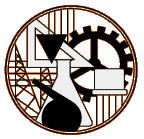
**Instituto Superior de Engenharia de Lisboa**

**Ano Lectivo 2011/2012 – Semestre Inverno**

**Segurança Informática**

**1ª Série**

**Professor:** José Simão

**Data:** 28 de Outubro de 2011

**Autores**:

Cláudia Crisóstomo nº 32142

Nuno Cancelo nº 31401

Telmo Rafael Pinto n.º30505

Índice

[Exercício 1: 3](#_Toc307584802)

[Exercício 2: 5](#_Toc307584803)

[Exercício 3: 6](#_Toc307584804)

[Exercício 4: 7](#_Toc307584805)

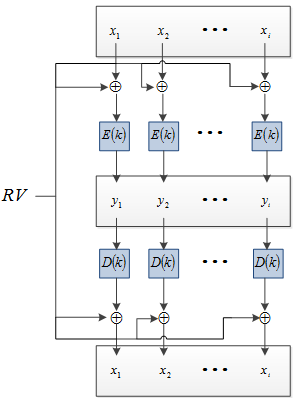
[Exercício 5: 8](#_Toc307584806)

# Exercício 1:

Considere o contexto dos esquemas e primitivas criptográficas:

* 1. **Considere um novo modo de operação definido por:**
* **Seja x = x1, … , xL a divisão nos blocos xi do texto em claro x.**
* **RV é um vector aleatório, com a dimensão do bloco, gerado por cada texto em claro x.**
* **Seja yi = E(k)(xiRV ), para i = 1, … ,L, onde E é a operação de cifra, denota o ou-exclusivo bit a bit.**

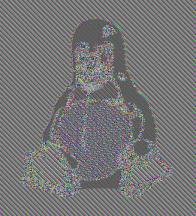
**i. Defina o algoritmo de decifra para este modo de operação.**

****

**ii. Compare este modo de operação com o modo CBC quanto a:**

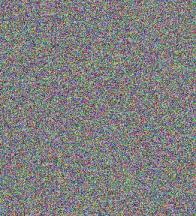
* + - 1. **Possibilidade de padrões no texto em claro serem evidentes no texto cifrado.**

O modo de operação definido na alínea anterior irá transpôr padrões no texto em claro porque para cada bloco iguais (x1, x2) o resultado do or-exclusivo destes blocos com RV será sempre igual, abaixo está desmonstrado um exemplo que esta vulnarebilidade apresenta.

Por outro lado, o modo de operação CBC (Cipher Block Chaining) descarta qualquer possibilidade de padrões no texto em claro porque o or-exclusivo é efeito entre o bloco anteriormente cifrado (ou RV caso seja o primeiro bloco) e o bloco da mensagem o que irá alterar os bytes do bloco original sendo desta forma muito improvável que blocos iguais tenham a mesma cifra.

Em seguida ilustramos a utilização do modo de operação CBC.



**b) Capacidade de paralelizar a cifra.**

O modo de operação definido na alínea i é paralelizável na cifra porque o RV é conhecido sendo desta forma possível cifrar parte da mensagem (por exemplo: a partir de x4), o mesmo não acontece no modo de operação CBC porque é necessário usar o bloco anteriormente cifrado pelo que obriga a cifrar toda a mensagem e não parte desta.

**1.2 Comente a seguinte frase, adaptada do livro Computer Security: ''Stream ciphers can process plain-text in chuncks that are smaller than the block size of the cipher algorithm".**

O modo de operação em stream tem a capacidade de efectuar uma operação de or-exclusivo a cada bloco da mensagem a “encriptar” pelo que o bloco “Key Stream” gera uma chave através de uma determinada primitiva (como por exemplo: RSA) cujo parâmetro respeita uma das operações CTR, OFB e CFB.

Desta forma, cada chave, produzida pelo Modo Stream, deverá ter o mesmo tamanho que o bloco da mensagem a ser submetida pela operação or-exclusivo, acontece que este tamanho poderá não ser respeitado no último bloco, por isso, dever-se-á acrescentar o respectivo “padding” à mensagem para sinalizar o termino desta.

**1.3 Porque razão a arquitectura dos esquemas assimétricos de cifra prevê a adição de aleatoriedade no texto em claro?**

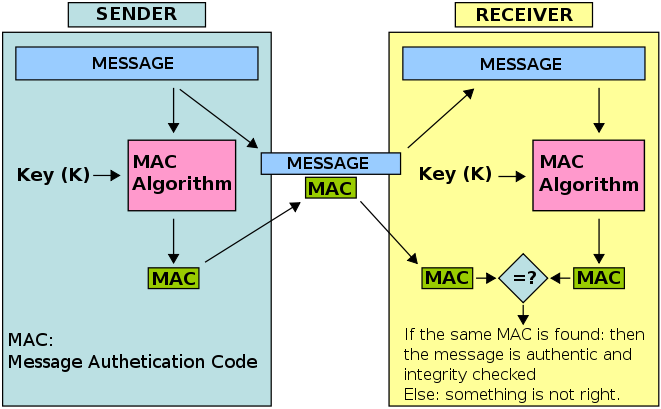
A arquitectura dos esquemas assimétricos de cifra prevê a adição de bits aleatórios no texto em claro porque blocos da mensagem iguais terão cifras iguais sendo desta forma transposta padrões da mensagem original, tal como acontece no modo de operação EBC.

# Exercício 2:

Considere o contexto dos esquemas criptográficos e da Java Cryptography Architecture (JCA)

**2.1. A proteccão de um keystore é feita usando um esquema MAC. Descreva em detalhe esta utilização e o tipo de protecção obtido.**

Cada *keystore* está protegido por uma palavra-chave que assegura de certa forma que quem acede a esta é apenas o dono do certificado. Desta forma, quando este (o utilizador em posse da palavra-chave) pretende obter o certificado deve facultar ao JCA a palavra-chave correcta e esta será validada através do esquema *Message Authentication Codes* que ao receber a palavra-chave aplica o algoritmo MAC com uma determinada chave (gerada no momento da adição do keystore) e se o resultado o novo MAC for igual ao MAC guardada nessa entrada o acesso ao certificado disponibilizado ao utilizador.

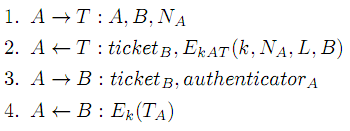


**2.2. O método doFinal da engine class Cipher pode ser chamado repetidamente. Após cada chamada, a instância volta ao estado em que ficou após a iniciação (método init). Assim sendo, qual a razão para a existência do método update?**

O método *doFinal* tem a capacidade de adicionar *padding* à mensagem sendo que o array de bytes facultado é interpretado como o último bloco da mensagem, desta forma, o método update aplica a primitiva ao bloco de bytes disponível por parâmetro ignorando o paradigma do padding. Desta forma é perceptível que após se concluir a cifra de uma mensagem (invocação ao método doFinal) qualquer submição de blocos serão lidos como uma nova mensagem até se invocar novamente o método doFinal.

# Exercício 3:

Considere a versão simplificada do protocolo Kerberos apresentada em seguida:



**3.1 Quais os mecanismos existentes neste protocolo para a protecção contra ataques de replay?**

O Protocolo Kerberos previne os ataques de replay através da validade do bilhete e da marca temporal( única e sequencial) enviada nas mensagens entre A e B. Assim, impedir ataques de replay porque o atacante ao replicar as mensagens enviadas por A as marcas temporais serão as mesmas e quando B recepcionar a mensagem irá verificar que essa não era a marca temporal esperada além de que a validade do bilhete já pode ter expirado.

**3.2. Tendo em consideração que B recebe o bilhete de A, pode B autenticar-se como A perante uma ca terceira entidade?**

Não, porque B não está em posse da chave secreta de A.

**3.3. A utilização da cifra no bilhete pode ser substituída por um esquema MAC (Message Authentication Code)? Se sim, indique como.**

Não,o esquema simétrico não pode ser substitído por um esquema MAC porque a informação enviada no bilhete para A é confidencial e o esquema MAC só garante integridade da mensagem, isto porque é no bilhete que o T envia a A que está presente a chave k que apenas pode ser conhecida por T, A e B.

**3.4. A utilização da cifra no authenticatorA pode ser substituída por um esquema MAC (Message Authentication Code)? Se sim, indique como.**

Sim, é possível porque o Authenticator de A é a identificação do cliente A, embora a sua identificação seja verificável.

# Exercício 4:

Considere os certificados definidos pela norma X.509 e o protocolo Secure Socket Layer (SSL).

**4.1. De que forma é́ obtida a chave autenticada do emissor de um certificado C?**

A chave autenticada do emissor do certificado C é obtida quando lhe é enviada uma mensagem cifrada com a chave pública do certificado C e este (emissor) decifra a mensagem com a sua chave privada provando desta forma que realmente é dono do certificado C.

**4.2. De que forma o record protocol evita ataques de replay.**

O protocolo Record evita ataques de replay através do número de sequência de cada mensagem trocada entre cliente e servidor. Assim, quando um atacante recolhe as mensagens trocadas entre cliente e servidor numa determinada sessão, o número de sequência irá corresponder ao preciso momento em que a mensagem foi enviada, então quando o atacante replicar estas mensagens para o servidor fazendo-se passar pelo cliente, na própria sessão ou noutra, o servidor irá rejeitar estas mensagens pois este está à espera de um número de sequência superior às indicadas nas mensagens guardas pelo atacante.

**4.3.Considere que o servidor malicioso S1 realiza uma instˆncia do protocolo handshake com o cliente a C. Como é́ que este protocolo impede que S1 se possa autenticar como C perante um outro servidor e S2 , nomeadamente através do reenvio das mensagens que C enviou para S1 .**

O protocolo handshake impede que S1 possa autenticar-se como C perante o servidor S2 porque no inicio da comunicação entre S1 e S2 é enviado para S2 o ID de sessão que é diferente do que foi enviado para o cliente C, o que irá originar que o resultado: PRF{(master\_secret, handshake\_messages)} não seja igual ao enviado por S1.

**4.4. As mensagens do sub-protocolo handshake são trocadas sobre um canal inseguro. Qual a técnica utizada neste sub-protocolo para detectar ataques de man-in-the-middle, no qual o atacante consegue interceptar e modificar as mensagens trocadas entre cliente e servidor.**

A técnica usada para detectar ataques de man-in-the-middle é a utilizar as mensagens trocadas durante o processo como mensagem a cifrar e caso o atacante intercepte e as adultere, o servidor irá verificar que as mensagens que enviou ao cliente não irão ser iguais às que o cliente recebeu.

# Exercício 5:

Realize, na plataforma Java, uma aplicação para geração de hashs cripográficos de ficheiros. A aplicação recebe na linha de comandos i) o nome da função de hash e ii) o ficheiro para o qual se quer obter o hash. O valor de hash é enviado para o standard output.

***public static OutputStream generateHash(String algoritm, InputStream message) throws NoSuchAlgorithmException, IOException{***

***MessageDigest md = MessageDigest.getInstance(algoritm);***

***OutputStream out = new ByteArrayOutputStream();***

***byte[] p = new byte[1024]; int l = 0;***

***while((l = message.read(p)) != -1) md.update(p,0,l);***

***byte[] r = md.digest();***

***StringBuffer hex = new StringBuffer();***

***for(int i = 0; i < r.length; ++i) hex.append(Integer.toHexString(0xFF & r[i]));***

***System.out.println(hex);***

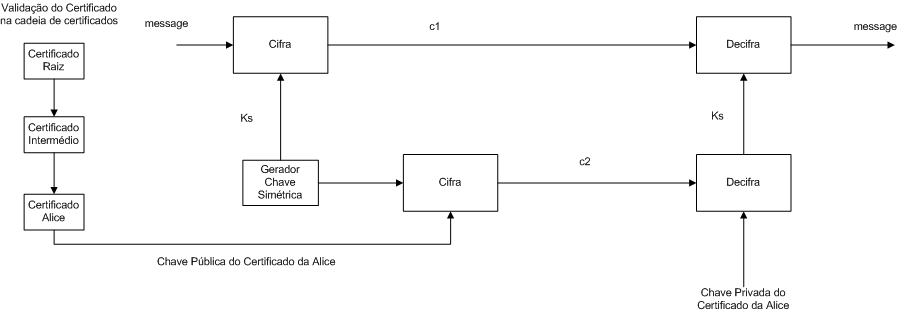
***out.write(md.digest());***

***return out;***

***}***

# Exercício 6:

Realize, na plataforma Java, uma aplicacão para a cifra e decifra de ficheiros. Os requisitos da aplicação são:

* Operação de cifra:
  + A operação de cifra recebe a localização do cheiro a cifrar e produz dois cheiros: um com o resultado da cifra e outro com os meta-dados da cifra.
  + A operação de cifra é também parametrizada por: ficheiro com o certicado X.509 do destinatário; directoria contendo certicados de autoridades de certicação intermédias; e key store com as âncoras de confiança utilizadas na validação das cadeia de certicados.
  + Os meta-dados devem incluir o certicado utilizado, por forma a permitir a selecção automática da chave no destinatário.
  + A cifra do conteúdo do ficheiro deve usar mecanismos simétricos, sendo os mecanismos assimétricos usados para o transporte da chave simétrica.
  + 

Código em anexo.

# Exercício 7:

Conﬁgure uma instalação do servidor HTTP Apache para aceitar ligações HTTPS (HTTP sobre SSL)

com os seguintes requisitos:

• Autenticação de cliente obrigat´oria;

• Aceitação, como trust anchor, do certiﬁcado auto-assinado presente no ﬁcheiro CA2.raiz.jks.

Resolução:

**# httpd.conf - Autenticação de cliente obrigatória;**

**#criação do user isel com pwd si**

**htpasswd.exe  -c ../conf/pwd isel**

**#configuração de httpd.conf para solicitar autenticação**

**<Directory />**

**AuthType Basic**

**AuthName "SI - serie1 - Ex. 7"**

**AuthUserFile conf/pwd**

**Require user isel**

**Options FollowSymLinks**

**AllowOverride None**

**Order deny,allow**

**#    Deny from all**

**Satisfy all**

**</Directory>**

**###########################################################################################**

**# httpd-ssl.conf - SSL**

**1. line 101 #SSLCertificateFile "conf/ssl.crt/localhost.pem"**

**2. line 109 #SSLCertificateKeyFile "conf/ssl.crt/localhost\_privateKey.pem"**

**3. line 118 #SSLCertificateChainFile "conf/ssl.crt/CA2.raiz.pem"**

**4. line 128 #SSLCACertificateFile "conf/ssl.crt/CA2.raiz.pem"**

**######## openssl / Keytool**

**# Publick Key**

**1. openssl.exe pkcs12 -in localhost.pfx -clcerts -nokeys -out localhost.pem**

**#import password : changeit**

**#Private Key**

**2. openssl.exe pkcs12 -in localhost.pfx -nocerts -out localhost\_privateKey.pem**

**# Thrust Anchor**

**3. keytool -keystore CA2.raiz.jks -exportcert -alias mykey -rfc -file CA2.raiz.pem**