Date
25.04.2020

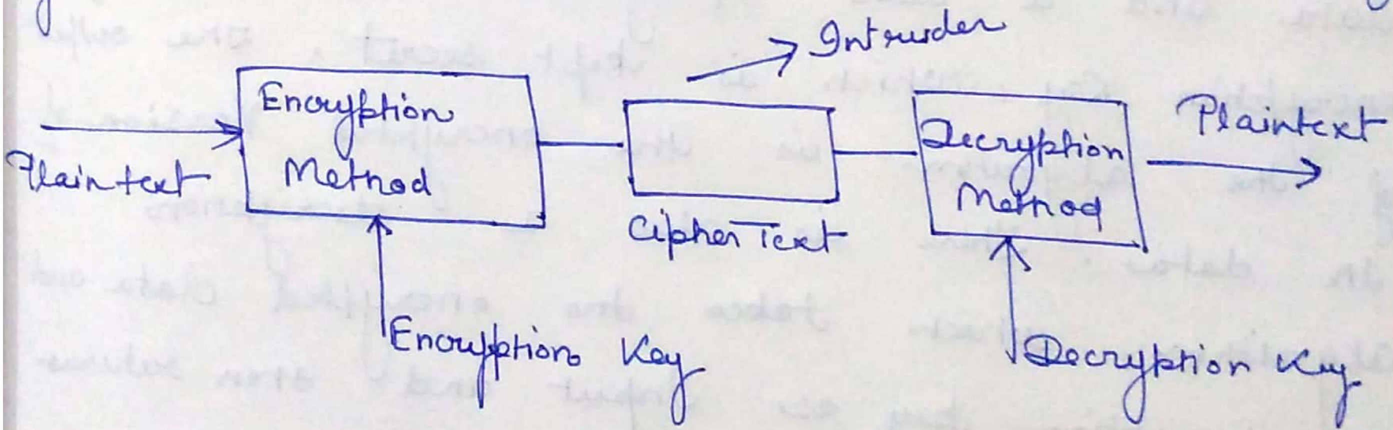
Computer Science 2nd Year

Subject - 'DBMS'

Data Encryption in DBMS

A DBMS can use encryption to protect Information in certain situation where the normal security mechanisms of the DBMS are not adequate. For example :-

An Intruder may steal tapes containing some data or tap a communication line. By storing and transmitting data in an encrypted form, The DBMS ensure that such stolen data is not Intelligible to the Intruder. Thus, encryption is a technique to provide privacy of data.



In encryption, the message to be encrypted is known as plaintext. The plaintext is transformed by a function that is parameterized by a key. The output of the encryption process is known as the cipher text. cipher text is then transmitted over the network. The process of converting the plaintext to ciphertext is called as Encryption and process of converting the ciphertext to plaintext is called as Decryption. Encryption is performed at the transmitting end and Decryption is performed at the receiving end. for encryption process we need the encryption key and for decryption key as shown in figure. without the knowledge of decryption key Intruder cannot break the ciper text to plaintext. this process is also called as cryptography.

The basic Idea behind encryption is to apply an encryption algorithm, which may be accessible to the Intruder, to the original data and a user-specified or DBA-specified encryption key, which is kept secret. The output of the algorithm is the encrypted version of the data. There is also a decryption algorithm, which takes the encrypted data and the decryption key as Input and then returns the original data. without the correct decryption key, The decryption algorithm produce gibberish. Encryption and decryption key may be same or different but there must be relation between the both which must me secret.

25/09/2020

Shardha Vaish