Segurança Informática - 1º Trabalho

Licenciatura em Engenharia Informática e de Computadores

44860	Inês Franco
44880	Ricardo Tomé
47179	Afonso Cabaço

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 vetor aleatório, com a dimensão do bloco, gerado por cada texto em claro x.

• Seja yi = E(k)(xi ⊕ RV), para i = 1, . . . , L, onde E é a operação de cifra, k é a chave da cifra, ⊕ denota o ou-exclusivo bit a bit.

1.1. Defina o algoritmo de decifra para este modo de operação.

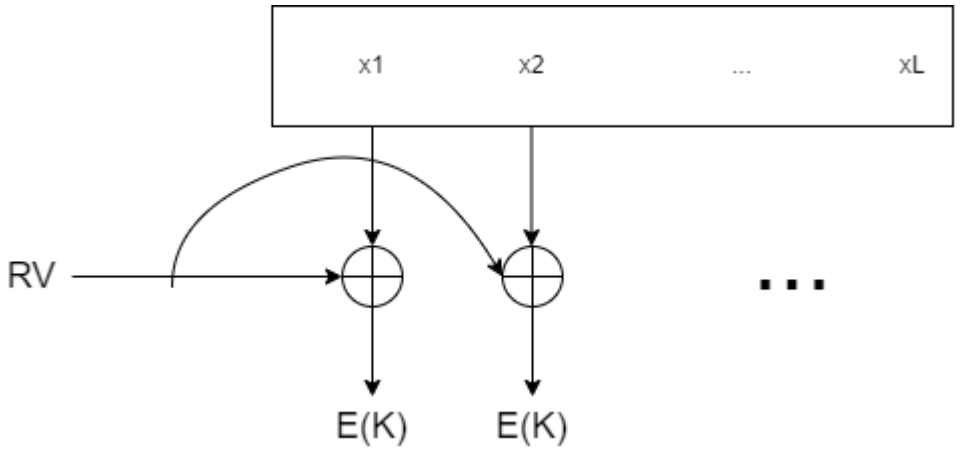

imagem 1.1: Esquema de cifra do modo de operação a ser estudado

Resposta:

O algoritmo de decifra é o seguinte:

$$D(K)\ (yi \oplus RV)$$

Teste :

m = 1 0 1 0 1 1
RV = 1 0 1 1 0 1

_____

cifra = 0 0 0 1 1 0
RV = 1 0 1 1 0 1

_____

decifra = 1 0 1 0 1 1

correto! m = decifra

1.2. Compare este modo de operação com o modo CBC quanto a:
a) possibilidade de padrões no texto em claro serem evidentes no texto cifrado
b) capacidade de paralelizar a cifra.

> **Resposta:** Este modo de operação, ao contrário do CBC, permite a paralelização das operações visto que os blocos não dependem uns dos outros para se cifrar e decifrar, neste sentido este modo pode ser mais rápido a concluir.
> Por outro lado, visto que os blocos não se influenciam, símbolos iguais a fazerem xor com o mesmo RV vão produzir cifras iguais o que quer dizer que vai ser perceptível padrões no texto cifrado.

---

2. O RFC 4880, "OpenPGP Message Format", especifica a cifra de mensagens (denominados objectos) como uma combinação entre esquemas assimétricos e simétricos: «[...] first the object is encrypted using a symmetric encryption algorithm. Each symmetric key is used only once, for a single object. A new "session key" is generated as a random number for each object (sometimes referred to as a session). Since it is used only once, the session key is bound to the message and transmitted with it. To protect the key, it is encrypted with the receiver's public key. [...]» Justifique a utilização desta abordagem com dois tipos de chave e explique sucintamente o processo de decifra de uma mensagem (object).

> **resposta:** As cifras assimétricas têm a vantagem de não produzirem a necessidade de existir uma troca de chaves entre o sujeito que envia e o sujeito que recebe a mensagem. Quem envia a mensagem apenas precisa saber a chave pública do receptor.

As cifras simétricas, por sua vez, têm a vantagem da encriptação e desencriptação da mensagem ser mais rápida que a assimétrica devido ao uso de apenas uma chave ao invés de duas.

Em suma, ao utilizar um sistema híbrido temos a segurança da cifra assimétrica com a velocidade da cifra simétrica.

Processo de decifra:

O receptor recebe a mensagem encriptada e uma session key encriptada.
Com a sua chave privada o receptor decifra a session key encriptada e
utiliza esta session key, agora já decifrada, para decifrar a mensagem.

3. A engine classe Signature da JCA contém, entre outros, os seguintes métodos:

void initSign(PrivateKey privateKey)
void initVerify(PublicKey publicKey)
void update(byte[] data)
byte[] sign()
boolean verify(byte[] signature)

3.1 Explique sucintamente o processamento realizado internamente no método sign com o objetivo de fazer a assinatura. Pode usar na explicação os métodos referidos que entenda relevantes.

resposta: Metodo Sign
initSign -> Update, Update, Update ... -> Sign -> s
initVerify -> (Update, Update, Update ...) -> Verify (s, v) -> True/False

v = chave privada do emissor

O Sign vai buscar o hashCode produzido no último update, encripta este com a
private key e retorna os bytes assinados. Estes serão posteriormente usados para verificação no método verify.

3.2 Considere que é instanciado um objeto Signature com a transformação "RSAwithMD5". Se em virtude de uma vulnerabilidade detectada na função de hash MD5 for computacionalmente fazível, dado x, obter x′ ≠ x tal que MD5(x′) = MD5(x), quais as implicações deste ataque para as assinaturas geradas/verificadas pelas transformação referida?

resposta: Visto que o MD5 é bastante vulnerável a colisões, isto faz com que as assinaturas legítimas geradas/verificadas por esta função de hash percam legitimidade/integridade além que correm o risco de ter informação e chaves privadas acedidas/expostas.
E para um usuário existe a possibilidade de estar a partilhar informação particular com um destinatário não legítimo.

4. Considere os certificados digitais X.509 e as infraestruturas de chave pública:

4.1 Em que situações é que a chave necessária para validar a assinatura de um certificado não está presente nesse certificado?

resposta: Em cadeias de certificação a chave necessária para a validação não está presente, excepto quando o certificado é o de raiz de confiança em que a sua chave pública valida a sua própria assinatura.

4.2 Porque motivo a proteção de integridade dos certificados X.509 não usa esquemas MAC (Message Authentication Code)?

resposta: O sistema mac necessita que exista um conhecimento de ambos os lados de uma chave privada.
O objeto é cifrado e decifrado com essa mesma chave (sistema simétrico).
Já o sistema PKI usa duas chaves, uma pública e outra privada. Todos podem cifrar, mas apenas o recetor pode decifrar (sistema assimétrico).
É necessário a existência de duas chaves, uma pública para cifrar e transmitir dados e outra privada do conhecimento apenas do proprietário para decifrar e conseguir aceder a estes dados.

4.3 Qual a diferença entre ficheiros .cer e ficheiros .pfx?

resposta:
A extensão.cer é usada para representar um único certificado, este é o formato que clientes têm acesso para ser feita verificação ou pedidos de autenticação.
Um ficheiro com extensão .pfx inclui um certificado que contém a chave pública e têm guardado também uma chave privada que pode ser usada para encriptar, assinar ficheiros.
O conteúdo destes pode estar protegido para preservar a integridade de certificados raiz e manter seguras as chaves privadas.