Segurança de dados

Aula 05 e 06 – Criptografia básica

Gustavo Bianchi Maia

gustavo.maia@faculdadeimpacta.com.br

Sumário

- História da criptografia
- A máquina Enigna
- Tipos de algoritmos
- Por dentro de um algoritmo - AES
- Níveis para aplicação da criptografia
- Exercícios

Criptografia

Criptografia (Do Grego kryptós, "escondido", e gráphein, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. É um ramo da Matemática, parte da Criptologia.

Durante muito tempo, o termo referiu-se exclusivamente à cifragem, o processo de converter uma informação comum (texto claro) em algo não-inteligível; o qual chama-se texto cifrado. A decifragem é a tarefa contrária, dado uma informação não-inteligível convertê-la em texto claro.

A cifra é um ou mais algoritmos que cifram e decifram um texto. Na linguagem não-técnica, um Código secreto é o mesmo que uma cifra. Porém, na linguagem especializada os dois conceitos são distintos. Um código funciona manipulando o significado, normalmente pela substituição simples de palavras ou frases. Uma cifra, ao contrário, trabalha na representação da mensagem (letras, grupos de letras ou, atualmente, bits).

Por exemplo, um código seria substituir a frase "Atacar imediatamente" por "Mickey Mouse".

Uma cifra seria substituir essa frase por "sysvst ozrfosyszrmyr".

Criptologia é o campo que engloba a Criptografia e a Criptoanálise.

Fonte: http://pt.wikipedia.org/wiki/Criptografia

História

O primeiro uso documentado da criptografia foi em torno de 1900 a.c., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição.

Entre 600 a.c. e 500 a.c., os hebreus utilizavam a cifra de substituição simples.

No Império romano, o chamado "Codificador de Júlio César" ou "Cifra de César" que apresentava uma das técnicas mais clássicas de criptografia.

Em 1586, destacam-se os estudos de Blaise de Vigenère que utiliza a substituição de letras com diferentes valores de deslocamento alfanumérico.

Modernamente, em 1918, Arthur Scherbius desenvolveu uma máquina de criptografia chamada Enigma.

Em 1976 foi publicado, pelo governo americano, o DES (Data Encryption Standard), um algoritmo aberto de criptografia simétrica. O DES foi o primeiro algoritmo de criptografia disponibilizado abertamente ao mercado.

Artigos: Historia da Computacao | PETNews - A História da Criptografia. (ufcg.edu.br)

História da criptografia – Wikipédia, a enciclopédia livre (wikipedia.org)

Uma breve história sobre Criptografia | CRYPTOID

Cryptography - Wikipedia

Enigma

Vídeo:

- (573) Como Funcionou a Máquina Enigma - YouTube

Discussões:

- A vida e o trabalho de Alan Turing
- Papel da criptografia no mundo moderno

Filmes:

- Enigma (2001) - IMDb
- O Jogo da Imitação (2014) - IMDb

Simulador:

- Enigma Simulator (telenet.be)

Criptografia

A criptografia tem quatro objetivos principais:

- **Confidencialidade da mensagem**: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem da sua forma cifrada. Além disso, a obtenção de informação sobre o conteúdo da mensagem (como uma distribuição estatística de certos caracteres) não deve ser possível, uma vez que, se o for, torna mais fácil a análise criptográfica.

- **Integridade da mensagem**: o destinatário deverá ser capaz de determinar se a mensagem foi alterada durante a transmissão.

- **Autenticação do remetente**: o destinatário deverá ser capaz de identificar o remetente e verificar que foi mesmo ele quem enviou a mensagem.

- **não-repúdio ou irretratabilidade do emissor**: não deverá ser possível ao emissor negar a autoria da mensagem.

Nem todas as técnicas garantem todos os objetivos.

Criptografia - Tipos básicos

2-WAY

Simétricos

Os algoritmos de chave simétrica (ou chave única / secreta) são uma classe de algoritmos para a criptografia, que usam chaves criptográficas relacionadas para as operações de cifragem ou decifragem (ou cifra/decifra, ou cifração/decifração).

Assimétricos (ou de chave pública/privada)

A criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. A chave pública é distribuída livremente para todos os correspondentes via e-mail ou outras formas, enquanto a chave privada deve ser conhecida apenas pelo seu dono.

1-WAY

Hash

Um hash (ou escrutínio) é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada (4 bits). O conceito teórico diz que "hash é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações".

Criptografia - Tipos básicos

Determinísticos

A criptografia determinística sempre gera o mesmo valor criptografado para qualquer valor de texto sem formatação. Usar a criptografia determinística proporciona pesquisas de ponto, junções de igualdade, agrupamento e indexação em colunas criptografadas. No entanto, ela também pode permitir que usuários não autorizados estimem informações sobre os valores criptografados examinando padrões na coluna criptografada, especialmente se há um conjunto pequeno de valores criptografados possíveis, como Verdadeiro/Falso ou região Norte/Sul/Leste/Oeste. A criptografia determinística deve usar uma ordenação de colunas com uma ordem de classificação binary2 para as colunas de caracteres.

Aleatórios

A criptografia aleatória usa um método que criptografa os dados de uma maneira menos previsível. A criptografia aleatória é mais segura, mas impede o uso de pesquisas, agrupamento, indexação e junção em colunas criptografadas.

fonte: Always Encrypted - SQL Server | Microsoft Docs

Criptografia - Tipos básicos

2-WAY

Simétricos

- Máquina Enigma (Máquina alemã de rotores utilizada na 2a Guerra Mundial)
- DES - Data Encryption Standard (FIPS 46-3, 1976)
- RC4 (um dos algoritmos criados pelo Prof. Ron Rivest)
- RC5 (também por Prof. Ron Rivest)
- Blowfish (por Bruce Schneier)
- IDEA - International Data Encryption Algorithm (J Massey e X Lai)
- AES (também conhecido como **RIJNDAEL**) - Advanced Encryption Standard (FIPS 197, 2001)
- RC6 (Ron Rivest)

Assimétricos (ou de chave pública/privada)

- Curvas elípticas
- Diffie-Hellman
- DSA de curvas elípticas
- El Gamal
- RSA

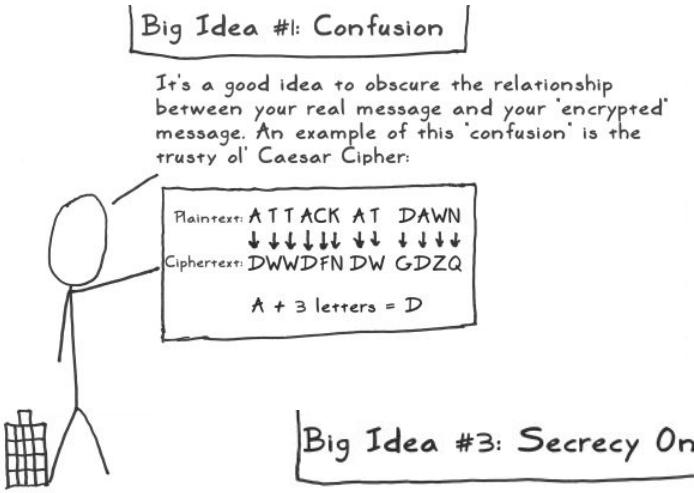
1-WAY

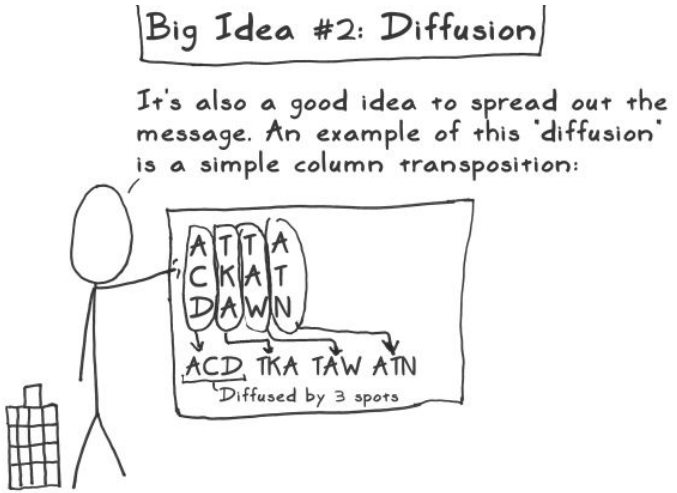
Hash

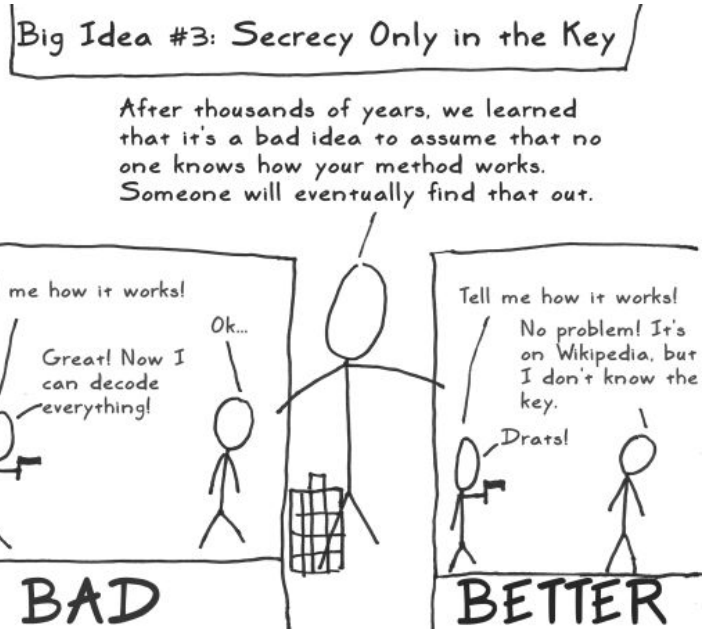
- MD5
- SHA-256
- SHA-1
- RIPEMD-160
- Tiger

Criptografia - Algotimo AES

História, origem, uso. [A Stick Figure Guide to the Advanced Encryption Standard (AES) (moserware.com)]

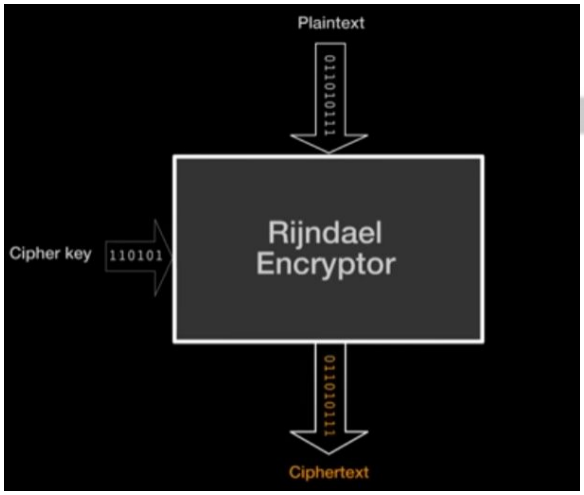


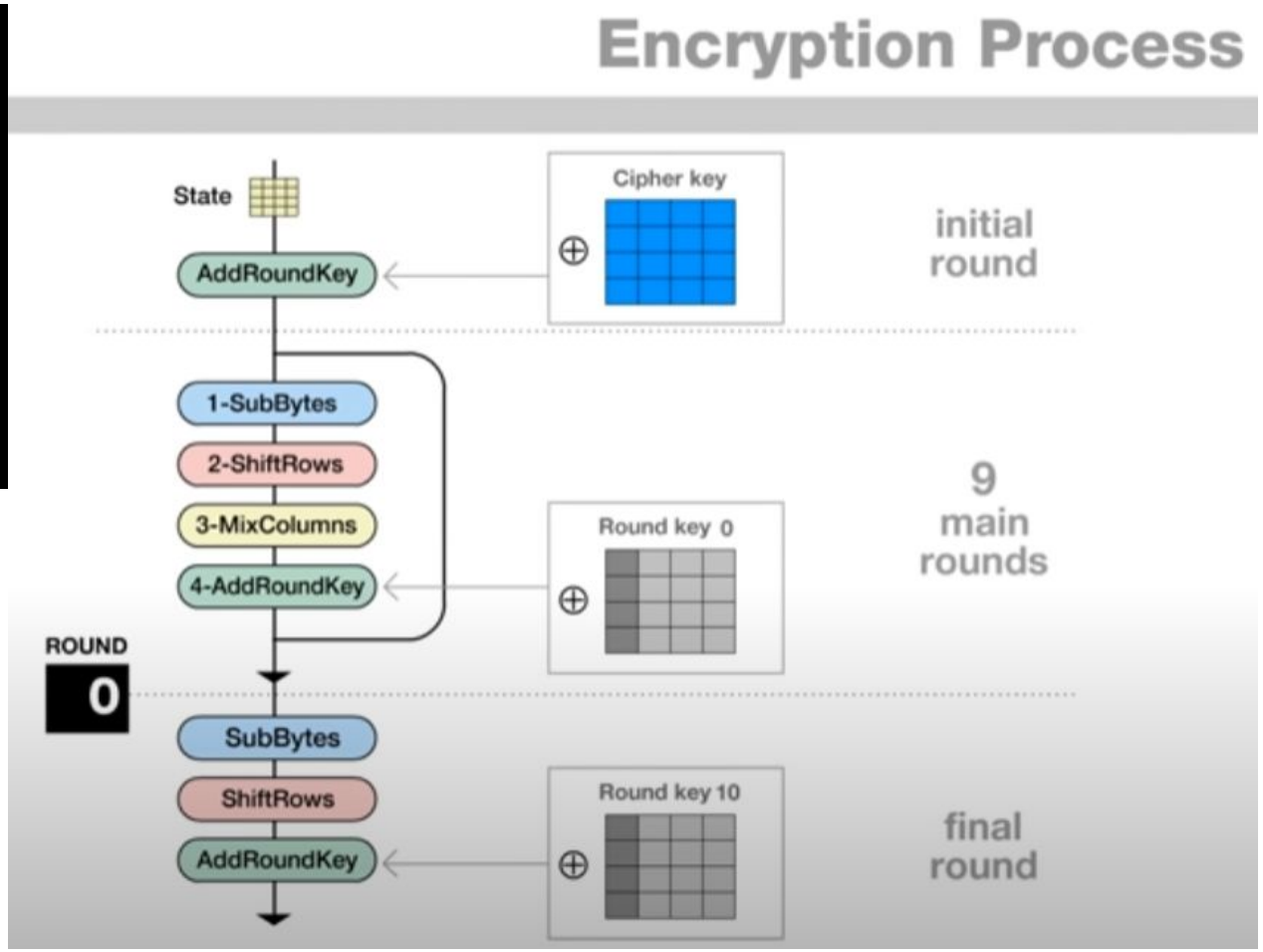




Criptografia - Algotimo AES

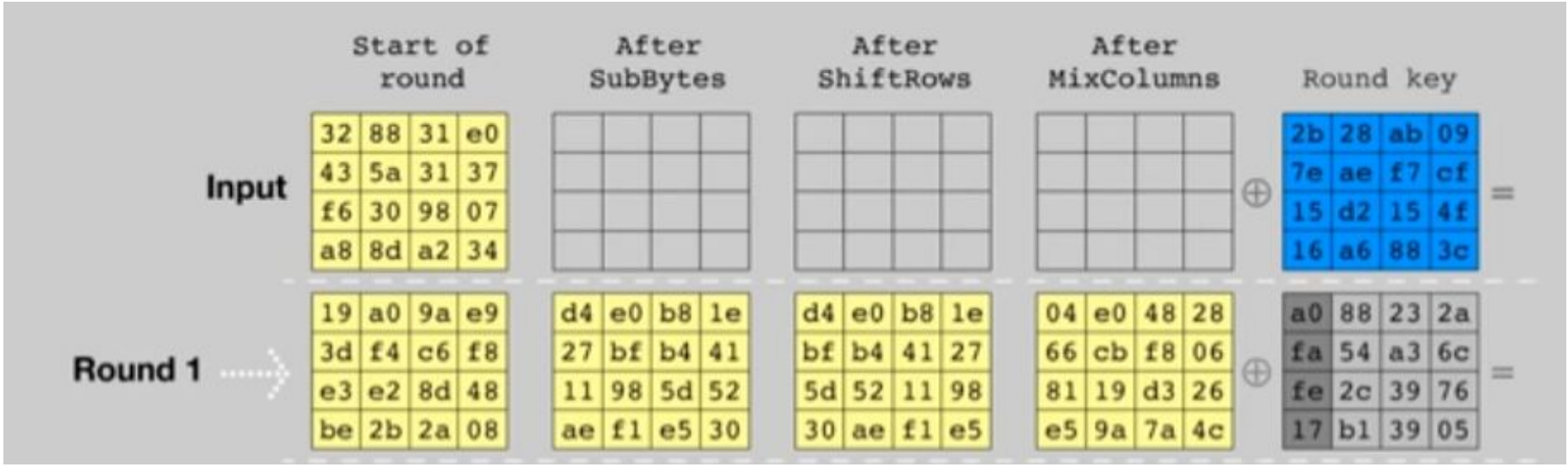
Animação com detalhes. [(574) AES Rijndael Cipher explained as a Flash animation - YouTube]



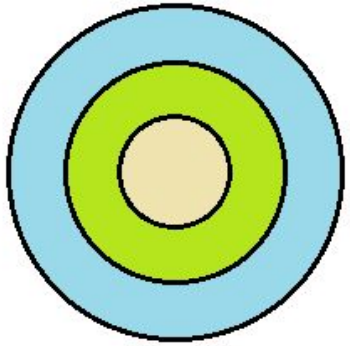


Criptografia - Algotimo AES

Animação com detalhes. [(574) AES Rijndael Cipher explained as a Flash animation - YouTube]



Criptografia - Técnicas por nível



Criptografia de dados em repouso:

Conjunto de técnicas que visam salvaguardar o dado da forma como ele é armazenado e/ou recuperado.

Mais detalhado

- **Dado**
  - Funções internas:
    - Hashbytes
    - EncryptByKey / DecryptByKey
    - EncryptByAsymKey / DecryptByAsymKey
- **Coluna**
  - AlwaysEncrypted(Always Encrypted - SQL Server | Microsoft Docs)
- **Banco de dados**
  - Transparent Data Encryption (TDE (Transparent Data Encryption) - SQL Server | Microsoft Docs)
- **Sistema Operacional**
  - Bitlocker (BitLocker Como implantar no Windows Server 2012 e posterior - Microsoft 365 Security | Microsoft Docs)
- **Disco**
  - Full Disk Encryption (How to Enable Full-Disk Encryption on Windows 10 (howtogeek.com)
  - EBS Encrypted Volumes (Amazon EBS encryption - Amazon Elastic Compute Cloud)

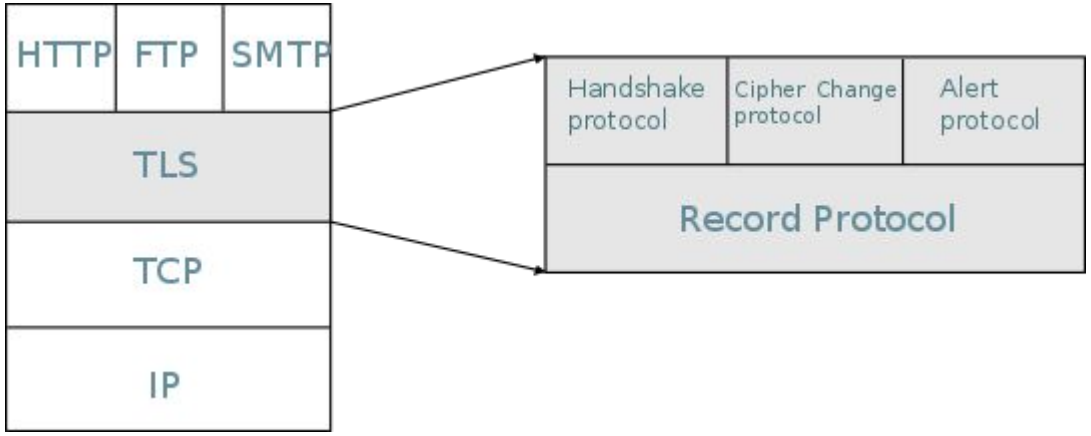
Menos detalhado

Criptografia - Técnicas por nível

Criptografia de dados em transito:

Conjunto de técnicas que visam salvaguardar o dado enquanto ele é utilizado em uma transferência ou comunicação.

SSL / TLS (Transport Layer Security – Wikipédia, a enciclopédia livre (wikipedia.org))



TLS no MSSQL (Habilitar conexões criptografadas - SQL Server | Microsoft Docs)

Criptografia - Funções internas

```
CREATE DATABASE cripto
go
USE cripto
go
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
--=X=-- HASH
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
DECLARE @Salt VARCHAR(50) = 'FIT'
DECLARE @pass VARCHAR(255) = 'teste'
DECLARE @value VARCHAR(255) = @pass + @salt
SELECT Hashbytes('md5', @value)
-- 0xF49D7CA29D54B25A20F8EE4D695F7748
SELECT Hashbytes('sha1', @value)
--0x7ECA82E54BFF01456689D9995DBD1241090FF458
```

Perguntas:

Hash é um algoritmo Determinístico ou Aleatório ?

Pelo ‘tamanho’ do resultado pode-se determinar a ‘força’ de um algoritmo ?

O que é o Salt ? ele ajuda a melhorar a segurança ? como ?

Qual tipo de dado é recomendado para salvar o valor criptografado em uma tabela ?

Criptografia - Funções internas

```
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
--=X=-- CHAVE SIMÉTRICA
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
CREATE symmetric KEY chavesimetrica01 WITH algorithm = aes_256 encryption BY
password = N'!@@QW#E#$R%dreud76'
OPEN symmetric KEY chavesimetrica01 decryption BY password =
N'!@@QW#E#$R%dreud76';

DECLARE @result VARBINARY(max)
DECLARE @key UNIQUEIDENTIFIER = (SELECT Key_guid('ChaveSimetrica01'))

SELECT @result = Encryptbykey(@key, 'OMG You Killed Kenny');
SELECT CONVERT(VARCHAR, Decryptbykey(@result))

CLOSE symmetric KEY chavesimetrica01
```

Perguntas: Este é um algoritmo Determinístico ou Aleatório ?

Preciso sempre abrir e depois fechar a chave para utilizar as funções citadas ?

Por que preciso converter para VARCHAR o dado decriptografado ?

Criptografia - Funções internas

```
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
--=X=-- CHAVE ASSIMÉTRICA
--=X=-- --=X=-- --=X=-- --=X=-- --=X=-- --=X=--
CREATE asymmetric KEY chaveassimetrica001 WITH algorithm = rsa_2048 encryption
BY password = N'!@@QW#E#$R%dreud76';
go

DECLARE @key_ID INT = (SELECT Asymkey_id('ChaveAssimetrica001'))
DECLARE @result VARBINARY(max)

SELECT @result = Encryptbyasymkey(@key_ID, 'OMG You Killed Kenny')

SELECT CONVERT(VARCHAR, Decryptbyasymkey(@key_ID, @result, N'!@@QW#E#$R%dreud76' ) )
```

Perguntas: Este é um algoritmo Determinístico ou Aleatório ?

Por que não preciso abrir ou fechar nesta técnica em comparação com a anterior ?

Qual pareceu mais segura ? justifique-se...

Exercícios - AC2

Sejam as seguintes funções (Que serão criadas na AC2)

```
--Função de criptografia
SELECT dbo.Fn_encrypt('oi')
```

Recebe uma string e devolve o respectivo valor criptografado em VARBINARY utilizando um algoritmo de 2 vias assimétrico de criptografia.

```
--Função de decriptografia
SELECT dbo.Fn_decrypt(dbo.Fn_encrypt('oi'))
```

Recebe um valor já criptografado e devolve o respectivo valor descriptografado já convertido em VARCHAR

```
--Função de criptografia de HASH
SELECT dbo.Fn_hash('oi')
```

Recebe uma string e devolve o respectivo valor criptografado em VARBINARY utilizando um algoritmo de HASH com a utilização de um SALT (por segurança).

Exercícios - AC2

```
--Criando a tabela TBL_CTRL_ACESSO
     CREATE TABLE tbl_ctrl_acesso
       (  [login]      VARCHAR(60) NOT NULL,
          [senha]      VARBINARY(max) NOT NULL,
          [dica_senha] VARBINARY(max) NULL,
          CONSTRAINT pk_ctrl_acesso PRIMARY KEY ( [login] )
       )
--Inserindo valores nas tabelas para testes:
INSERT INTO tbl_ctrl_acesso( [login], [senha], [dica_senha] )
VALUES      ( 'José', dbo.Fn_hash('senha'),dbo.Fn_encrypt('aquela lá') )
go
--Testando valores brutos inseridos na tabela
SELECT * FROM   tbl_ctrl_acesso
go
--Testando valores decriptografados lidos da tabela
SELECT [login], [senha],
       CONVERT(VARCHAR, dbo.Fn_decrypt([dica_senha])) AS [dica_senha]
FROM   tbl_ctrl_acesso
go
```

Exercícios - AC2

Seja a seguinte procedure (que também será criada na AC2)

```
EXEC Pr_login  @login,   @senha,   @result output
```

Que, recebe um login e senha (ambos varchar) e devolve 1 se ele foi autenticado, ou seja, se aquele usuário foi cadastrado com aquela senha, e 0 caso contrário.

Exemplo de utilização:

```
--testando procedure de login
DECLARE @result BIT
--autenticado
EXEC Pr_login   'josé',   'senha',   @result output
SELECT CASE WHEN @result = 1 THEN 'Autenticado' ELSE 'Não autenticado' END

--não autenticado
EXEC Pr_login   'josé',   'senha errada',   @result output
SELECT CASE WHEN @result = 1 THEN 'Autenticado' ELSE 'Não autenticado' END
go
```

Exercícios - AC2

Seja a seguinte procedure (que também será criada na AC2)

```
EXEC Pr_esqueci_senha   @login,   @result output
```

Que, recebe um login (varchar) e devolve a dica da senha decriptografada, cadastrada para aquele login.

Exemplo de utilização:

```
--Testando a procedure esqueci senha
DECLARE @result VARCHAR(60)

EXEC Pr_esqueci_senha   'josé',   @result output

SELECT 'Sua dica da senha é: "' + @result + '"'
go
```

Exercícios - AC2

Crie as funções:

- FN_ENCRYPT
- FN_DECRYPT
- FN_HASH

E as procedures:

- PR_LOGIN
- PR_ESQUECI_SENHA

De modo que elas funcionem nos códigos de exemplo apresentados....

Obrigado

Segurança de dados

Aula 06 – Criptografia básica

- **Gustavo Bianchi Maia**

gustavo.maia@faculdadeimpacta.com.br