Date
27/04/2020

Subject - 'DBMS'
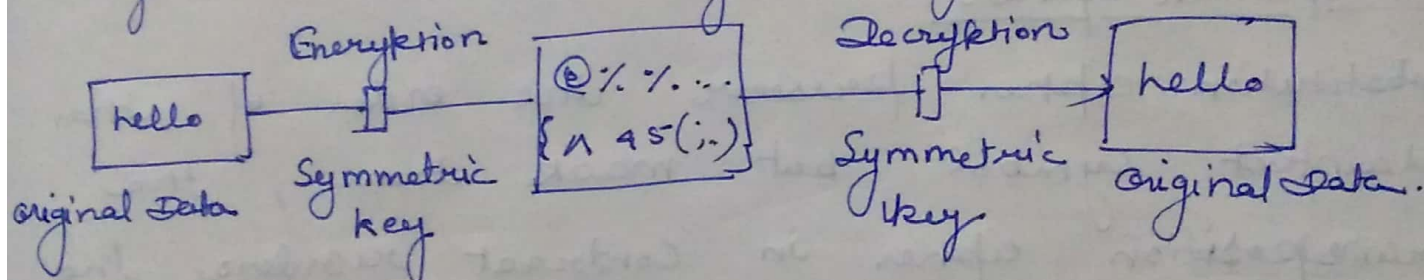
Types of Encryption (Algorithm)

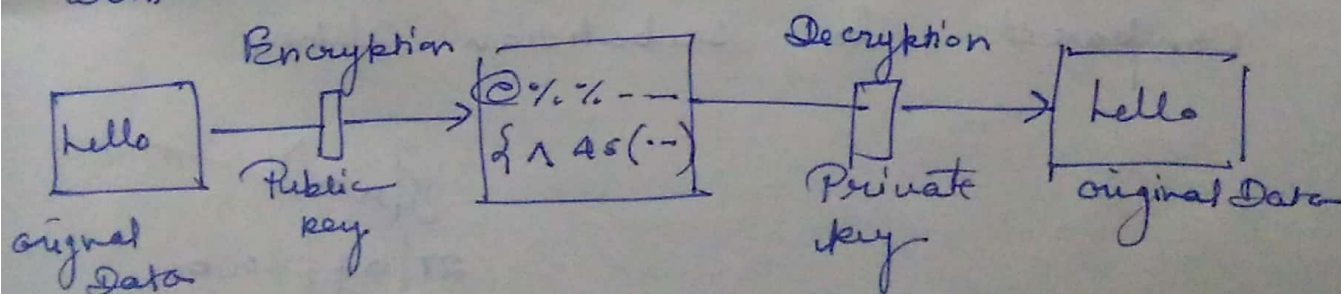There are two type of encryptions scheme as listed below.

1) Symmetric key encryption

2) Public key encryption

Symmetric key encryption

algorithm uses Cryptographic keys for both encryption and decryption of cipher text.

Encryption → [@%.%...{^45(;.)] → Decryption → hello

hello
original Data
Symmetric key

Symmetric key
Original Data.

Public key encryption

algorithm uses pair of keys one of which is a secret key and one of which is public. These two keys are mathematically linked with each other

Encryption → [@%.%--{^45(.-)] → Decryption → hello

hello
original Data
Public key

Private key
original Data

Techniques used for encryption

There are following techniques used for encryption process I

Substitution cipher

In a substitution cipher each letter or group of letter is replaced by another letter or group of letters to mask them. For example if a is replaced with D, b with E, c with F and z with C. In this way attack becomes DWWDFN. The substitution cipher are not much secure because intruder can easily guess the substitution cipher character.

Transposition cipher

Substitution cipher preserve the order of the plaintext symbol but mask them, the transposition cipher in contrast reorders the letter but do not mask them. For this process a key is used for example if iliveingʃadian may be coded as divienaniqmti the transposition cipher are more secure as compared to substition cipher.

27/04/2020

Shardha Vaish