

Segurança Informática

Trabalho 1

Parte 1

Exercício 1

A falha principal neste esquema é que apenas os primeiros L bits do resultado do MAC são cifrados e anexados à mensagem. Isso significa que qualquer atacante pode modificar os bits além dos primeiros L bits da mensagem cifrada sem ser detetado.

Exercício 2

É comum proteger chaves simétricas com esquemas de cifra assimétricos pois estes providenciam mais segurança do que apenas utilizar chaves simétricas. Contudo só usar a cifra assimétrica tem um custo computacional demasiado elevado fazendo com que deixe de ser um método fiável. Assim sendo usa-se um esquema híbrido que dá mais segurança às chaves assimétricas e sem um custo computacional muito elevado.

Exercício 3

Semelhanças:

Ambos fornecem autenticidade para a mensagem e ambos utilizam chaves para gerar e verificar a autenticação.

Diferenças:

Chave Usada: Um esquema MAC usa uma chave secreta compartilhada para gerar a autenticação, enquanto uma assinatura digital usa uma chave privada do remetente para gerar a assinatura.

Verificação da Autenticidade: A autenticidade de um MAC é verificada usando a mesma chave que foi usada para gerar o MAC, enquanto a autenticidade de uma assinatura digital é verificada usando a chave pública correspondente à chave privada usada para gerar a assinatura.

Exercício 4

Resposta 4.1:

O certificado C pode ser considerado de confiança pelo sistema Sa e não por Sb com base na confiança atribuída às Autoridades Certificadoras envolvidas na cadeia de certificação. Se a AC que emitiu o certificado C é confiável e aceita por Sa, então o certificado C também será considerado confiável por Sa. No entanto, Sb pode não confiar na AC que emitiu C ou pode ter políticas de confiança diferentes.

Resposta 4.2

Para tornar inválidos os certificados assinados com chaves privadas de entidades folha, o mecanismo primário é a revogação de certificados. Este processo envolve a emissão de uma lista de certificados revogados (CRL - Certificate Revocation List) pela AC, que lista os certificados que não são mais considerados válidos antes da expiração de sua validade. Além disso, o Online Certificate Status Protocol (OCSP) é usado para obter informações de revogação em tempo real. Quando um certificado é revogado, ele não deve mais ser considerado válido para operações de confiança.

Parte 2

Exercício 5

Na resolução deste exercício nós utilizamos os seguintes comandos.

* Comandos para geração de chave:
  + rand -hex 16
  + rand -hex 8
* Comandos para cifrar o body consoante o modo e o algoritmo:
  + aes-128-cbc -in <arquivo de entrada> -out <arquivo de saída> -K <chave em hexadecimal> -iv 0
  + aes-128-ecb -in <arquivo de entrada> -out <arquivo de saída> -K <chave em hexadecimal>
  + des-cbc -in <arquivo de entrada> -out <arquivo de saída> -K <chave em hexadecimal> -iv 0
  + des-ecb -in <arquivo de entrada> -out <arquivo de saída> -K <chave em hexadecimal>

Uma imagem com texto, captura de ecrã, Saturação de cores, Retângulo

Descrição gerada automaticamente

Observações:

Após a concatenação dos *body’s* cifrados com *header* observamos que as imagens produzidas através do modo de operação ECB não estão tão elegíveis como as imagens em que o modo utilizado foi CBC. Isso acontece, pois, no modo ECB a cifra é realizada de forma independente de bloco para bloco fazendo com que blocos iguais obtenham uma cifra igual entre si. Já no CBC a cifra é realizada de forma dependente utilizando o bloco cifrado para cifrar o seguinte, fazendo com que os blocos cifrados sejam diferentes.

Exercício 6

Resposta 6.3:

Neste caso, quando a integridade da cadeia de blocos for ser validada o *hash* do bloco 9 será calculado e comparado com o *hash* presente no bloco 10. Se os resultados não forem os mesmos será identificado que os blocos foram adulterados.

Resposta 6.4:

Para alterar o valor da transação do bloco 10 teríamos de criar um bloco com os valores da transição que queremos e adicionar o *hash* gerado com o bloco 9, pois não vamos realmente alterar o bloco, mas sim substituí-lo. Após essa ação teríamos de criar novos blocos, onde o 11 teria o *hash* baseado no novo bloco 10 e todos os outros blocos seriam novamente gerados a partir dos seus blocos anteriores.