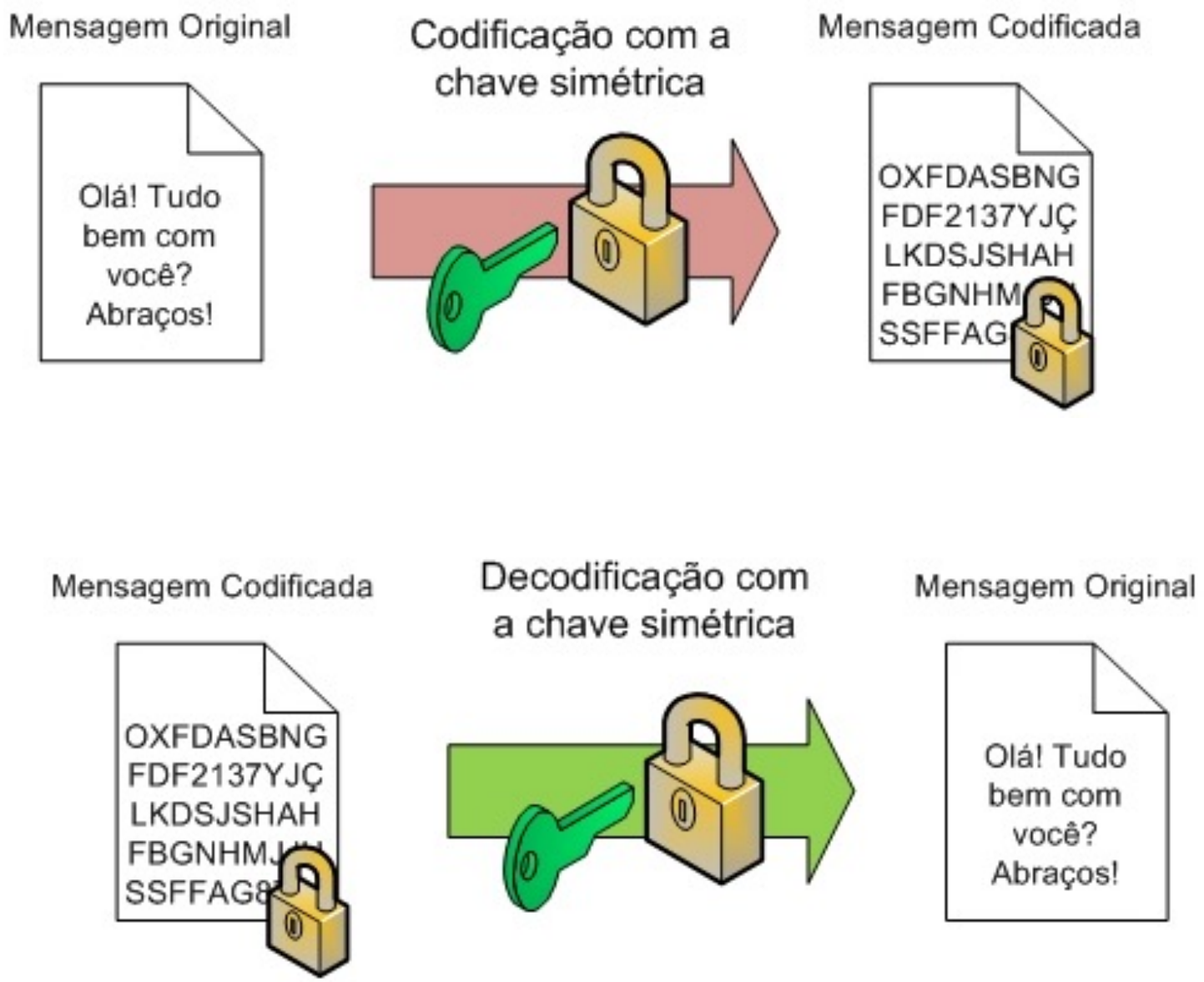
CC8130
Segurança no desenvolvimento de Software

Criptografia

centro universitário FEI

Prof. Dr. Ricardo Destro
2º Semestre de 2020

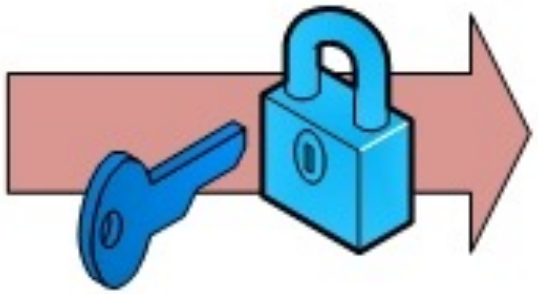


centro universitário FEI

Mensagem Original

Olá! Tudo bem com você? Abraços!

Codificação com a chave assimétrica



Mensagem Codificada

OXFDASBNG
FDF2137YJÇ
LKDSJSHAH
FBGNHM
SSFFAG

Mensagem Codificada

OXFDASBNG
FDF2137YJÇ
LKDSJSHAH
FBGNHMJ
SSFFAG8

Decodificação com a chave assimétrica

Mensagem Original

Olá! Tudo bem com você? Abraços!

centro universitário FEI

Geração das chaves

- **Números Aleatórios**
  - Distribuição Uniforme
  - Valores não predizíveis
  - Cadeia longa e integralmente alcançavel

- SSL no Netscape
  - http://www.cs.berkeley.edu/~daw/papers/ddj-netscape.html
- CodeRed II
  - http://en.wikipedia.org/wiki/Code_Red_(computer_worm)
- ASF Texas Hold´em
  - http://www.onlinecasinoreports.com/news/theheadlines/2004/3/21/flaw-in-asfs-software.php

- **FIPS 140-1 e 186-2**
- **NIST Special Publication 800-90A (Janeiro/2012)**

- **CryptGenRandom** (Desktop APP)
  - http://msdn.microsoft.com/en-us/library/windows/desktop/aa379942(v=vs.85).aspx

centro universitário FEI

Requisitos de segurança
Módulos de criptografia

- Federal Information Processing Standards
- FIPS 140-1
  - Testes de Aleatoriedade
    - Gerar uma sequencia de 20.000 bits aleatórios

centro universitário FEI

Requisitos de segurança
Módulos de criptografia

- Testes de Aleatoriedade

The Monobit Test

1. Count the number of ones in the 20,000 bit stream. Denote this quantity by X.

2. The test is passed if $9{,}654 < X < 10{,}346$.

The Poker Test

1. Divide the 20,000 bit stream into 5,000 contiguous 4 bit segments. Count and store the number of occurrences of each of the 16 possible 4 bit values. Denote $f(i)$ as the number of each 4 bit value i where $0 \le i \le 15$.

2. Evaluate the following:

$$X = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

3. The test is passed if $1.03 < X < 57.4$.

centro universitário FEI

Requisitos de segurança
Módulos de criptografia

- Testes de Aleatoriedade

The Runs Test

1. A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros, which is part of the 20,000 bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (≥ 1) in the sample stream should be counted and stored.

2. The test is passed if the number of runs that occur (of lengths 1 through 6) is each within the corresponding interval specified below. This must hold for both the zeros and ones; that is, all 12 counts must lie in the specified interval. For the purpose of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	*Required Interval*
1	2,267 - 2,733
2	1,079 - 1,421
3	502 - 748
4	223 - 402
5	90 - 223
6+	90 - 223

The Long Run Test

1. A long run is defined to be a run of length 34 or more (of either zeros or ones).

2. On the sample of 20,000 bits, the test is passed if there are NO long runs.

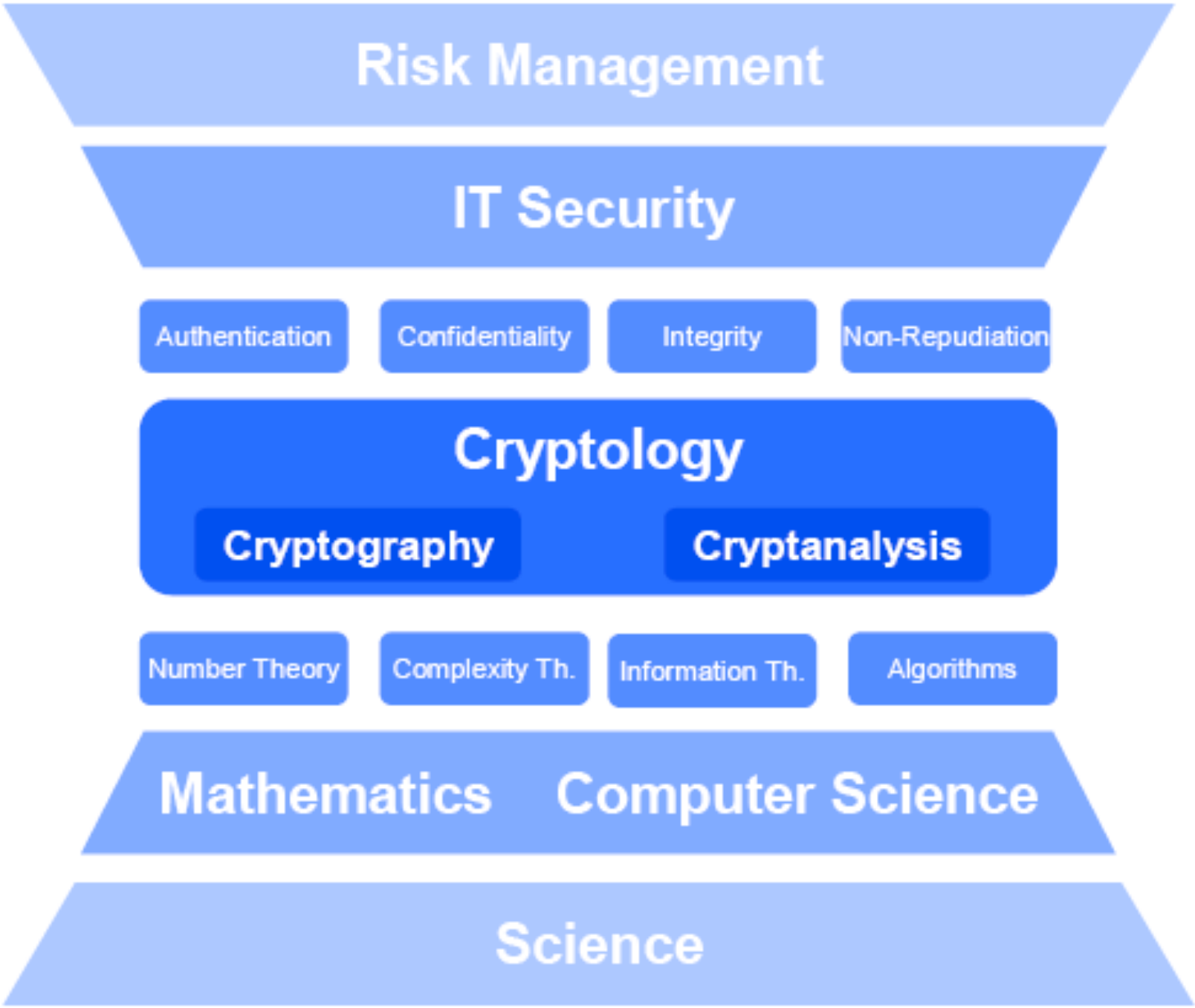
centro universitário FEI

Chaves de Criptografia

- **Short-term**

- **Long-term**

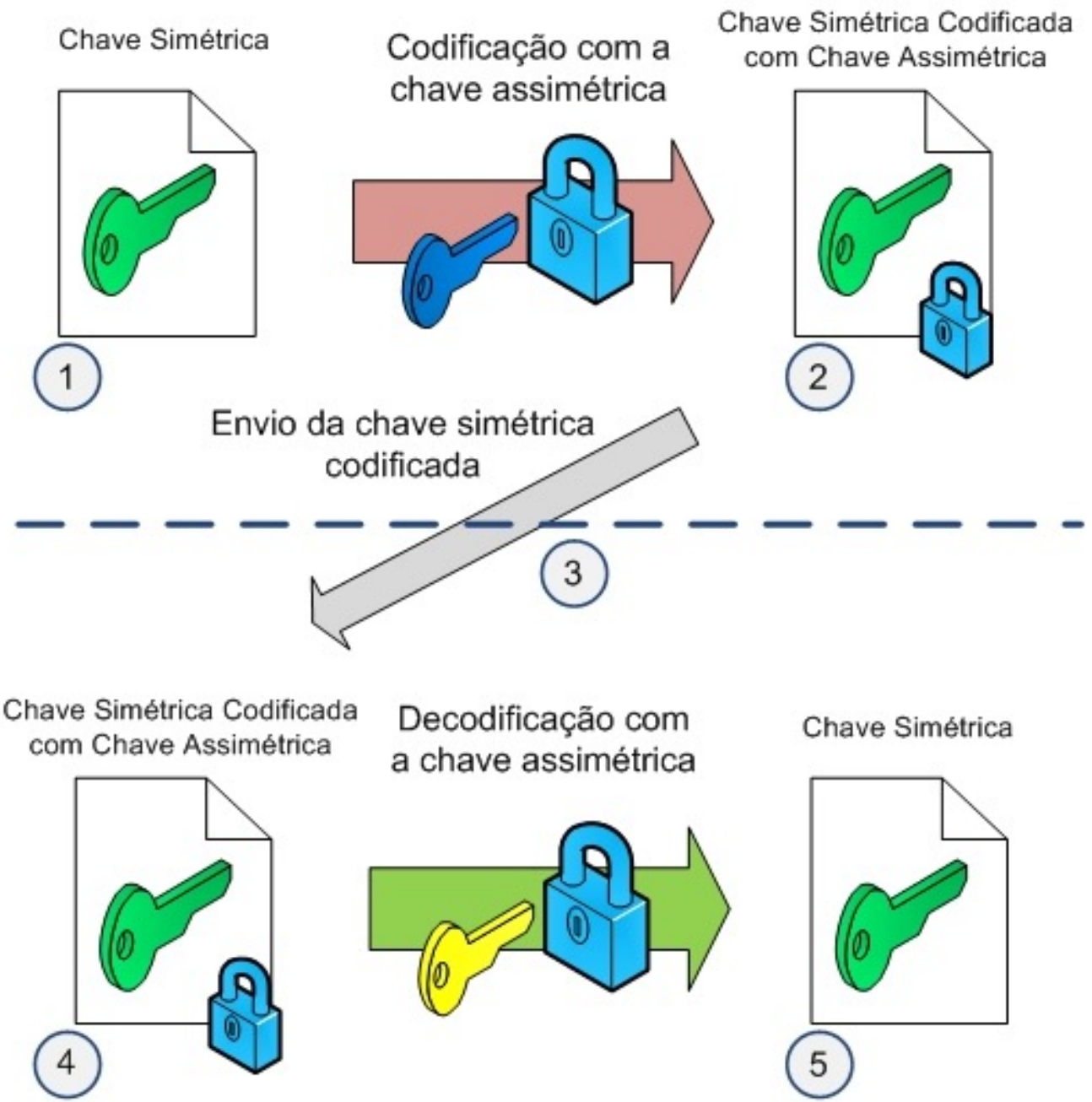
centro universitário FEI



centro universitário FEI

#ficadica

O que é isso?



centro universitário FEI

CC8130
Segurança da informação

SSL – Secure Socket Layer

centro universitário FEI

Prof. Dr. Ricardo Destro
1º Semestre de 2020

Secure Socket Layer (SSL)

- Versão 3.0 disponível em:
  - https://tools.ietf.org/html/rfc6101
-

- Objetivos:

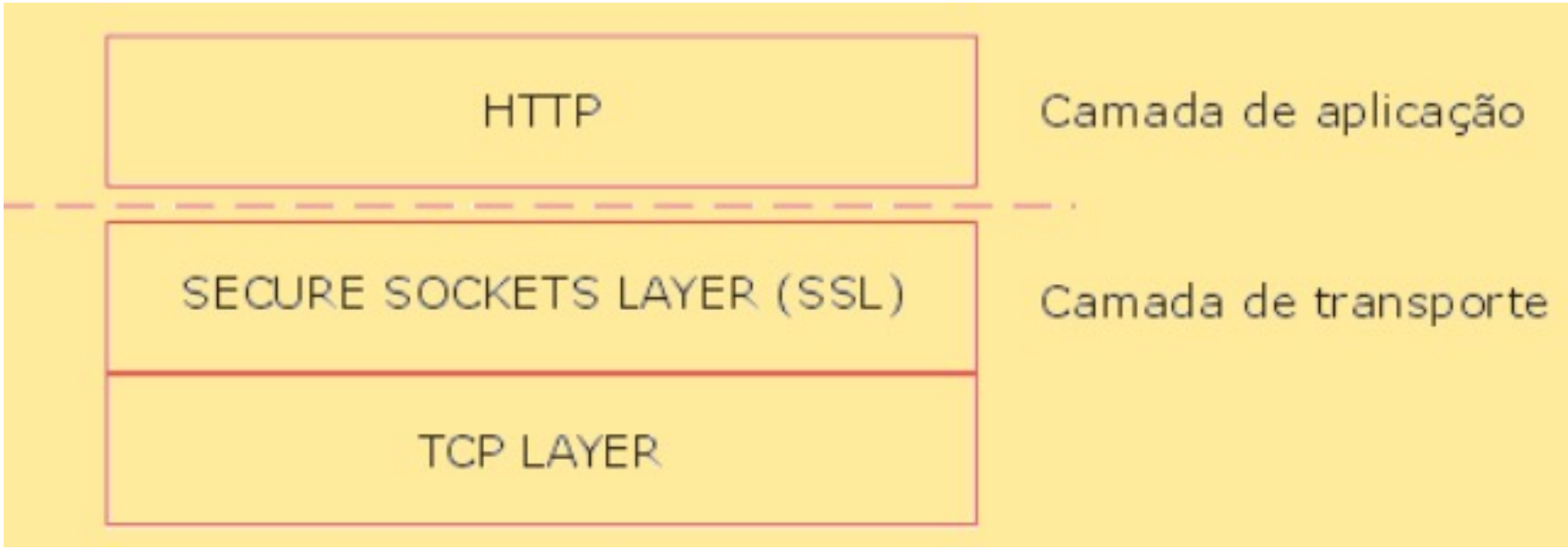
  Cryptographic security: estabelecer conexão segura entre duas dois atores

  Interoperability: independência de implementação entre as várias plataformas

  Extensibility: permitir a inclusão de novos algoritmos de criptografia

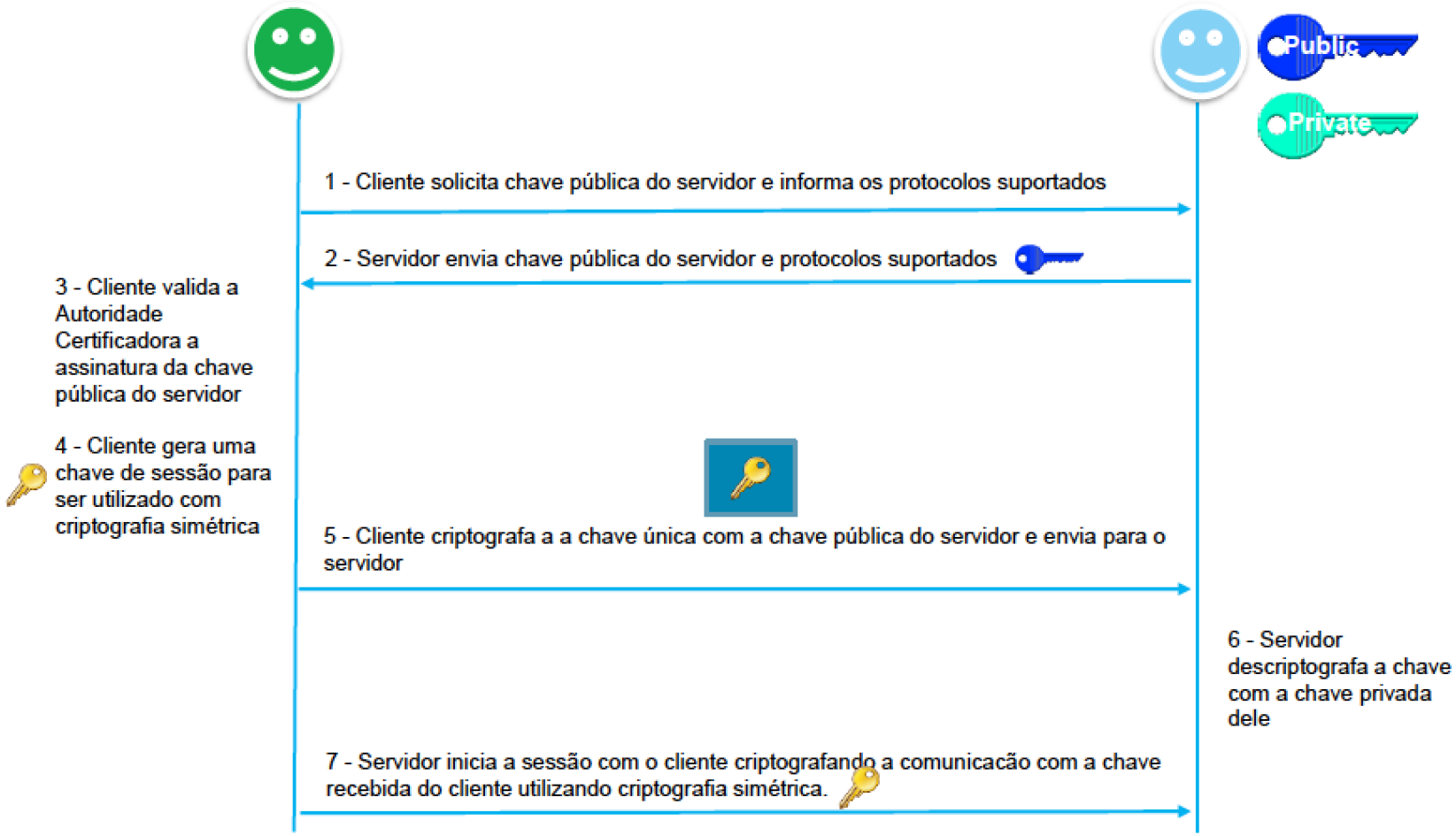
  Efficiency: reduzir o consumo de CPU e tráfego de rede (caching scheme)

centro universitário FEI


HTTP
Camada de aplicação
SECURE SOCKETS LAYER (SSL)
Camada de transporte
TCP LAYER

SSL - Simplificado

- SSL/TLS (Hybrid)



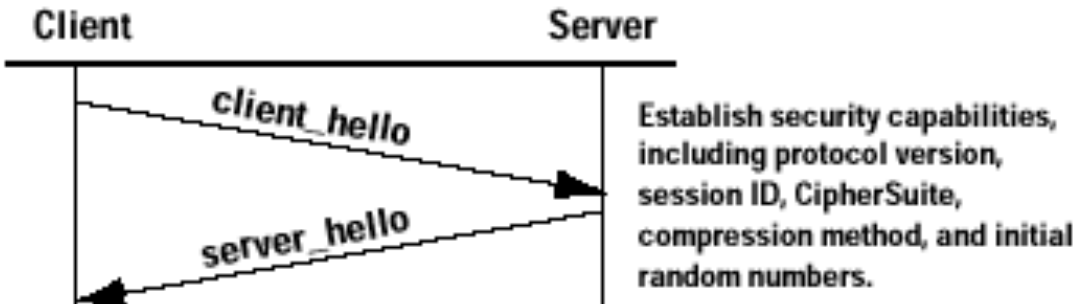
centro universitário FEI

Secure Socket Layer (SSL)

- Desenvolvido pela Netscape com o intuito de possibilitar o envio de informações criptografadas pela Internet.

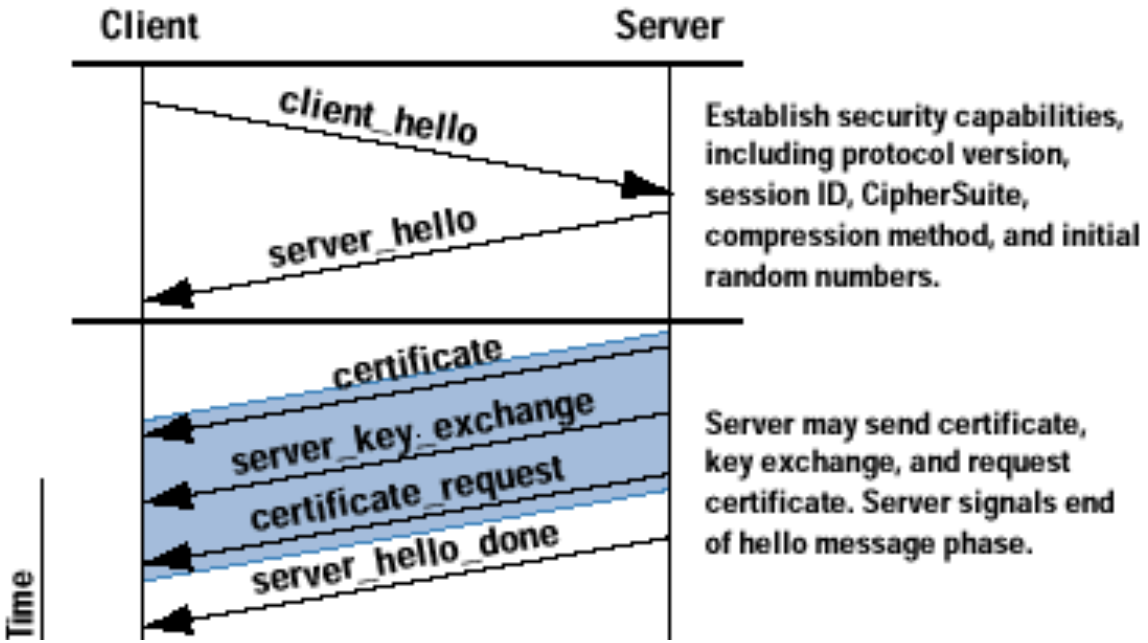
- Funciona como uma camada adicional entre as camadas inferiores do protocolo TCP/IP e a camada de aplicação. Ele adiciona à capacidade de envio de fluxo de informações do protocolo TCP/IP as seguintes características:
  - autenticação e não repudiação do servidor e do cliente através do uso de assinaturas digitais;
  - confidencialidade de dados através da criptografia;
  - integridade de dados através de códigos de autenticação de mensagens.

centro universitário FEI


Client
Server
client_hello
server_hello
Establish security capabilities, including protocol version, session ID, CipherSuite, compression method, and initial random numbers.

SSL - Funcionamento 1

- **1.** *client hello message*
  - versão do protocolo SSL que deseja utilizar
  - relação do conjunto de algoritmos de criptografia e compressão de dados suportados pelo cliente
  - identificador a sessão de comunicação entre o servidor e o cliente.
- **2.** *server hello message*
  - algoritmos de compressão e criptografia escolhidos pelo servidor
  - Caso o servidor não responda a mensagem inicial do cliente, o processo de abertura de conexão é abortado.

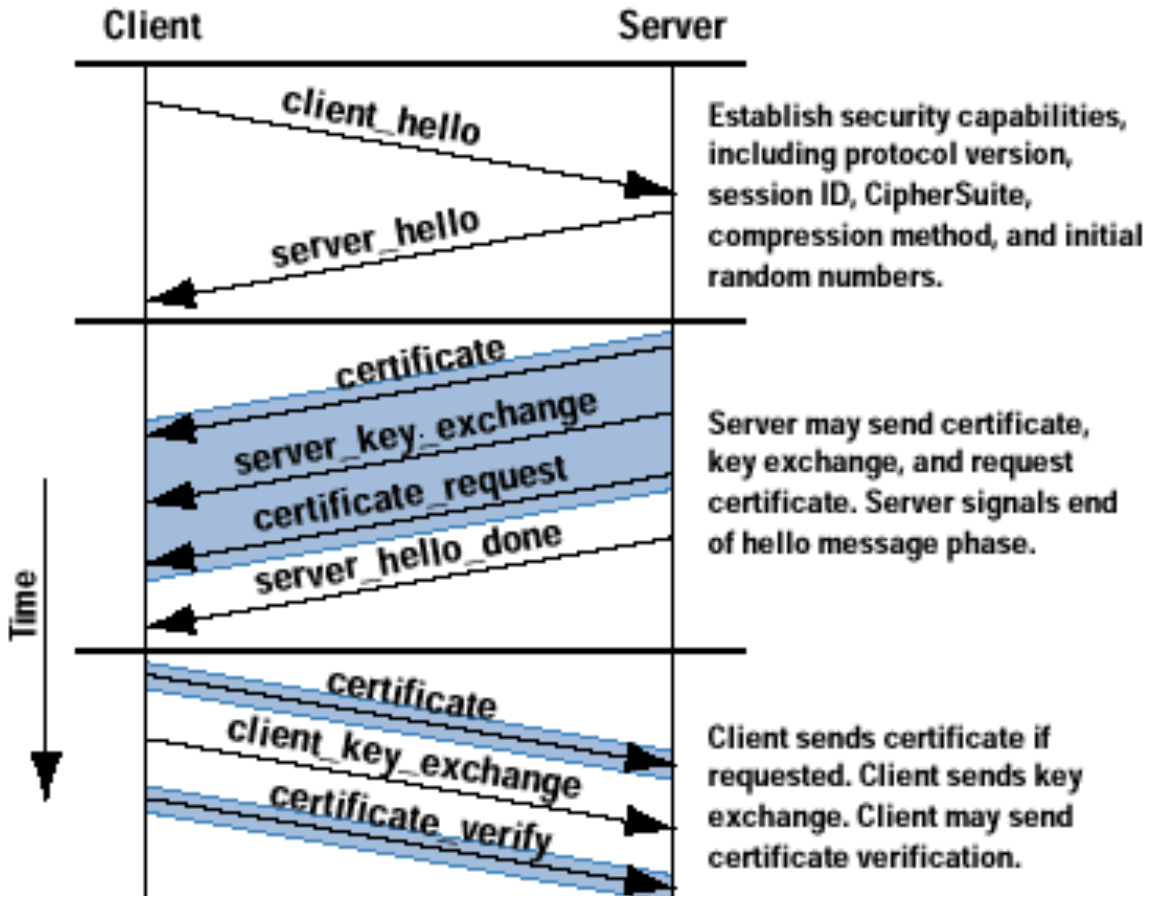

Client
Server
client_hello
server_hello
Establish security capabilities, including protocol version, session ID, CipherSuite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time

SSL - Funcionamento 2

- Após enviar a mensagem *hello*, o servidor envia seu certificado digital (chave publica) para que o cliente possa autenticar o servidor com o qual irá se conectar.

- Depois que o servidor enviou o seu certificado, este pode opcionalmente requerer o certificado digital do cliente. Somente um servidor autenticado pode requerer o certificado digital do cliente.

- O servidor envia uma mensagem (*hello done*) indicando que o processo de especificação dos protocolos de criptografia da sessão foi finalizado. Após enviar esta mensagem, o servidor irá aguardar a resposta do cliente.

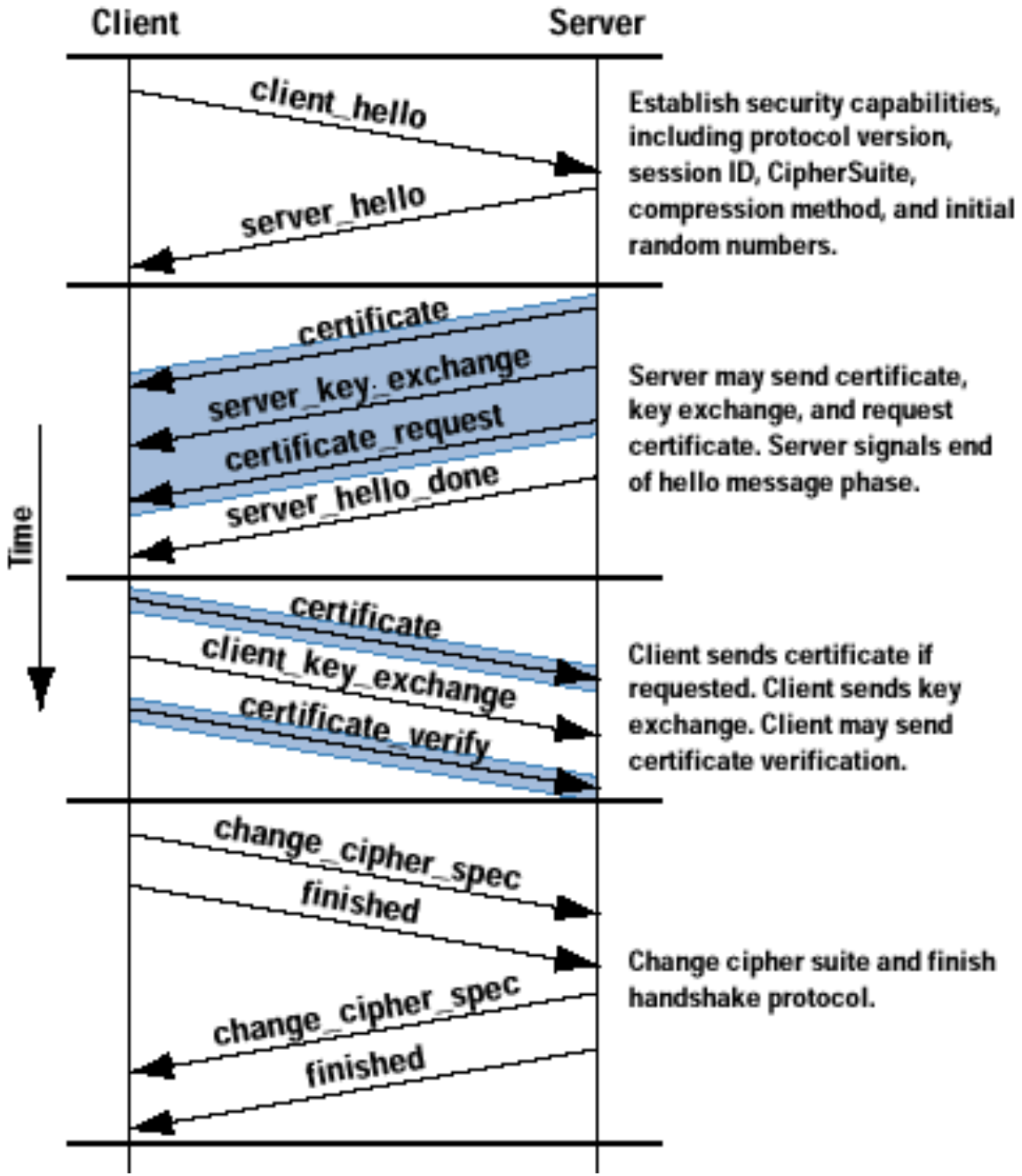


centro universitário FEI

SSL - Funcionamento 3

- Após receber a mensagem de *hello done*, o cliente irá validar o certificado do servidor e verificar se os parâmetros definidos na conexão são aceitáveis.
- Caso a autenticação do cliente seja requisitada, o cliente irá enviar seu certificado digital para o servidor ou uma mensagem indicando que não possui um certificado digital.
- O cliente gera então uma pré-chave (*pre-master secret*) e enviará a pré-chave criptografa com a chave pública do servidor (especificada no certificado digital) para este.

centro universitário FEI



centro universitário FEI

SSL - Funcionamento 4

- O cliente e o servidor podem agora gerar uma chave chamada *master secret* a partir da pré-chave, que será utilizada para gerar as demais chaves dos algoritmos de criptografia definidos anteriormente.

- Em seguida, o cliente envia duas mensagens para o servidor: uma mensagem (*change cipher message*) sinalizando que a comunicação passará a ser criptografa com os algoritmos de criptografia negociados e outra de *finished* indicando o término do processo de negociação e início do envio de dados.

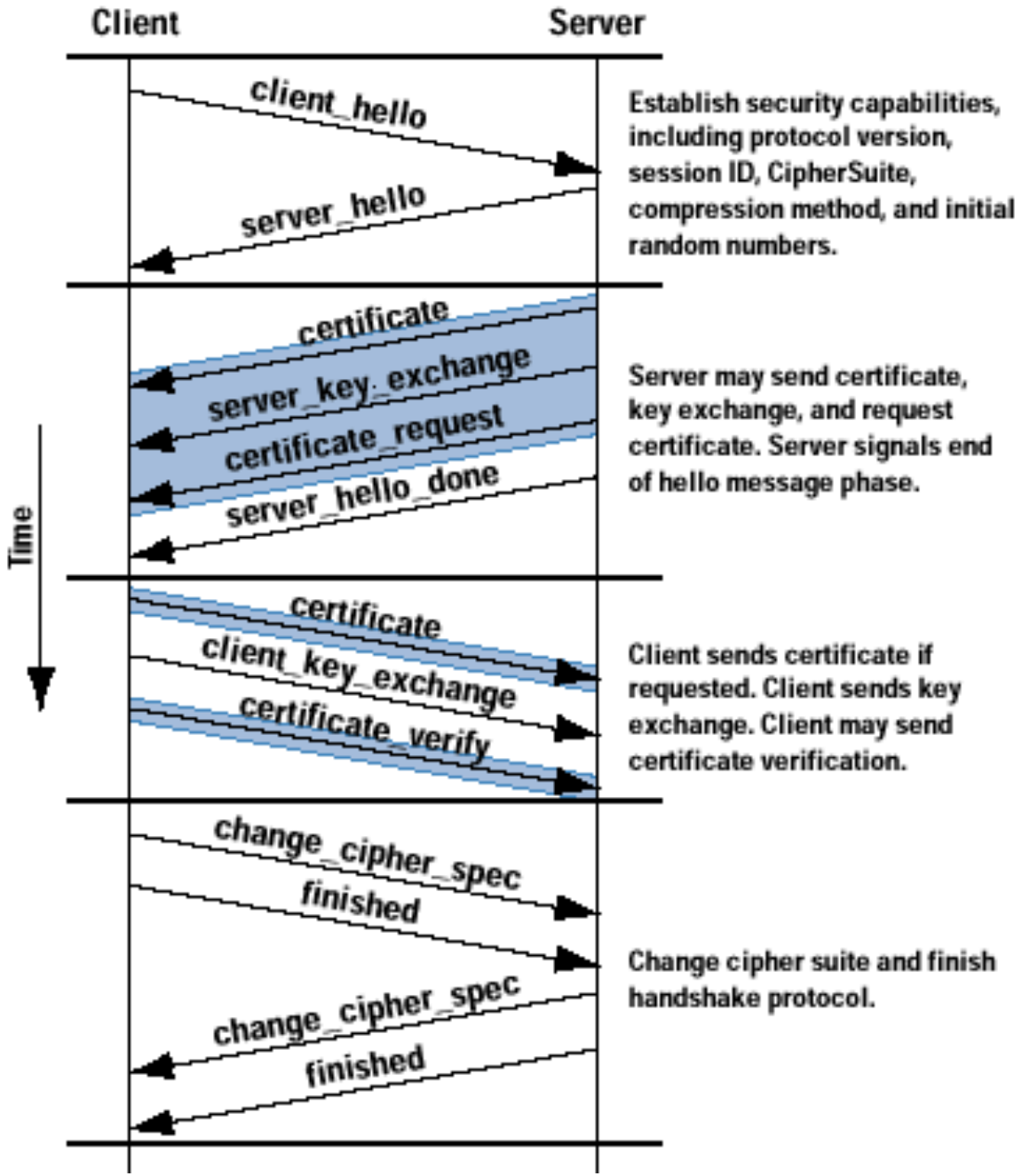
- O servidor responde enviando uma mensagem *change cipher message* (indicando que está pronto para receber mensagens criptografadas com o algoritmo negociado) e uma *finished* (indicando que está sincronizado com o cliente e pronto para enviar e receber dados).

centro universitário FEI

SSL – Características

- Utiliza algoritmos e chaves diferentes para executar as funções de criptografia, autenticação, integridade de dados e autenticação;
- Utiliza um único par de chaves públicas e privadas durante as conexões com um determinado cliente;
- A autenticação do cliente e do servidor é feita através de certificados digitais emitidos por uma entidade certificadora;
- Oferece proteção contra ataques de interceptação de dados e reenvio de mensagens;
- Suporta compressão de dados.

centro universitário FEI

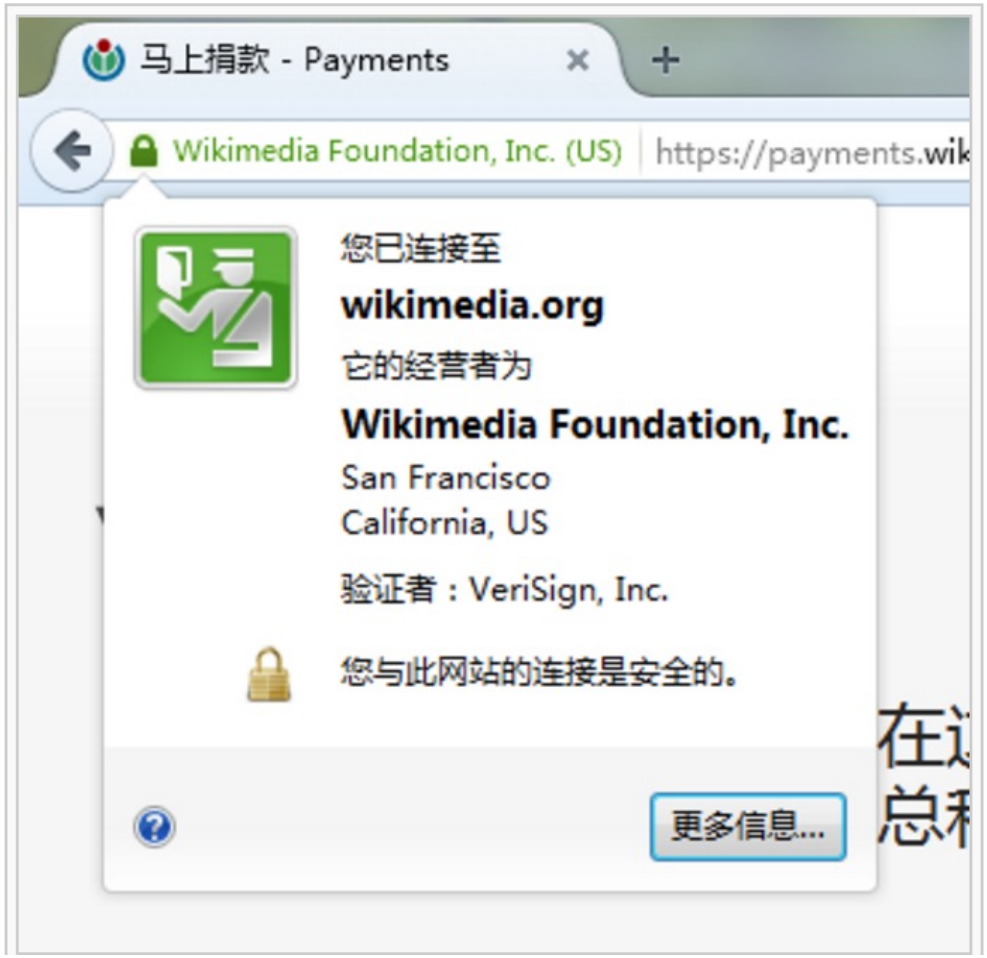


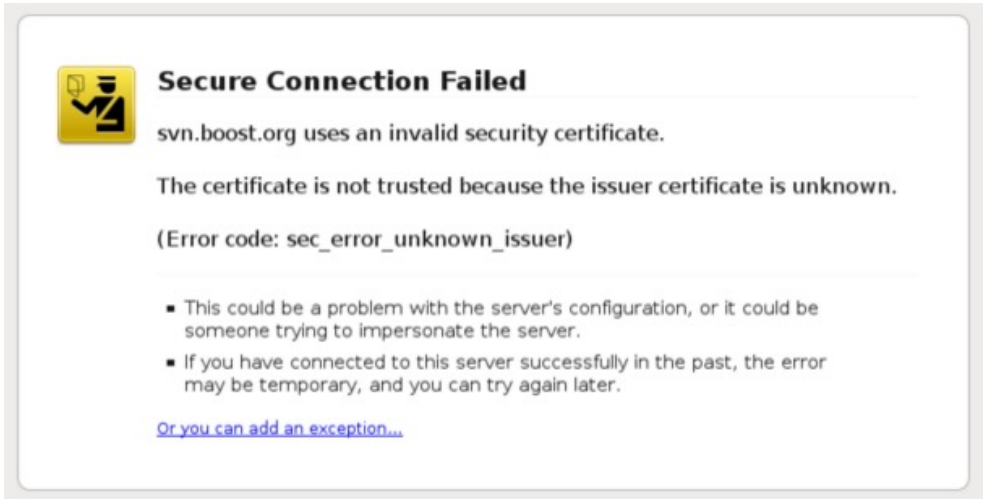
centro universitário FEI

Difusão do SSL

- Problemas?

Confia no certificado?





centro universitário FEI

centro universitário FEI

Algoritmos de criptografia

- **Standard**

- **Home made**

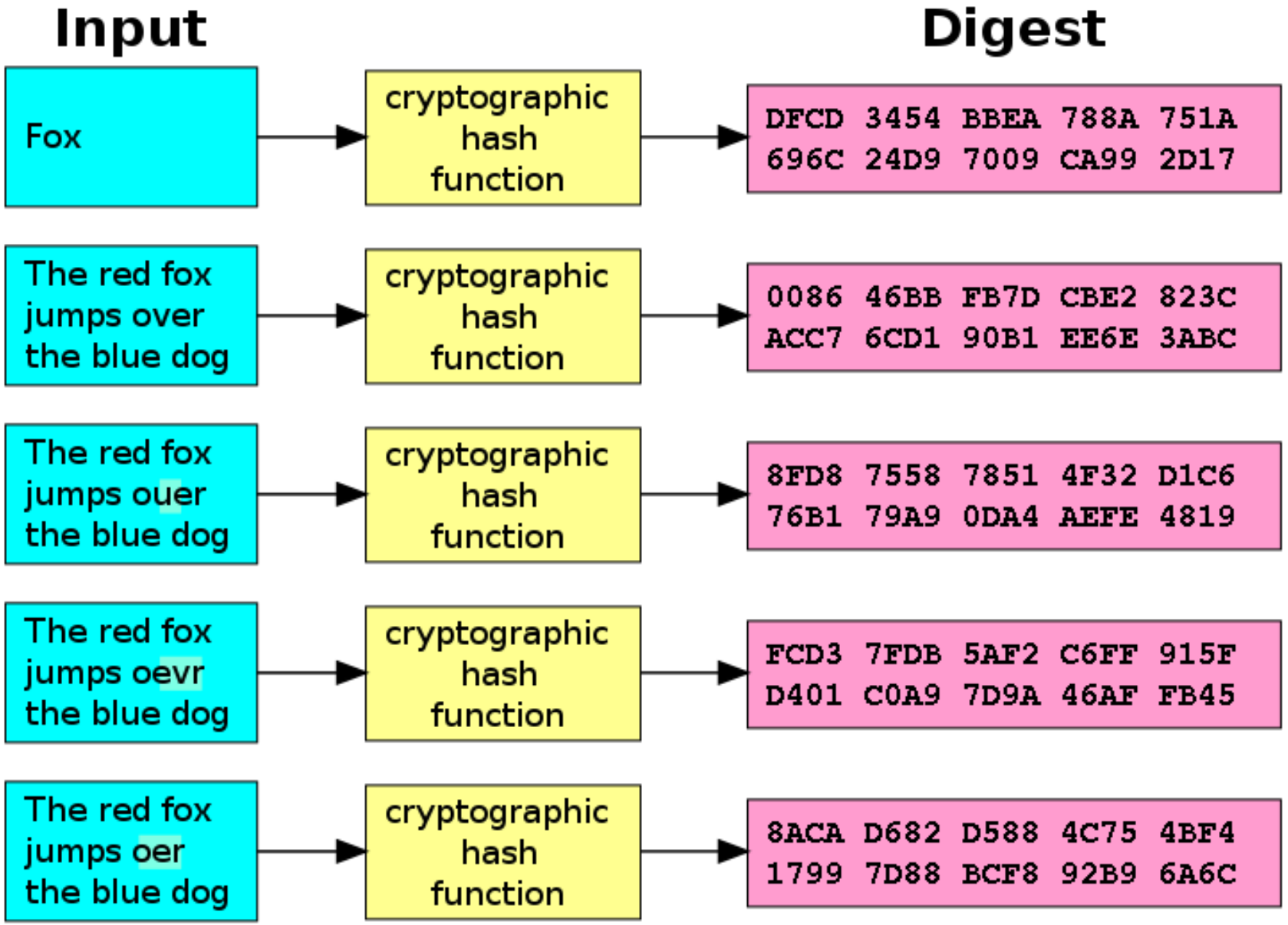
centro universitário FEI

CC8130
Segurança da informação

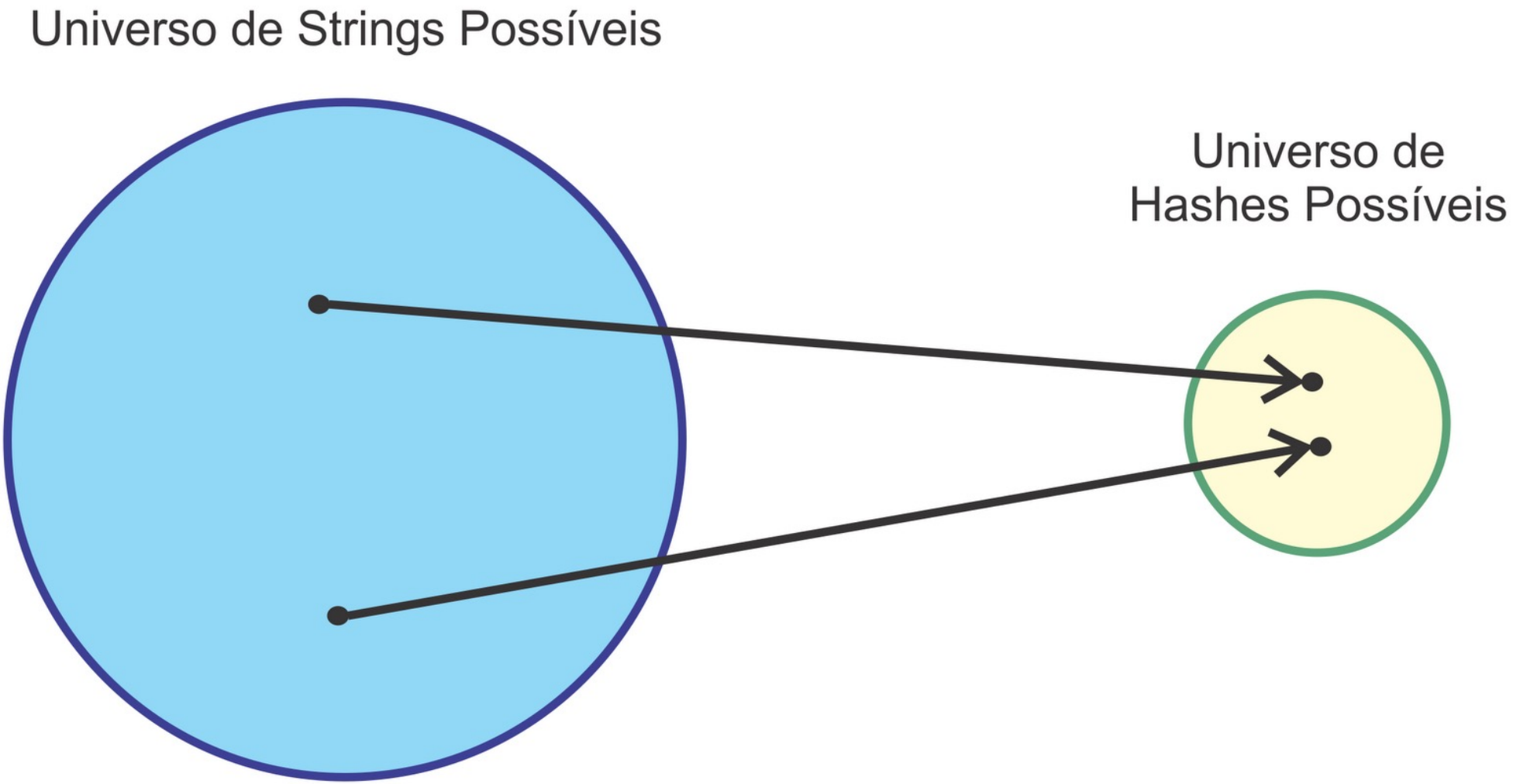
Função HASH
Assinatura Eletrônica

centro universitário FEI

Prof. Dr. Ricardo Destro
1º Semestre de 2020



centro universitário FEI


Universo de Strings Possíveis
Universo de
Hashes Possíveis

Função Hash

Requisitos para o uso em Criptografia:

Fácil de calcular o *valor Hash*;

Resistência à 1ª inversão, ou seja, é computacionalmente inviável, dado y, encontrar x tal que h(x) = y;

Resistência à 2ª inversão, ou seja, é computacionalmente inviável, dado x_1, encontrar $x_2 \neq x_1$ tal que $h(x_1) = h(x_2)$;

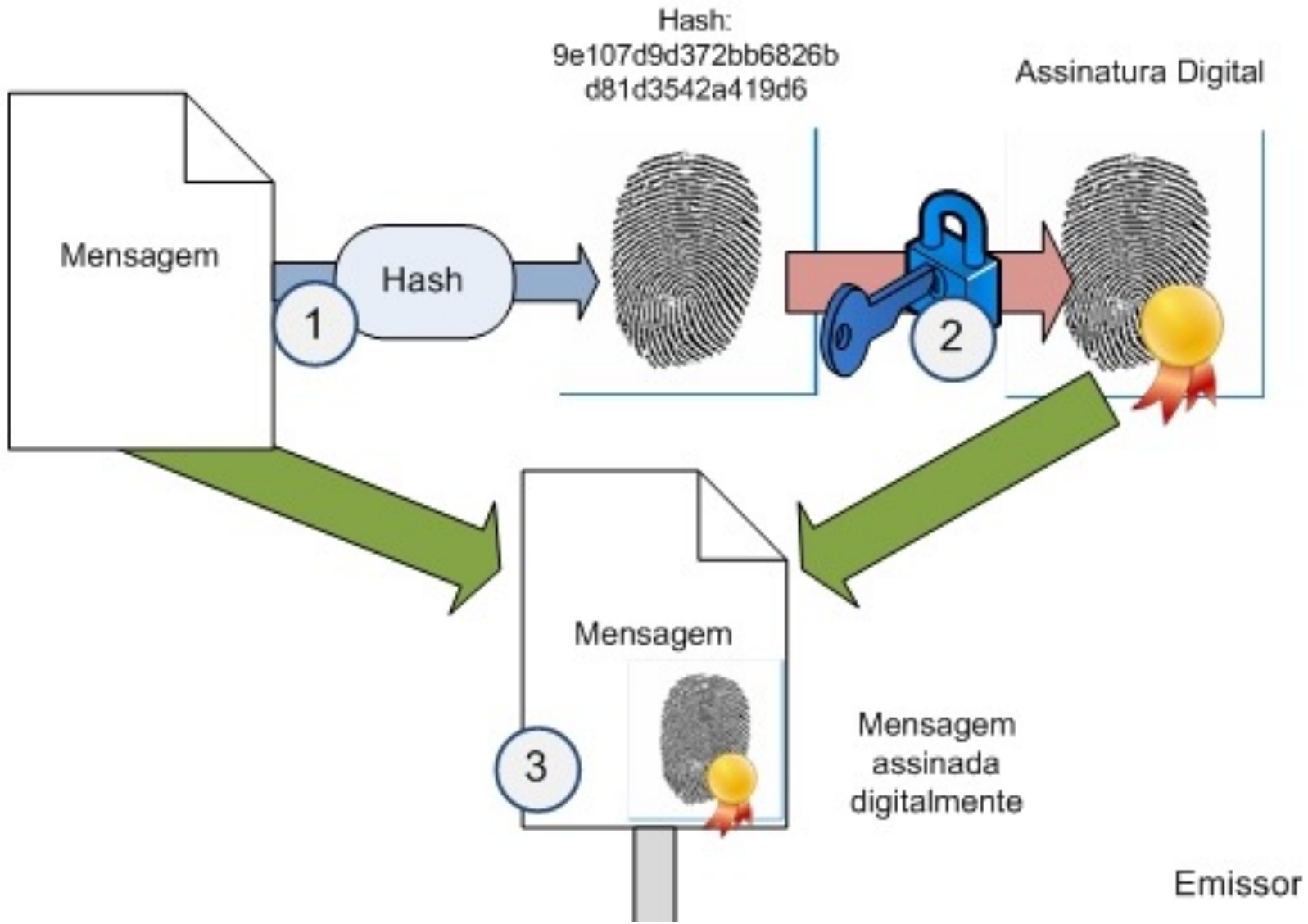
Resistência a colisões, ou seja, é computacionalmente inviável, encontrar quaisquer x_1 e x_2 tais que $h(x_1) = h(x_2)$.

centro universitário FEI

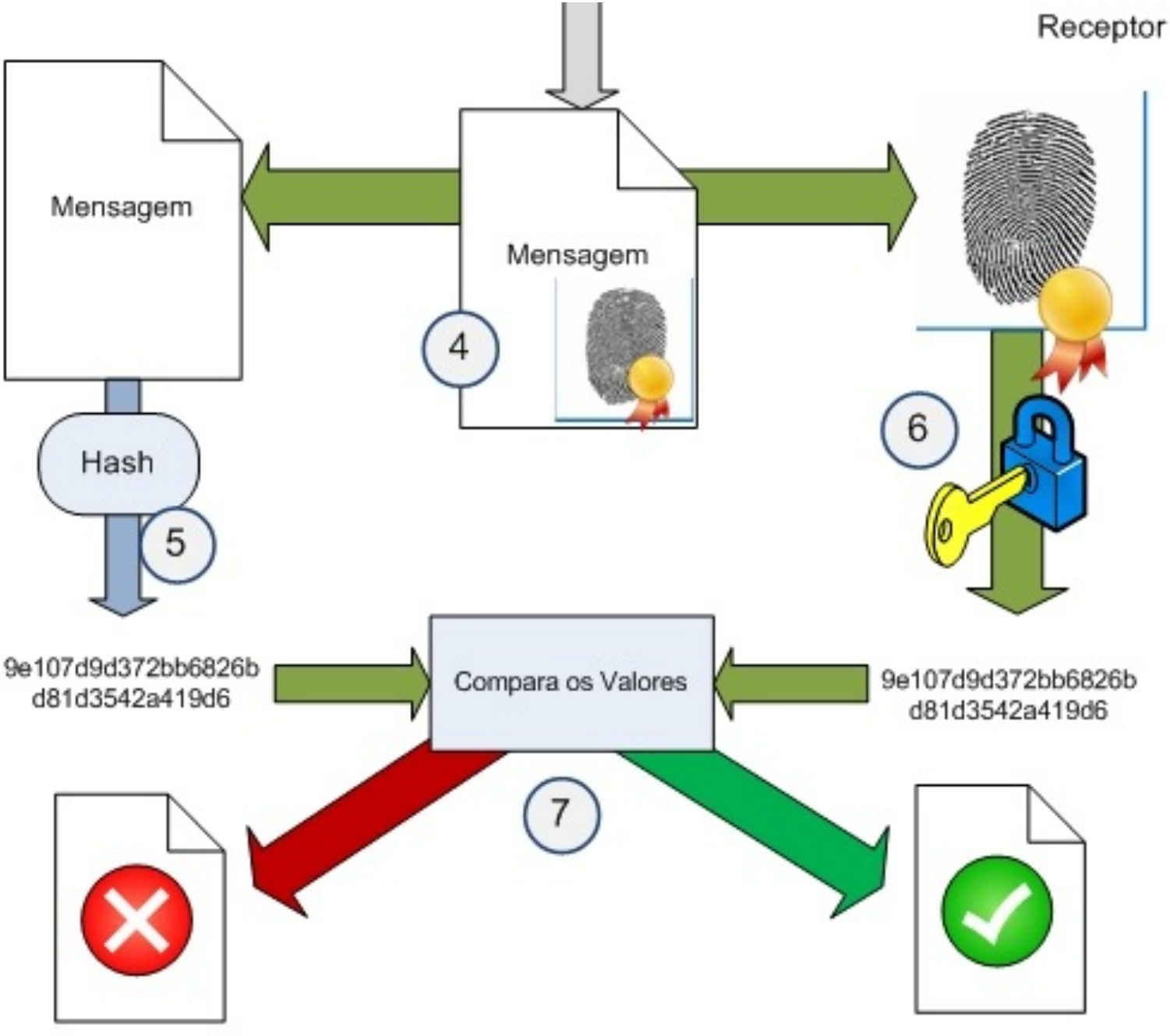
Função Hash

Algoritmo	Saída (bits)	Bloco (bits)	Messagem (bits)	Ciclos
MD5	128	512	$2^{64}-1$	64
SHA-0	160	512	$2^{64}-1$	80
SHA-1	160	512	$2^{64}-1$	80
SHA-2 256	256	512	$2^{64}-1$	64
SHA-2 512	512	1024	$2^{128}-1$	80

centro universitário FEI



centro universitário FEI



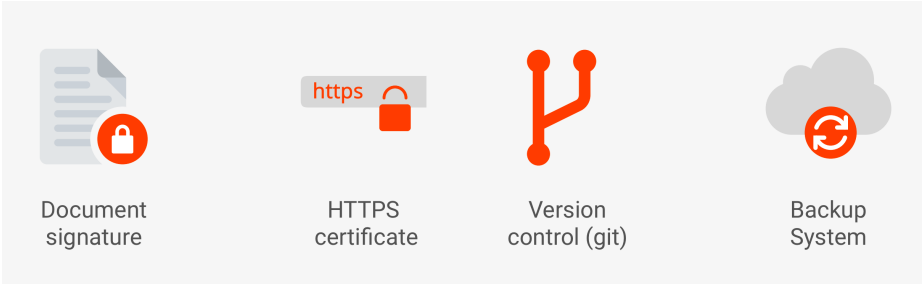
centro universitário FEI

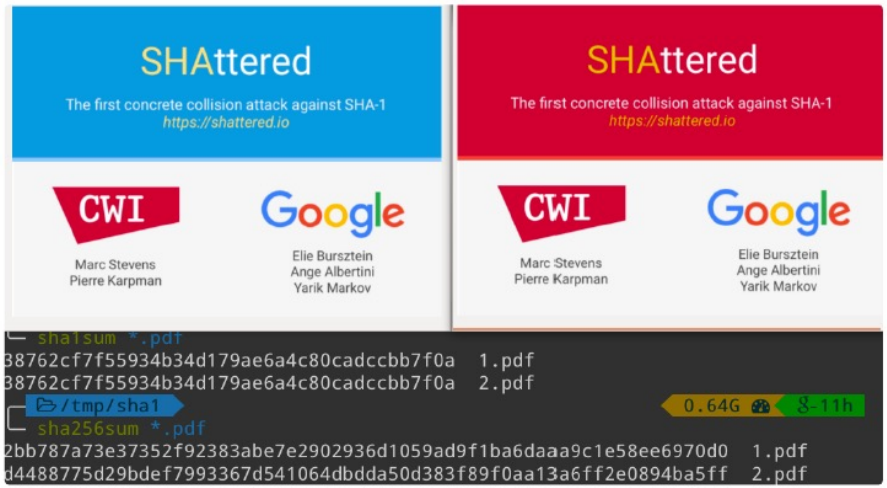
SHA1 Atacado

https://shattered.io/

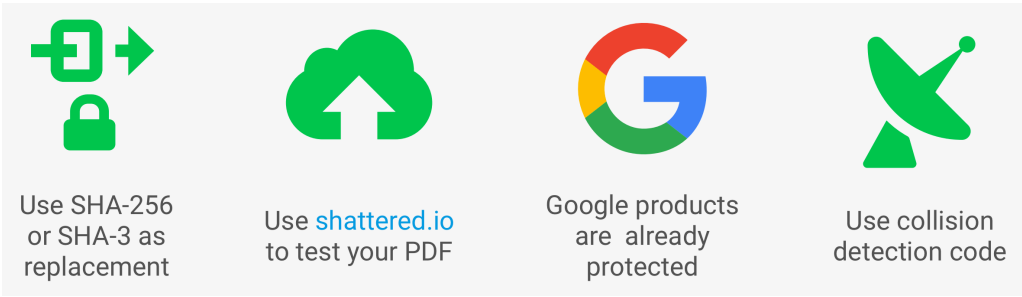
Ataques teóricos desde 2005
Descontinuado pelo NIST em 2011
Descontinuado pelo Chrome e Firefox em 2017

Impactados





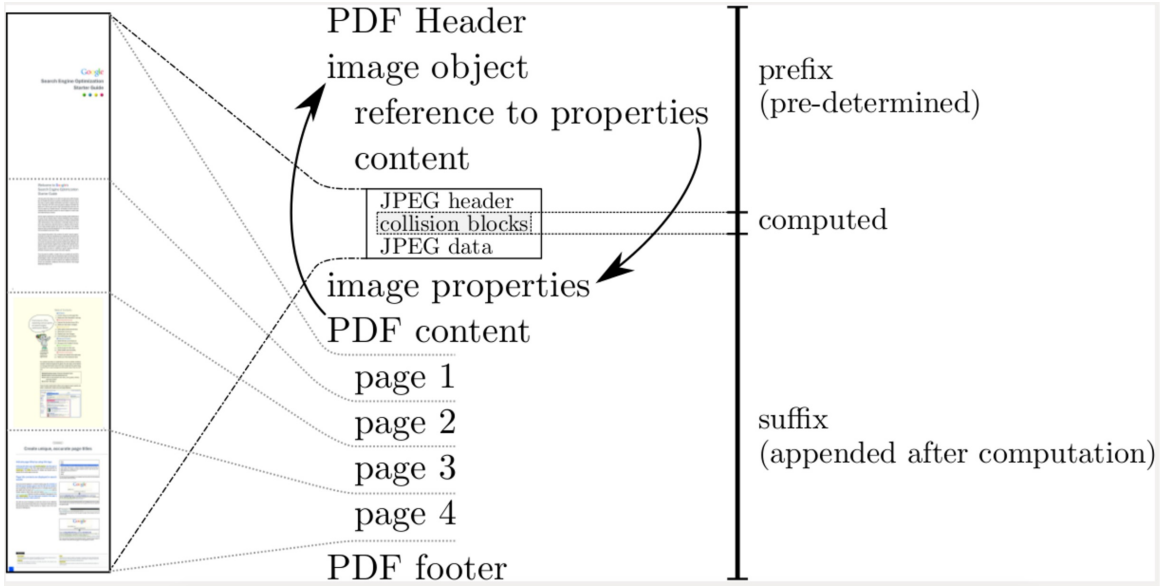
Como se proteger



centro universitário FEI

SHA1 Atacado

https://shattered.io/



Exemplo ”vítimas”: GIT | SVN

Ataques teóricos desde 2005
Descontinuado pelo NIST em 2011
Descontinuado pelo Chrome e Firefox em 2017

centro universitário FEI