Criptografia: Parte 3

Key management

Imagine that we have N agents. The agents need to communicate between each other in a p2p way. But this will lead us to store `N(N-1)/2` keys in the system.

KDC (Key Distribution Center)

To avoid this, we might have a central entity, that will manage that key distribution in the system.

How can we make two peers communicate between each other?

We need to have **one key per user.** These are long term keys, since they will be used forever.

To A communicate with B, we can use the **KDC** to send the communication key o both computers

The big disadvantage is that we have a **central point of failure**.

Long term and ephemeral keys

Long term (longa duração)

Are the ones that are shared when a user logs in a system, for example, and will live for a long time. They have strong constraints to make their storage: hardware security module, smartcard, etc

Ephemeral messages

Messages that lately will be discarded. There are session keys.

Compromising a session key must not have any consequence to the remain part of the system. Only the data associated with these session must be in risk.

> Perhaps this is a kind of isolation.

Limitations of symmetrical cryptography

Problem 1

In a opened system it's necessary to communicate other computer that we don't know if we trust. Even if the source is trusted, symmetric keys requires that the key is pre-shared.

- **A solution** is to use **public keys** in async systems.
- **Another solution is** to use digital signatures and key according.

The communication sometimes is bidirectional and we need to exchange keys. Using public keys in this type of situation adds a big overhead.

Problem 2 (não repúdio)

It means that lately we cannot deny the reception of a document from another machine.

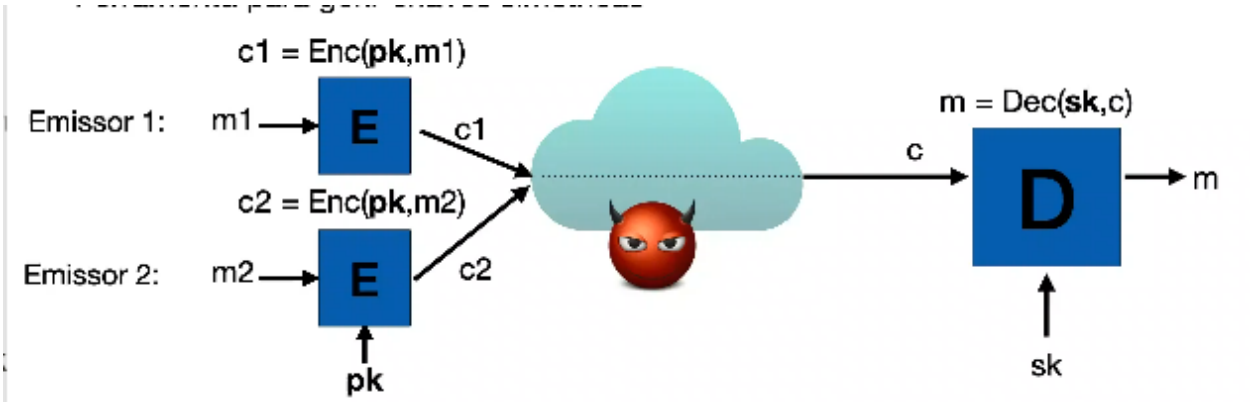
How do we know if another person has the key and falsified the message?

We can use digital signatures.

Public keys (asymmetric)

This is used to solve the problem of sharing keys. Nowadays is mainly used to transport symmetric keys from one computer to another.

Anyone can know the public key.



> There’s one person that knows more than the others. That’s why the name is private key.

We can use the public key to encrypt the message, but only the person with the private key can decrypt it.

Paradigma híbrido: emissor gera chave de sessão **simétrica** e usa essa chave para cifrar a mensagem. Depois usa-se a chave pública do destinatário para cifrar a chave da sessão e manda-se os dois.

Como construir cifra de chave pública [não sai]

Na verdade hoje em dia a cifra de chave em pública só é utilizada no email, já que não muito eficiente.

One-way trapdoor permutation **não é uma cifra,** porque *aparentemente não o fator aleatorio. Se tivermos uma mensagem que pode ser sim ou não, podemos descobrir facilmente seu conteúdo, verificando se a permutação de sim é igual a mensagem.*

One-way trapdoor permutation

KeyGen: produzir pk, sk

Eval: y = F(pk,x)

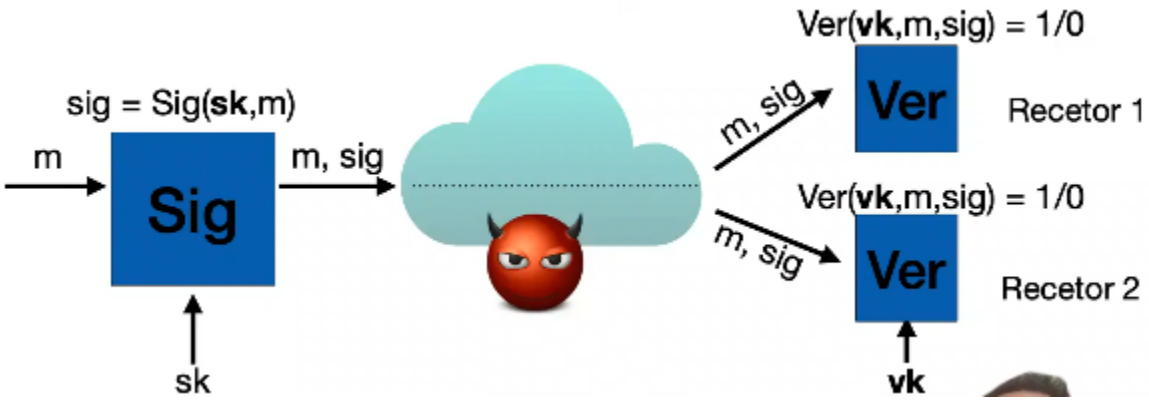
Invert: $x = F^{-1}(sk,y)$

Permutação:
- conhecendo sk
- dado F(pk,x)
- é possível recuperar x

One-way:
- se x for aleatório
- F(pk,x) é difícil de inverter
- mesmo conhecendo pk

Assinatura digital

As assinaturas garantem que a autenticação e integridade (já que não é possível alterar o documento depois da assinatura).



Temos dois tipos de chaves:

- **Chave de assinatura:** é a chave secreta

- **Chave de verificação:** que é a chave conhecida por todos, usada para verificar a autenticação.

Ter uma chave que é conhecida por várias pessoas destrói o princípio do repúdio. Porque MAC tem repúdio?

Note que as assinaturas de digitais funcionam de forma contrária as chaves públicas. Nas chaves públicas apenas uma pessoa pode receber a mensagem, nas assinaturas digitais vários podem receber a mensagem, mas apenas um pode enviar. *Isto lembra um pouco publisher/subscriber (assinaturas digitais) e push/pull (chaves públicas).*

As assinaturas digitais possuem algumas propriedades:

- Não é possível falsificar, reutilizar e não é repudiável.
- Garantia de autoria do documento
- Documento não pode ser alterado depois da assinatura.

No entanto as garantias também dependem de alguns pressupostos:

- Chave de assinatura não comprometida
- Algoritmo de assinatura criptograficamente seguro
- Chave pública (aquela que verifica) é autentica.

Mas como podemos verificar se a assinatura que é usada para verificação vem da pessoa certa?

Como contruir uma assinatura digital?

O algoritmo de RSA é muito lento do que assinaturas com base em curvas elípticas (ECDSA). tem chaves públicas mais pequenas.

Envelopes digitais

Combinamos assinaturas digitais e cifras assimétricas.

Tinhamos visto que há vantagens em autenticarmos o conteúdo já cifrado (porquê isto evita que código malicioso fique em memória durante a verificação). Para garantir não repúdio de envelopes precisamos assumir que se saiba qual é o conteúdo da mensagem.

> Analogia do envelope, não faz sentido uma pessoa assinar um envelope lacrado sem saber o que está la dentro.

Por isso, para garantir o não repúdio, precisamos na verdade assinar o conteúdo digital e só depois cifrar.

Perguntas

1) O que é o KDC? Como o KDC faz com que duas outras máquinas possam estabelecer um comunicação segura?

▼ Resposta

É uma máquina central que possui chaves pré-definidas com outras máquinas. Este componente central estabelece a comunicação entre outras duas máquinas conectadas a ela. Imagine que **Alice** e **Bob** queiram falar entre si. Ambos possuem chaves pré partilhadas com o KDC. O KDC usa a sua comunicação segura para enviar a chave simétrica para a comunicação entre **Bob** e **Alice.**

2) Quais são as limitações das chaves simétricas? Explique.

▼ Resposta

As chaves simétricas não garantem autenticidade e integridade, já que não há nenhum tipo de confirmação sobre quem enviou a mensagem. ~~Além disso precisam ser pré-partilhadas.~~ Além disso, não garantem o não repúdio. O não repúdio consiste em provar para uma third-party (C) de que a mensagem foi enviada por uma certa pessoa (A). No entanto, (C) pode alegar que já que (B) conhece o conteúdo da mensagem, porque possui a key, (B) poderia ter alterado o conteúdo.

3) Como podemos utilizar chaves públicas para transmitir a chave da cifra simétrica? Porque este tipo de comunicação não garante autenticidade?

▼ Resposta

Imagine que **Alice** (A) deseja estabelecer uma comunicação com **Bob** (B) e enviar uma chave simétrica para este. **A** vai encriptar a mensagem com a chave pública de **B** e como apenas **B** possui a chave privada, apenas ele consegue desencriptar o conteúdo. A chave pública é disponível para qualquer um e por isso este de

comunicação não garante autenticidade: há ainda a possibilidade de haver um man-in-the-middle na comunicação **Bob** e **Alice.**

4) O que é o paradigma híbrido?

▼ Resposta

O paradigma híbrido é uso em conjunto de chaves públicas e privadas para transferir chaves simétricas.

5) Explique a assinatura digital. Quais são as suas garantias?

▼ Resposta

As assinaturas digitais garantem autenticidade e integridade. Temos dois tipos de chaves em assinaturas digitais: chaves de verificação e chaves de assinatura. As chaves de verificação são públicas e chaves de assinatura são privadas. Quando um agente assina uma mensagem, outras pessoas podem verificar a assinatura. Não é possível alterar o conteúdo da mensagem sem alterar a assinatura.

6) Explique a analogia do envelope. Como esta analogia explica o não repúdio de assinaturas digitais?

▼ Respota

A analogia do envelope serve para explicar o porquê de ser necessário fazer primeiramente a assinatura e só então a encriptação. A analogia explica que se primeiro encriptamos a mensagem e só depois assinamos é a mesma coisa de assinarmos um envelope lacrado sem saber o seu conteúdo. Encriptar e depois assinar permite que alguem alegue que assinou uma mensagem sem saber o seu conteúdo.

7) Atualmente “garantimos” ou alegamos que as assinaturas manuais possuem algumas propriedades. As assinaturas digitais procuram garantir estas mesmas. Quais são?

▼ Resposta

Não repudiável
Não falsificável
Não reutilizável

8) Quais são as vantagens de se utilizar assinaturas digitais e não MACs?

▼ Resposta

Não necessitam chave pré partilhada
Garantem o não repúdio

9) Por que MAC não garante o não repúdio?

▼ Resposta

Ver questão 2.