

**UNIVERSIDAD TECNOLÓGICA DE**

**SAN LUIS RIO COLORADO**

**Database encryption**

**MTRA. ARIADNA ALEJANDRA DERBEZ**

**ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS**

San Luis Rio Colorado, Sonora Noviembre, 2020

**What is data encryption?**

Encryption is the conversion of data from a readable format to an encoded format, which can only be read or processed after it has been decrypted.

Encryption is the cornerstone of data security and is the simplest and most important way to prevent someone from stealing or reading information on a computer system for malicious purposes.

Used by both individual users and large corporations, encryption is widely used on the Internet to ensure the inviolability of personal information sent between browsers and servers.

That information could include everything from payment details to personal information. Businesses of all sizes often use encryption to protect sensitive data on their servers and databases.

**The need for data encryption**

Beyond the obvious advantage of protecting private information against theft or threats, encryption also offers a means of proving both the authenticity and the origin of the information. It can be used to verify the origin of a message and confirm that it has not been modified during transmission.

**Methods**

A number of methods are used to encode and decode information, and these methods evolve as computer software and the methods of interception and theft of information change. These methods include the following:

* **Symmetric key encryption:** also known as the secret key algorithm, it is a unique method of decoding messages that must be provided to the receiver before the message can be decoded. The key used in encryption is the same as that used in decryption, which is more convenient for individual users and closed systems. Otherwise, the key has to be sent to the recipient, which increases the risk of tampering if third parties, such as a hacker, intercept it. The advantage is that this method is much more agile than the asymmetric method.
* **Asymmetric cryptography:** This method uses two different keys (public and private), which are linked to each other mathematically. Keys are just long numbers linked to each other, but they are not identical, hence the term asymmetric. The public key can be shared with anyone, while the private key must be kept secret. Both can be used to encrypt a message, and the opposite key from the one used to encrypt it is then used to decode it.

AES\_ENCRYPT() function

MySQL AES\_ENCRYPT() function encrypts a string using AES algorithm.

AES stands for Advance Encryption Standard. This function encodes the data with 128 bits key length but it can be extended up to 256 bits key length. It encrypts a string and returns a binary string. The return result will be NULL when an argument is NULL.

Syntax:

AES\_ENCRYPT(str, key\_str);

AES\_DECRYPT() function

MySQL AES\_DECRYPT() function decrypts an encrypted string using AES algorithm to return the original string. It returns NULL if detects invalid data.

Syntax:

AES\_DECRYPT(crypt\_str, key\_str);