Universidad de Costa Rica

Mario Quirós Luna B76090

Administración de bases de datos.

Tarea Corta 6

Criptografía:

La criptografía está asociada con el proceso de convertir texto sin formato ordinario en texto ininteligible y viceversa.

Es un método para almacenar y transmitir datos en una forma particular para que solo aquellos a quienes está destinado puedan leerlos y procesarlos.

La criptografía no solo protege los datos contra robos o alteraciones, sino que también se puede utilizar para la autenticación de usuarios.

La criptografía proporciona una comunicación segura en presencia de terceros. El cifrado utiliza un algoritmo y una clave para transformar una entrada (es decir, texto sin formato) en una salida cifrada (es decir, texto cifrado). Un algoritmo dado siempre transformará el mismo texto sin formato en el mismo texto cifrado si se usa la misma clave.

Control basado en privilegios:

Control de acceso basado en roles (de las siglas ***role based access control***), es un paradigma de seguridad basado en la asignación de funciones y autorizaciones dentro de la infraestructura informática de una organización. En este modelo, esas funciones y autorizaciones se engloban en los denominados **roles de usuario**, que determinan el grado de acceso que tienen los usuarios dentro del sistema y las acciones que pueden llevar a cabo dentro del mismo.

Tipos de encriptación.

- Encriptación simétrica: es aquella donde se utiliza la misma clave tanto para cifrar como para descifrar los datos.
- Encriptación asimétrica: Consta de una clave pública para cifrar y una clave privada para descifrar.
- Encriptación hibrida:

Algoritmos se usan.

Algunos algoritmos de encriptación son: DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 de 128 bits, DESX, AES de 128 bits, AES de 192 bits y AES de 256 bits.

No obstante, se aplican los siguientes principios generales:

- El cifrado seguro suele consumir más recursos de la CPU que un cifrado menos seguro.
- Las claves largas suelen producir un cifrado más seguro que las claves cortas.
- El cifrado asimétrico es más lento que el simétrico.
- Las contraseñas largas y complejas son más seguras que las contraseñas cortas.
- Por lo general, el cifrado simétrico se recomienda en los casos en los que la clave solo se almacena de forma local, mientras que el asimétrico es pertinente cuando las claves deben compartirse a través de la conexión.
- Si cifra una gran cantidad de datos, debe cifrar los datos con una clave simétrica y cifrar la clave simétrica con una clave asimétrica.
- Los datos cifrados no se pueden comprimir, pero los datos comprimidos se pueden cifrar. Si usa compresión, debe comprimir los datos antes de cifrarlos.

Motor de BD, qué formas de encriptar tiene, como lo hace.

SQL Server permite a los administradores y los desarrolladores de software elegir entre varios algoritmos, incluidos DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, RC4 de 128 bits, DESX, AES de 128 bits, AES de 192 bits y AES de 256 bits.

Ejemplo:

Algoritmo TRIPLE DES

Este algoritmo usa claves de 128 bits de largo. Necesita una misma frase tanto para encriptar como para desencriptar el dato que se encripto, aunque se acceda a los datos estos no pueden ser desencriptados sin contar con la frase correspondiente. Este es un algoritmo de encriptación simétrica.

```
/*************************************************************************/

--Crea tabla para prueba

CREATE TABLE Tarea6_Encriptacion
(
    Usuario VARCHAR(50),
    Contrasenna_Encryptada VARBINARY(256)
)

/*************************************************************************/
```

Creación de procedimientos almacenados

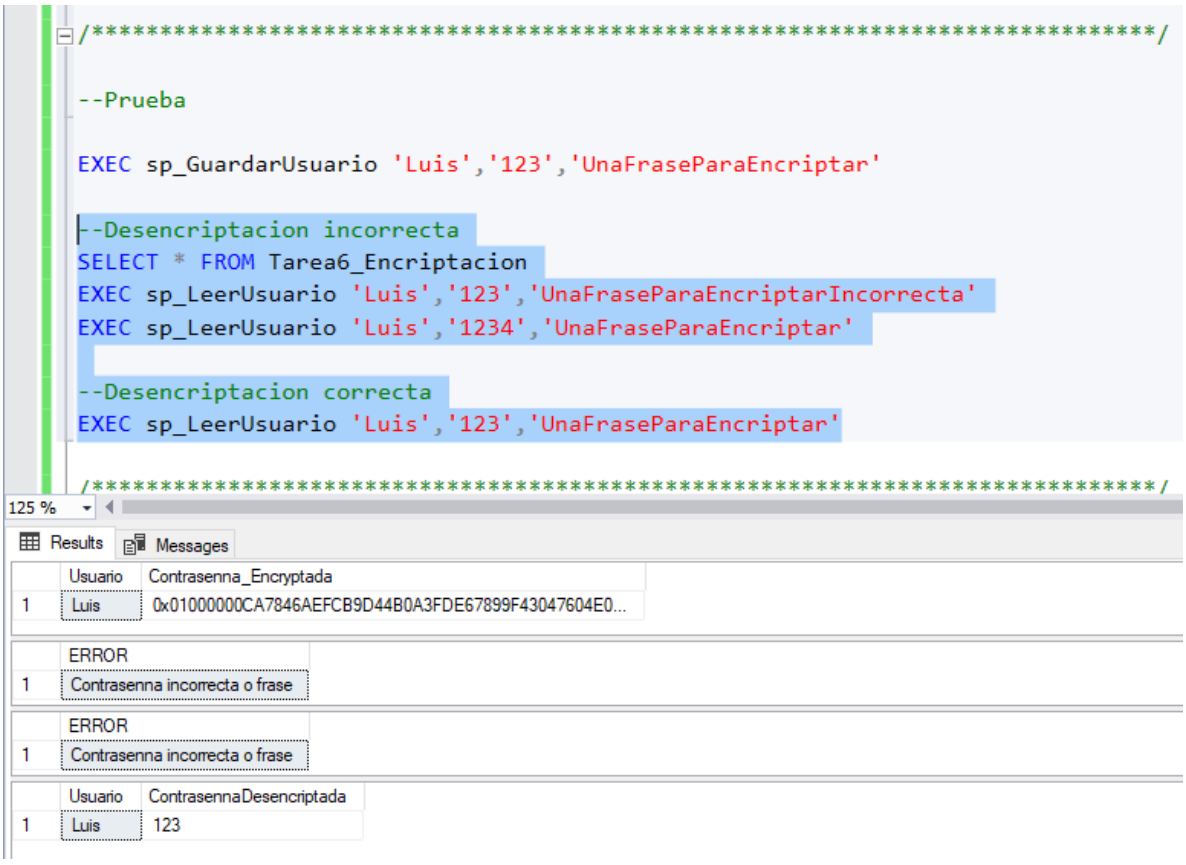
```sql
/*************************************************************************************/

--Crea procedimiento almacenado para guardar los usuarios

CREATE PROCEDURE sp_GuardarUsuario
    @usuario VARCHAR(50),
    @contrasenna VARCHAR(50),
    @fraseEncryptacion VARCHAR(50)
AS
DECLARE @contrasennaEncryptada VARBINARY(256)
BEGIN
    --Encriptacion de la clave con una frase que ingresa el usuario
    SET @contrasennaEncryptada = (ENCRYPTBYPASSPHRASE(@fraseEncryptacion, @contrasenna))

    --Guarda la cuenta del usuario con la contrasenna encriptada
    INSERT INTO Tarea6_Encriptacion(Usuario,Contrasenna_Encryptada)
        VALUES(@usuario,@contrasennaEncryptada)
END

/*************************************************************************************/
```

```sql
/*************************************************************************/

--Crea procedimiento que lee los datos del usuario desencriptados

CREATE PROCEDURE sp_LeerUsuario
    @usuario VARCHAR(50),
    @contrasenna VARCHAR(50),
    @fraseEncryptacion VARCHAR(50)
AS
DECLARE @contrasennaDesencriptada VARCHAR(256)
BEGIN
    --Devuelve la contrasenna despues de ser desencriptada con la frase ingresada por el usuario
    IF((CONVERT(VARCHAR(256), DECRYPTBYPASSPHRASE(@fraseEncryptacion,(SELECT Contrasenna_Encryptada FROM Tarea6_Encriptacion)))) = @contrasenna)
    BEGIN
        SELECT Usuario, CONVERT(VARCHAR(256), DECRYPTBYPASSPHRASE(@fraseEncryptacion,Contrasenna_Encryptada)) AS ContrasennaDesencriptada
        FROM Tarea6_Encriptacion
    END
    ELSE
    BEGIN
        SELECT 'Contrasenna incorrecta o frase' AS ERROR
    END
END

/*************************************************************************/
```

Prueba de funcionamiento

1. Si se consultan todos los datos, se obtiene la contraseña encriptada.
2. Si se ingresa una frase de desencriptar incorrecta no logra ser desencriptada la contraseña.
3. Si se ingresa una contraseña incorrecta no logra desencriptar la contraseña.

4. Si usa la frase y contraseña correcta logra mostrar la contraseña desencriptada.



```
/*************************************************************************/

--Prueba

EXEC sp_GuardarUsuario 'Luis','123','UnaFraseParaEncriptar'

--Desencriptacion incorrecta
SELECT * FROM Tarea6_Encriptacion
EXEC sp_LeerUsuario 'Luis','123','UnaFraseParaEncriptarIncorrecta'
EXEC sp_LeerUsuario 'Luis','1234','UnaFraseParaEncriptar'

--Desencriptacion correcta
EXEC sp_LeerUsuario 'Luis','123','UnaFraseParaEncriptar'

/*************************************************************************/
```

125 %

Results | Messages

	Usuario	Contrasenna_Encryptada
1	Luis	0x01000000CA7846AEFCB9D44B0A3FDE67899F43047604E0...

	ERROR
1	Contrasenna incorrecta o frase

	ERROR
1	Contrasenna incorrecta o frase

	Usuario	ContrasennaDesencriptada
1	Luis	123

Bibliografía:

Arguelles, G. T. (2021). *El cifrado de Datos (Tipos y Soluciones) - Access Quality*. Access Quality - Líderes en Servicios TI y SOC y NOC. https://www.accessq.com.mx/cifrado-de-datos/

Ramírez, H. (2021). *Control de acceso basado en roles (RBAC): Una forma de mejorar la seguridad del sistema*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/control-de-acceso-basado-en-roles-rbac/

Hurtado, J. S. (2021). *Qué es la criptografía y para qué sirve*. Thinking for Innovation. https://www.iebschool.com/blog/que-es-la-criptografia-y-para-que-sirve-finanzas/

To, V., Neugebauer, N. et al. (2021). *ENCRYPTBYPASSPHRASE (Transact-SQL) - SQL Server*. Microsoft Docs. https://docs.microsoft.com/en-us/sql/t-sql/functions/encryptbypassphrase-transact-sql?view=sql-server-ver15