



# INF1416

# Segurança da Informação

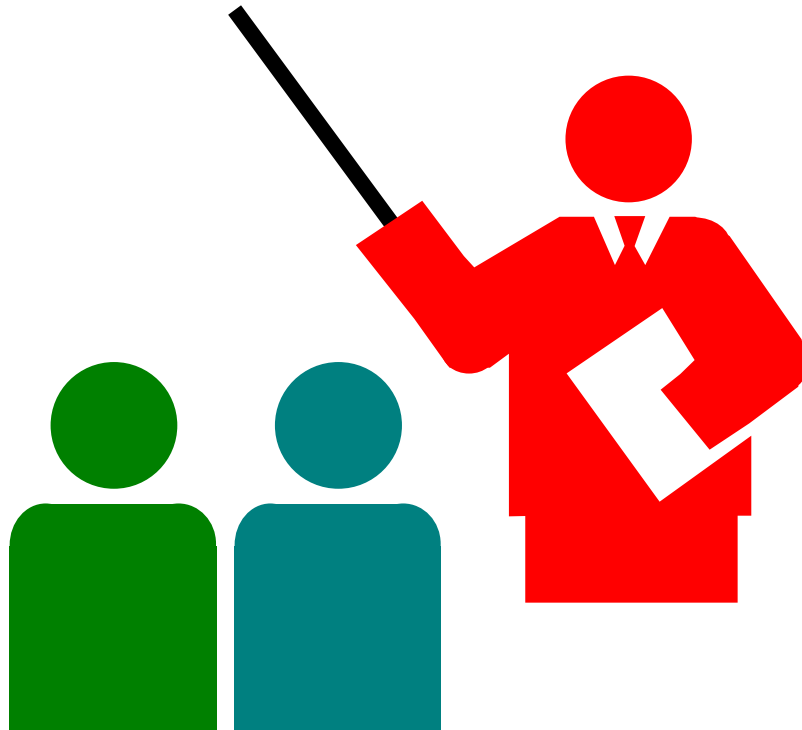
**Prof. Anderson Oliveira da Silva**  
**D. Sc. Ciências em Informática**  
**Engenheiro de Computação**  
**[anderson@inf.puc-rio.br](mailto:anderson@inf.puc-rio.br)**

**Departamento de Informática**  
**PUC-Rio**

# Trabalho 4 - Detalhamento

- Segurança da Informação  
Prof. Anderson O. da Silva

2



# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

3

## Especificação:

- O cofre digital (digital vault) é armazenado dentro de uma pasta de um sistema de arquivos tradicional (ex: FAT32, NTFS, EXT3, etc), chamada *pasta segura*.
- Um arquivo armazenado na pasta segura é chamado *arquivo protegido* e é composto por três meta-arquivos:
  - *nome\_codigo.enc*: é o criptograma do arquivo protegido;
  - *nome\_codigo.env*: é o envelope digital do arquivo protegido;
  - *nome\_codigo.asd*: é a assinatura digital do arquivo protegido.
- O *nome\_codigo* de um arquivo protegido é uma sequência aleatória de caracteres alfanuméricos.

# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

4

## Especificação:

- A pasta segura possui um *arquivo de índice*, cujo nome\_codigo é *index*, que mantém os atributos dos arquivos protegidos e pertence ao administrador do sistema.
- O arquivo de índice é um arquivo texto ASCII formado por zero ou mais linhas no seguinte formato:

NOME\_CODIGO\_ARQUIVO<SP>NOME\_SECRETO\_ARQUIVO<SP>DONO\_ARQUIVO<SP><GRUPO\_ARQUIVO><EOL>

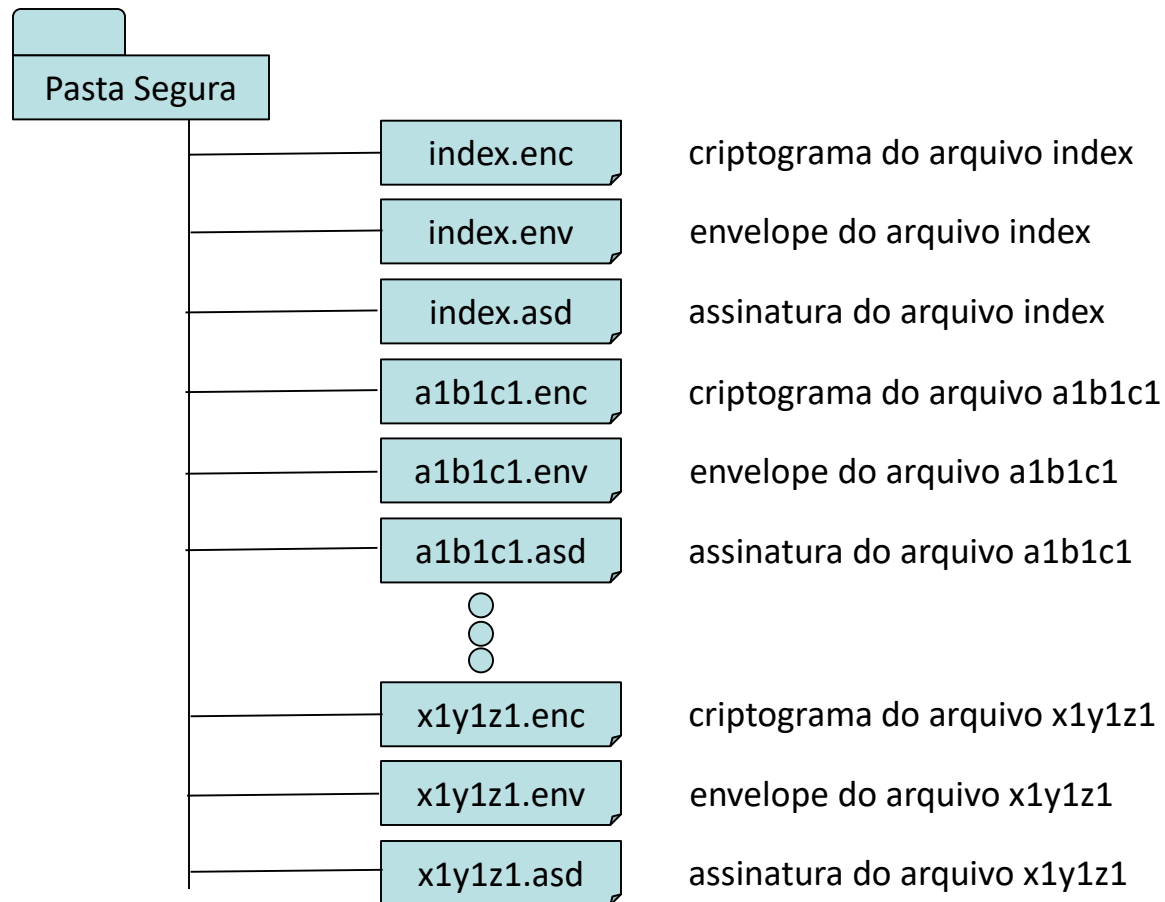
- NOME\_CODIGO\_ARQUIVO: caracteres alfanuméricos.
- NOME\_SECRETO\_ARQUIVO: caracteres alfanuméricos (nome real do arquivo protegido).
- DONO\_ARQUIVO: caracteres alfanuméricos (identificação do dono autorizado a acessar o arquivo).
- GRUPO\_ARQUIVO: caracteres alfanuméricos (identificação do grupo autorizado a acessar o arquivo).
- <SP> = caractere espaço em branco.
- <EOL> = caractere nova linha (\n).

# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

5

Esquema:



# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

6

## Processo de validação do arquivo protegido:

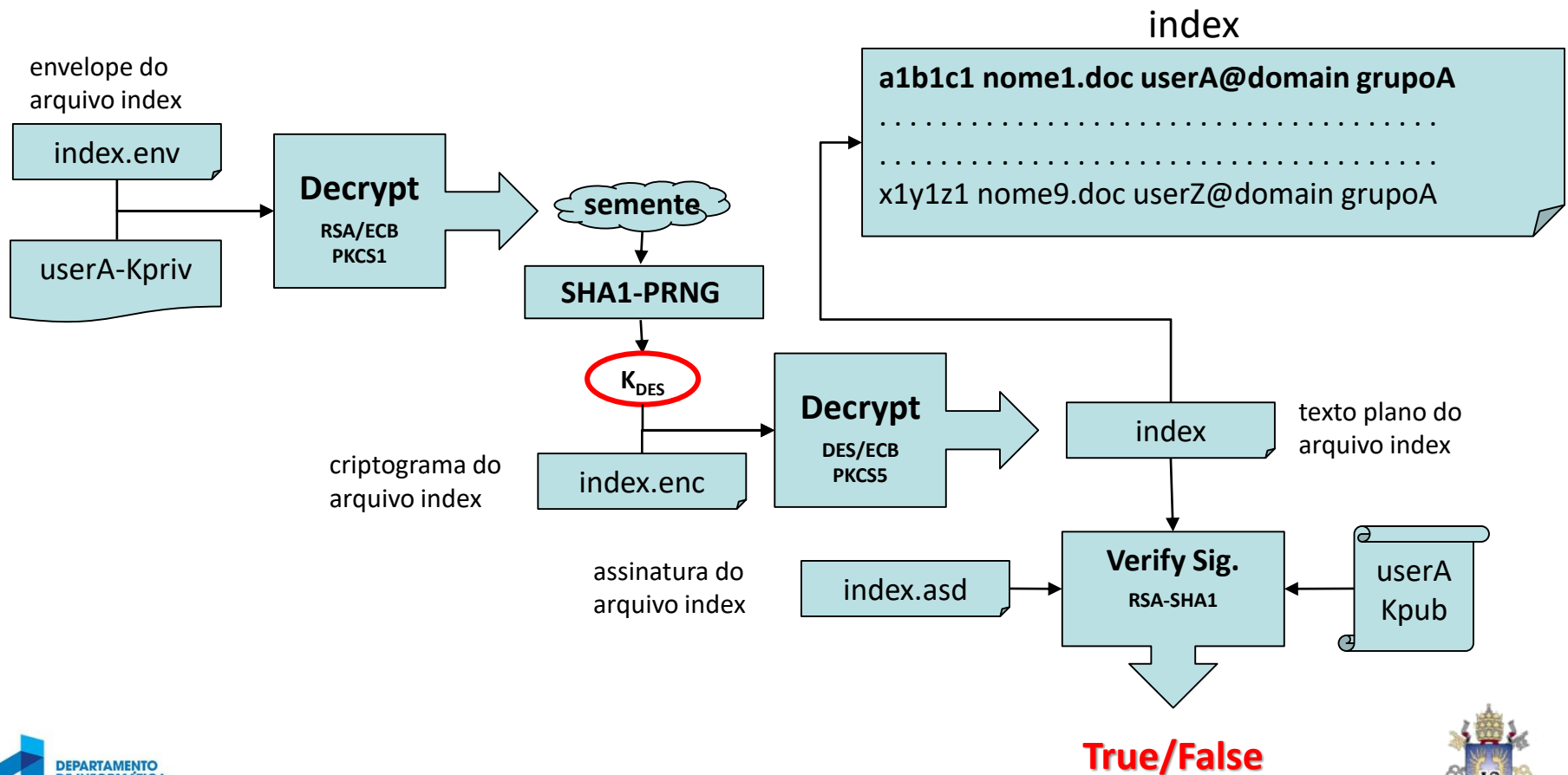
- Cada usuário do sistema possui uma *chave privada*, um *certificado digital* e uma *pasta protegida* particulares.
- A *chave privada* é utilizada para produzir a assinatura digital (SHA1-RSA) dos arquivos protegidos (*nome\_codigo.asd*).
- A *chave pública* é utilizada para produzir o envelope digital dos arquivos protegidos (*nome\_codigo.env*).
- O *envelope digital* possui a *semente* da *chave simétrica* usada para produzir o criptograma (DES/ECB/PKCS5padding) do arquivo protegido (*nome\_codigo.enc*).

# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

7

## Processo de validação do arquivo protegido:

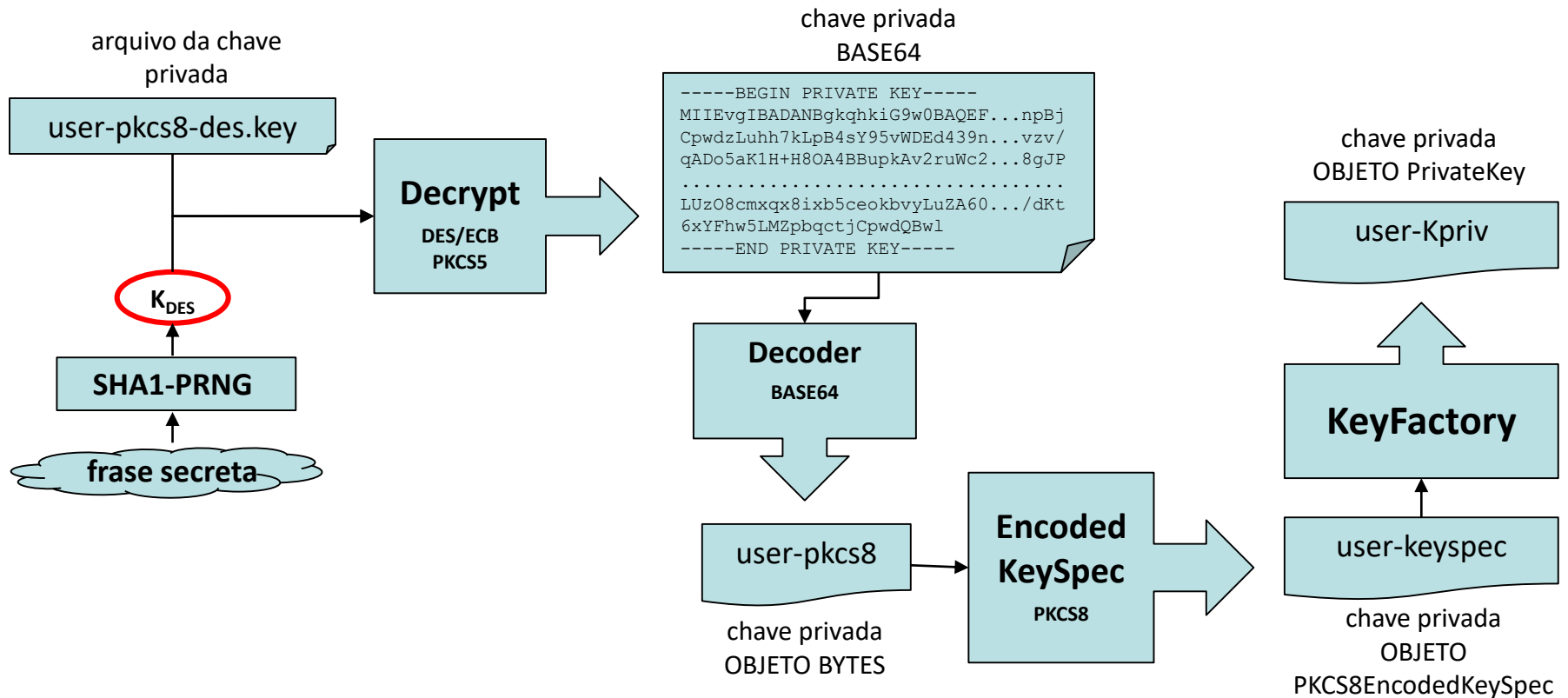


# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

8

## Restauração da chave privada:



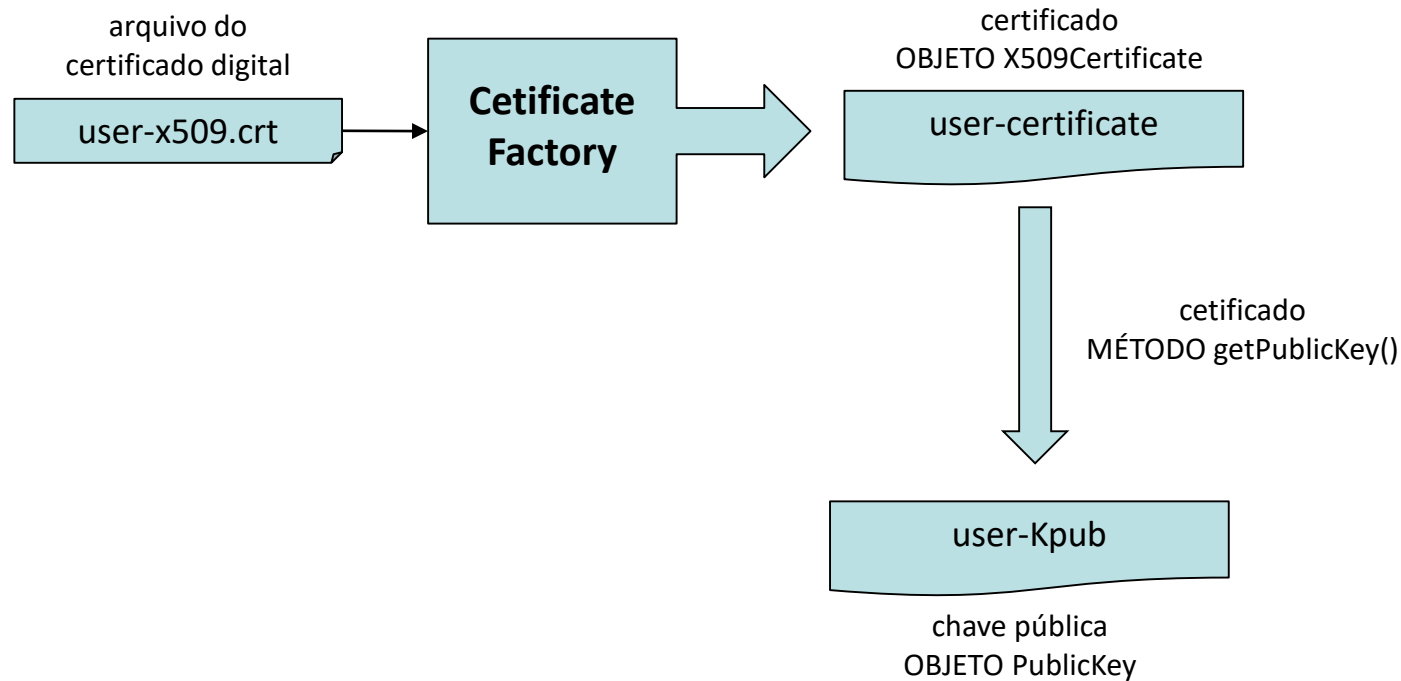


# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

9

## Restauração da chave pública:



# Cofre Digital (Digital Vault)

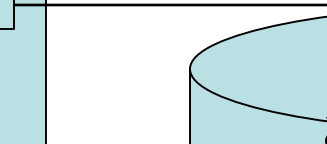
- Segurança da Informação  
Prof. Anderson O. da Silva

10

## Autenticação bifator: Etapa 1 – Validação do login name

**Cofre Digital - Autenticação**

Login name:



UID	EMAIL	HASH	TOKEN	KEYID	CT	BLK

# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

11

## Autenticação bifator: Etapa 2 – Validação da Senha Pessoal

### Cofre Digital - Autenticação

Senha pessoal:

•

1 9

8 7

3 5

OK

6 2

0 4

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal:

• •

2 4

5 7

0 9

OK

1 3

6 8

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal:

• • •

8 9

0 1

5 7

OK

6 2

3 4

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal:

• • • •

1 5

7 9

0 8

OK

2 4

3 6

LIMPAR

# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

12

## Autenticação bifator: Etapa 2 – Validação da Senha Pessoal

### Cofre Digital - Autenticação

Senha pessoal: ● ● ● ● ●

0 1

7 9

3 4

OK

2 6

5 8

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal: ● ● ● ● ● ●

6 7

0 9

1 3

OK

2 5

4 8

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal: ● ● ● ● ● ● ●

8 9

0 7

3 5

OK

1 6

2 4

LIMPAR

### Cofre Digital - Autenticação

Senha pessoal: ● ● ● ● ● ● ● ●

1 7

5 9

3 4

OK

0 6

3 8

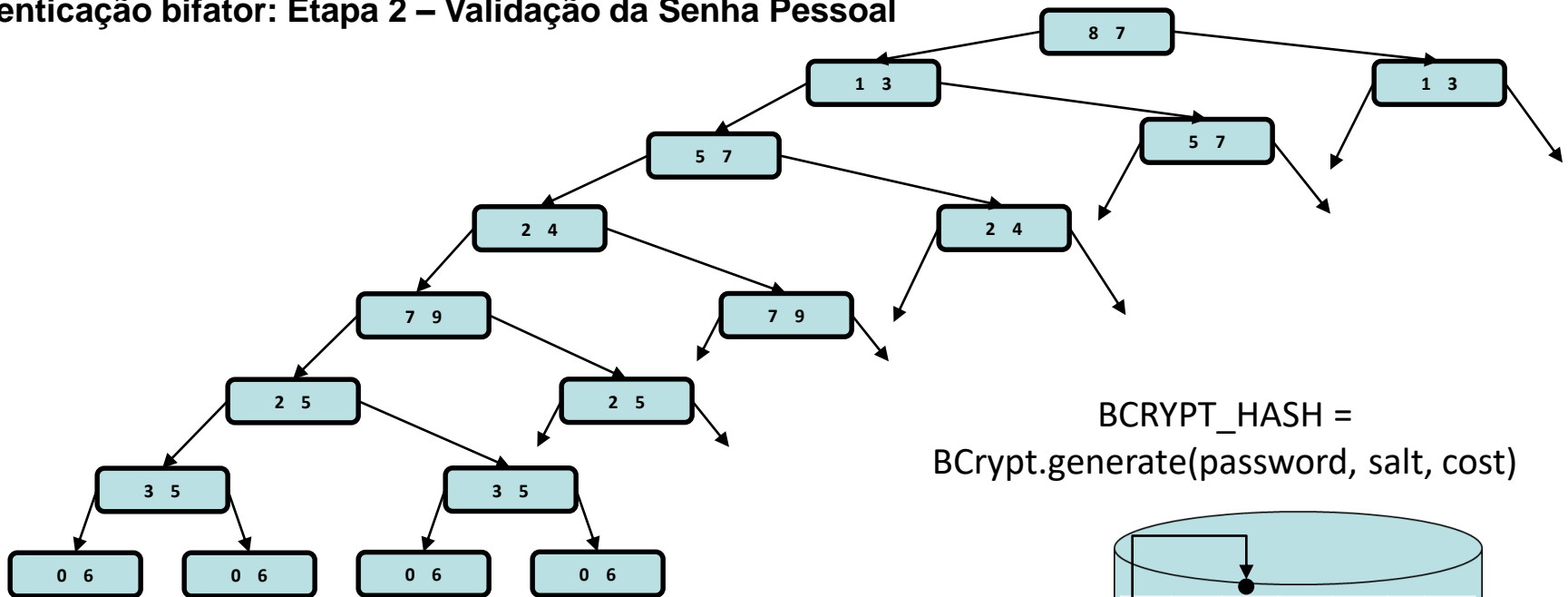
LIMPAR

# Cofre Digital (Digital Vault)

• Segurança da Informação  
Prof. Anderson O. da Silva

13

## Autenticação bifator: Etapa 2 – Validação da Senha Pessoal



1ª sequência: 81527230

2ª sequência: 81527236.

3ª sequência: 81527250

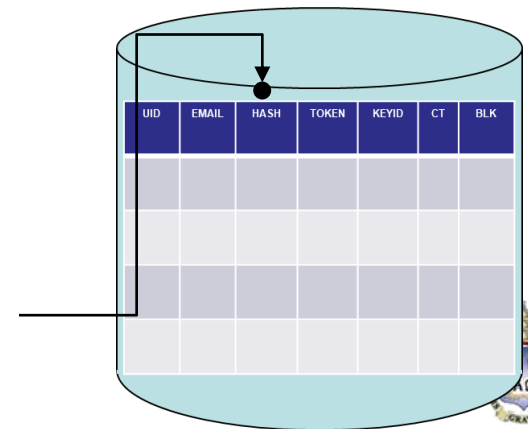
4ª sequência: 81527256.

5ª sequência: 81527530

6ª sequência: 81527536

+ SALT

BCRYPT\_ HASH



# Cofre Digital (Digital Vault)

- Segurança da Informação  
Prof. Anderson O. da Silva

14

## Autenticação bifator: Etapa 3 – Validação do Token

