Tópicos de Segurança

Ano letivo 2020/2021

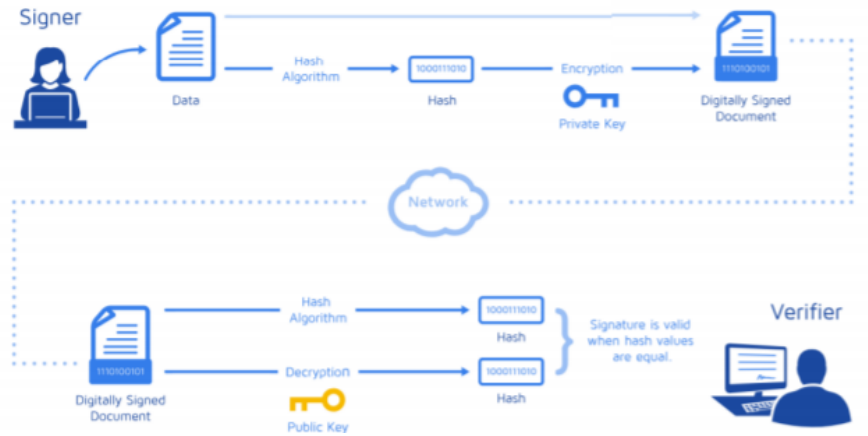
Cofinanciado por:

POCH PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

IPL instituto politécnico de leiria

Assinaturas e certificados digitais (1)

Quando se cria uma hash de um conjunto de dados para autenticar uma mensagem apenas estamos a garantir a integridade dos dados.



Integridade: Os dados são os originais

Autenticidade: Sabemos de onde vêm

Não repúdio: Sabemos quem os enviou

Uma assinatura digital garante a integridade dos dados, o não repúdio e a autenticidade da mensagem:

• O emissor cria uma hash da mensagem e cifra-a com a sua chave privada enquanto o recetor a decifra utilizando a chave pública do emissor.

Cofinanciado por:
POCH PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

Assinaturas e certificados digitais (2)

Um certificado digital é um documento eletrónico utilizado para identificar uma entidade (indivíduo, equipamento, empresa, etc…) e que lhe associa uma chave pública.

Quem valida a identidade e gera esses certificados é uma CA (Autoridade de Certificação), que atua como terceiro membro na comunicação e assegura que as chaves públicas utilizadas são fidedignas.

Um certificado tem o nome da entidade, a data de expiração e o nome da CA que emitiu o certificado.

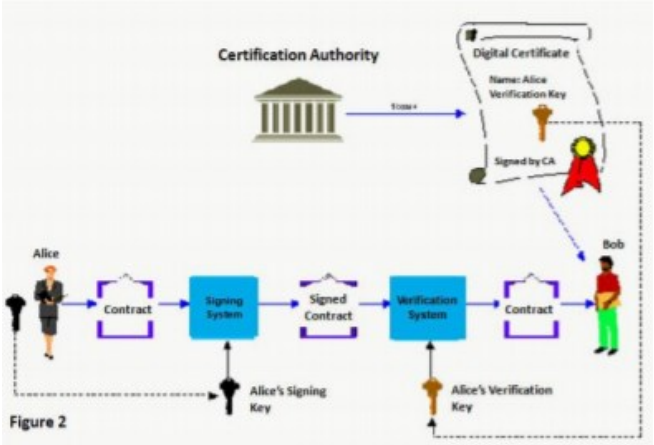


Figure 2

Cofinanciado por:
POCH PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

Assinaturas e certificados digitais (3)

Código em c# de exemplo para assinar:

```
using (SHA256CryptoServiceProvider sha256 = new SHA256CryptoServiceProvider())
{
        byte[] signature = rsa.SignData(Encoding.UTF8.GetBytes(“Texto para assinar!”),sha256);
}
using (SHA256CryptoServiceProvider sha256 = new SHA256CryptoServiceProvider())
{
        byte[] hash = sha256.ComputeHash(Encoding.UTF8.GetBytes(“Texto para assinar!”));
        byte[] signature = rsa.SignHash(hash,CryptoConfig.MapNameToOID("SHA256"));
}
```


Cofinanciado por:

Assinaturas e certificados digitais (4)

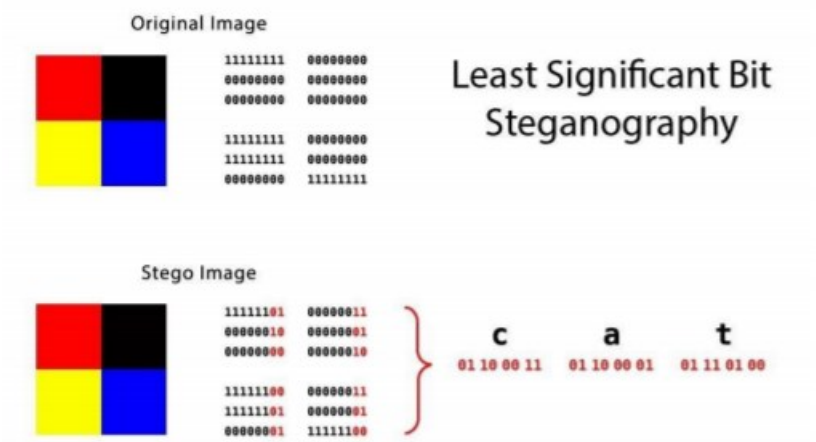
Código em c# de exemplo para verificar:

```
rsaRecipient = new RSACryptoServiceProvider();

rsaRecipient.FromXmlString(publicKey);

using (SHA256CryptoServiceProvider sha256 = new SHA256CryptoServiceProvider())

{

        bool verified = rsaRecipient.VerifyData(Encoding.UTF8.GetBytes(“Texto para assinar!”),sha256,Convert.FromBase64String(“54gfgdhsdsfsdfsdfdsfsg”));

}

using (SHA256CryptoServiceProvider sha256 = new SHA256CryptoServiceProvider())

{

        byte[] hash = sha256.ComputeHash(Encoding.UTF8.GetBytes(Texto para assinar!));

        bool verified = rsaRecipient.VerifyHash(hash, CryptoConfig.MapNameToOID("SHA256"), Convert.FromBase64String(“54gfgdhsdsfsdfsdfdsfsg”));

}
```


Cofinanciado por:

Esteganografia (1)

A esteganografia é a prática de esconder dados dentro de dados (texto, imagem ou vídeo dentro de texto, imagem ou vídeo).

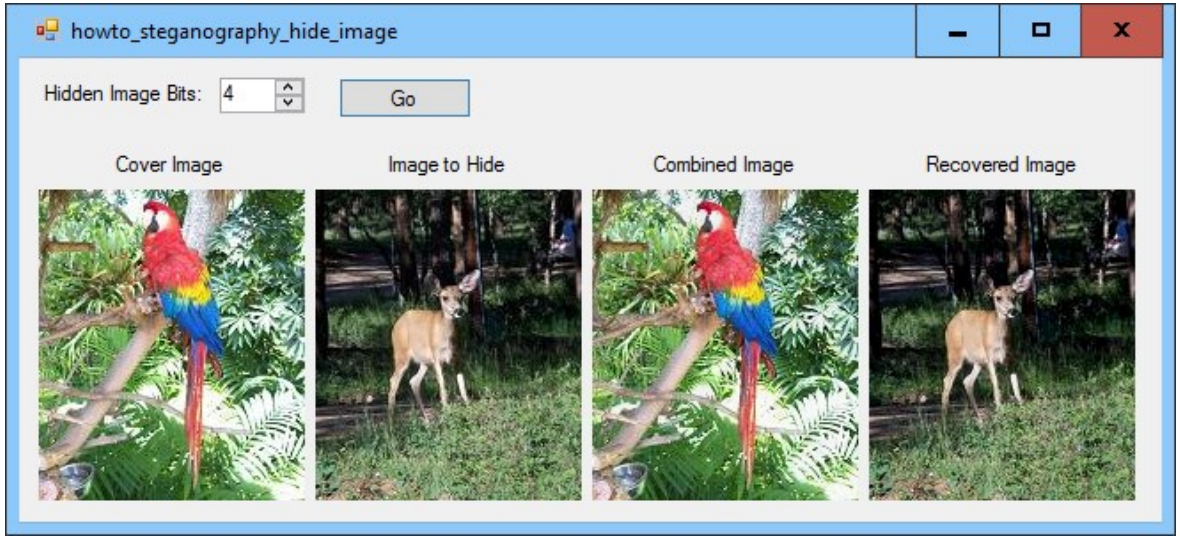


No mundo digital isto consegue-se através da manipulação de bits nos dados, seja por acrescento de bits ou pela modificação do bit menos significativo (LSB).

Cofinanciado por:
POCH PORTUGAL 2020 UNIÃO EUROPEIA Fundo Social Europeu

Esteganografia (2)

Esconder uma imagem dentro de uma imagem é possível



(http://csharphelper.com/blog/2016/09/use-steganography-to-hide-one-picture-inside-another-in-c/)

- Dependendo do tamanho do conteúdo a esconder pode ser praticamente impossível saber se a imagem tem dados escondidos ou não!

Cofinanciado por: