**Data Encryption Standard -DES**

**Introduction:**

As mentioned earlier there are two main types of cryptography in use today - **symmetric**

or **secret key** cryptography and **asymmetric** or **public key** cryptography. Symmetric

key cryptography is the oldest type whereas asymmetric cryptography is only being

used publicly since the late 1970’s1. Asymmetric cryptography was a major milestone

in the search for a perfect encryption scheme.

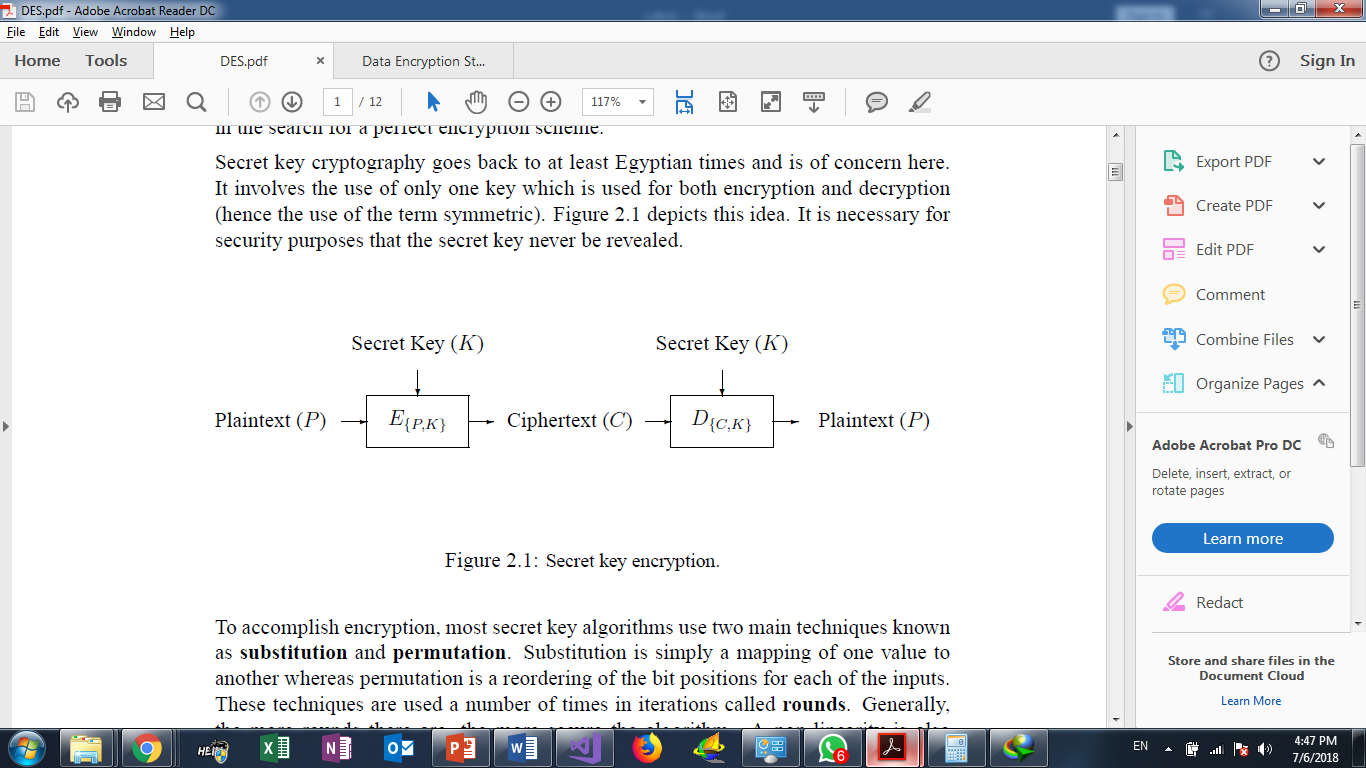
Secret key cryptography goes back to at least Egyptian times and is of concern here.

It involves the use of only one key which is used for both encryption and decryption

(hence the use of the term symmetric). Figure 2.1 depicts this idea. It is necessary for

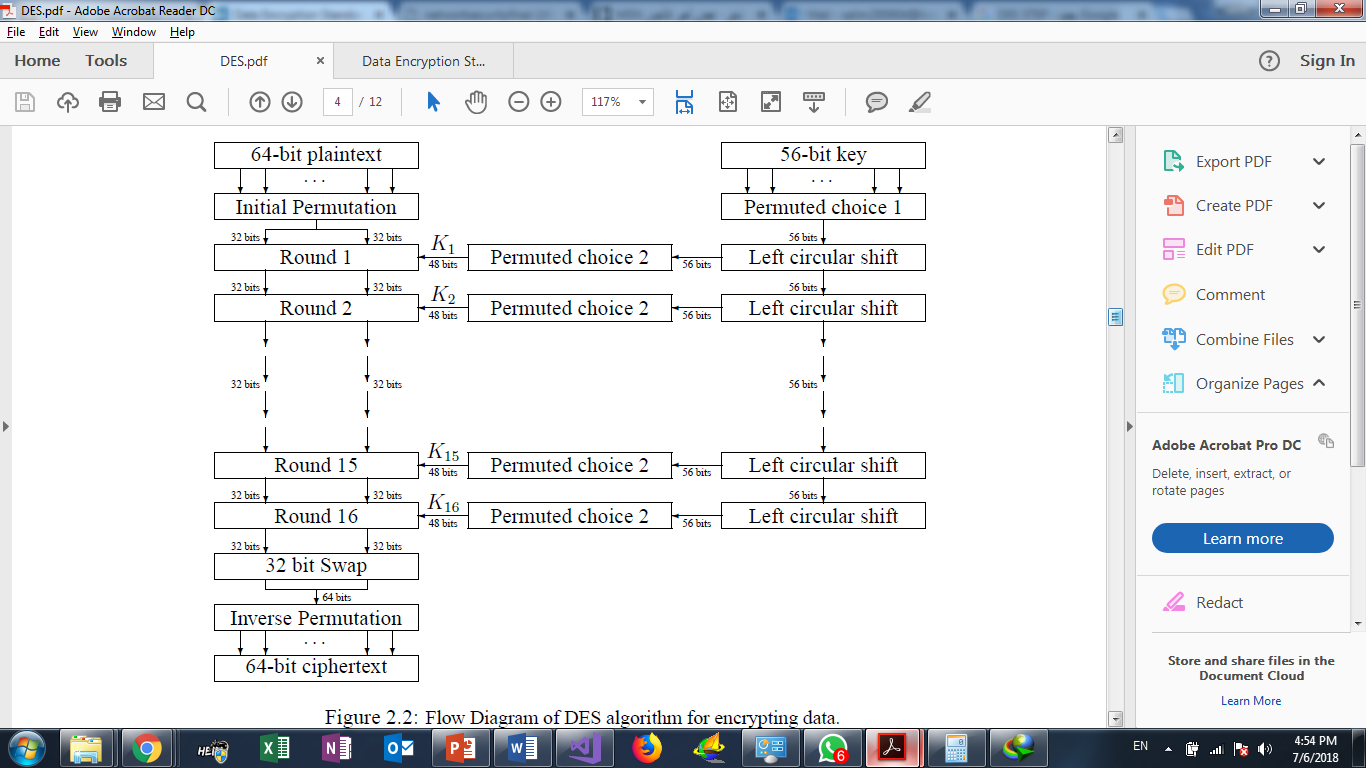
security purposes that the secret key never be revealed.

Several types of symmetric algorithms are used today. They have different methods of providing encryption and decryption functionality.



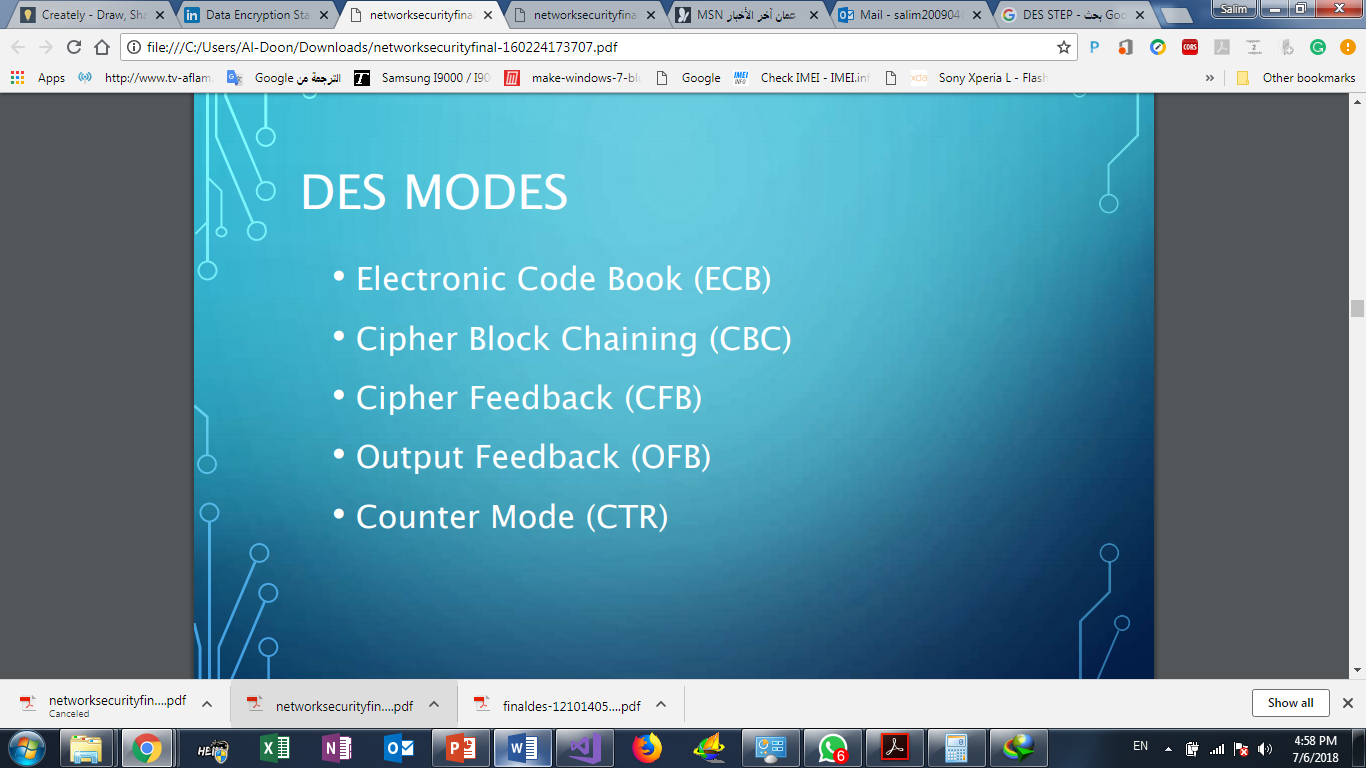
**How does DES work?**

* DES is a symmetric block encryption algorithm. When 64-bit blocks of plaintext go in, 64-bit blocks of cipher text come out.
* It is also a symmetric algorithm, meaning the same key is used for encryption and decryption.
* It uses a 64-bit key: 56 bits make up the true key, and 8 bits are used for parity.
* When the DES algorithm is applied to data, it divides the message into blocks and operates on them one at a time.
* The blocks are put through 16 rounds of transposition and substitution functions.
* The result is 64-bit blocks of ciphertext.



**DES Modes:**

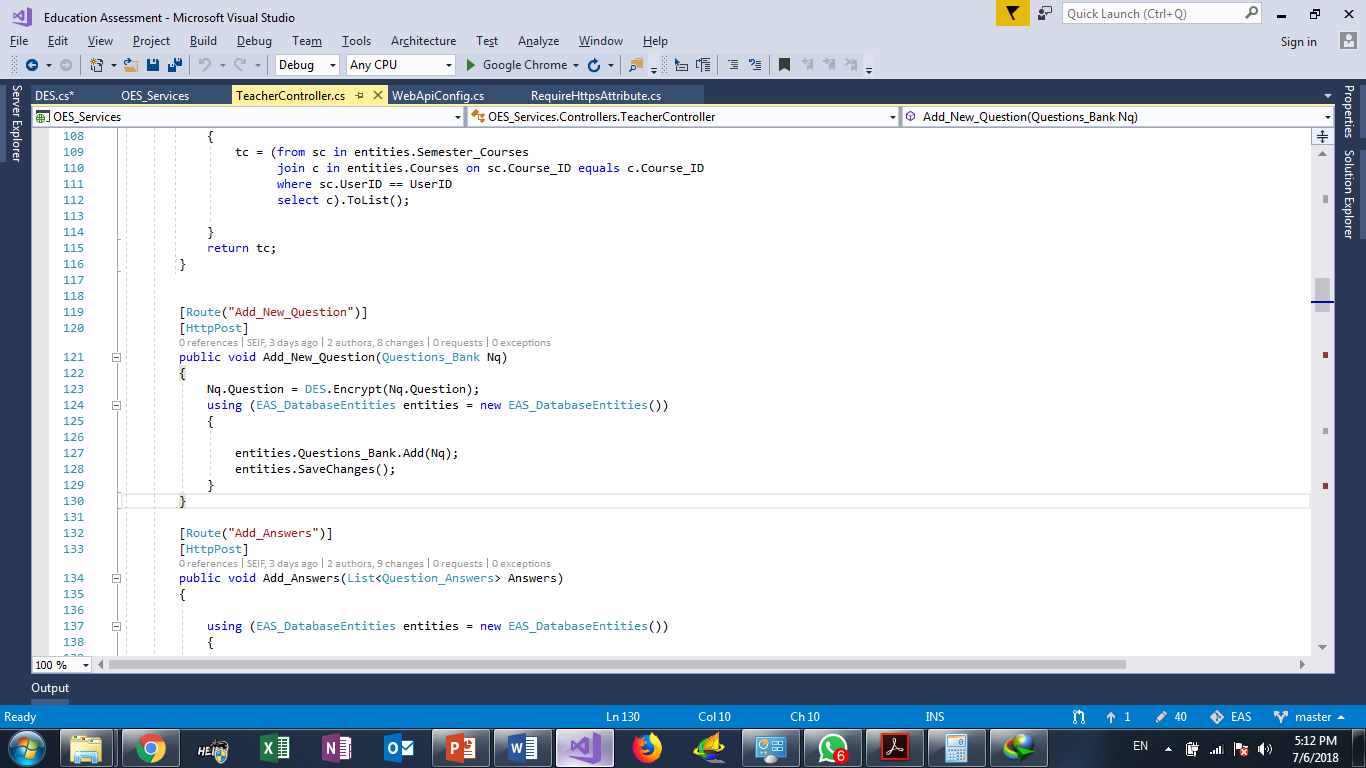
Block ciphers have several modes of operation. Each mode specifies how a block cipher will operate.



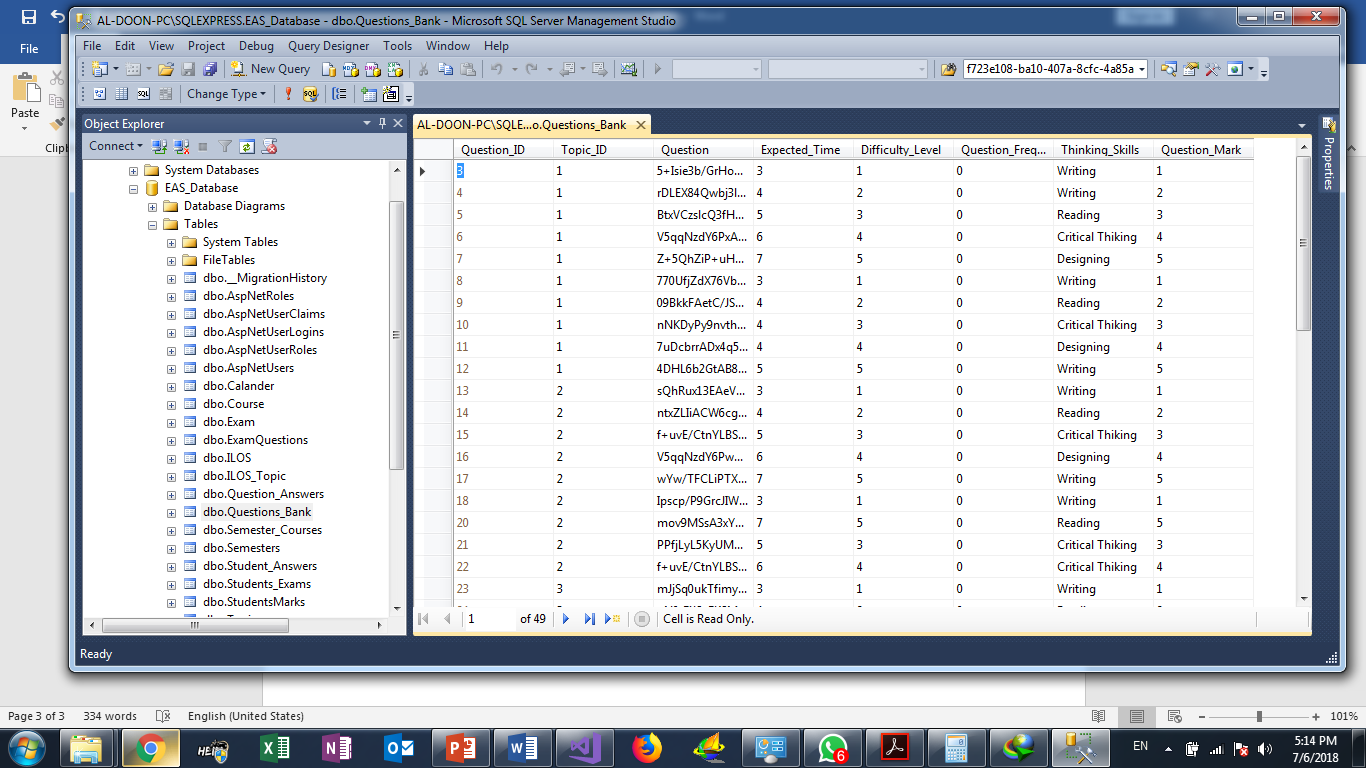
**How we apply DES in our system?**

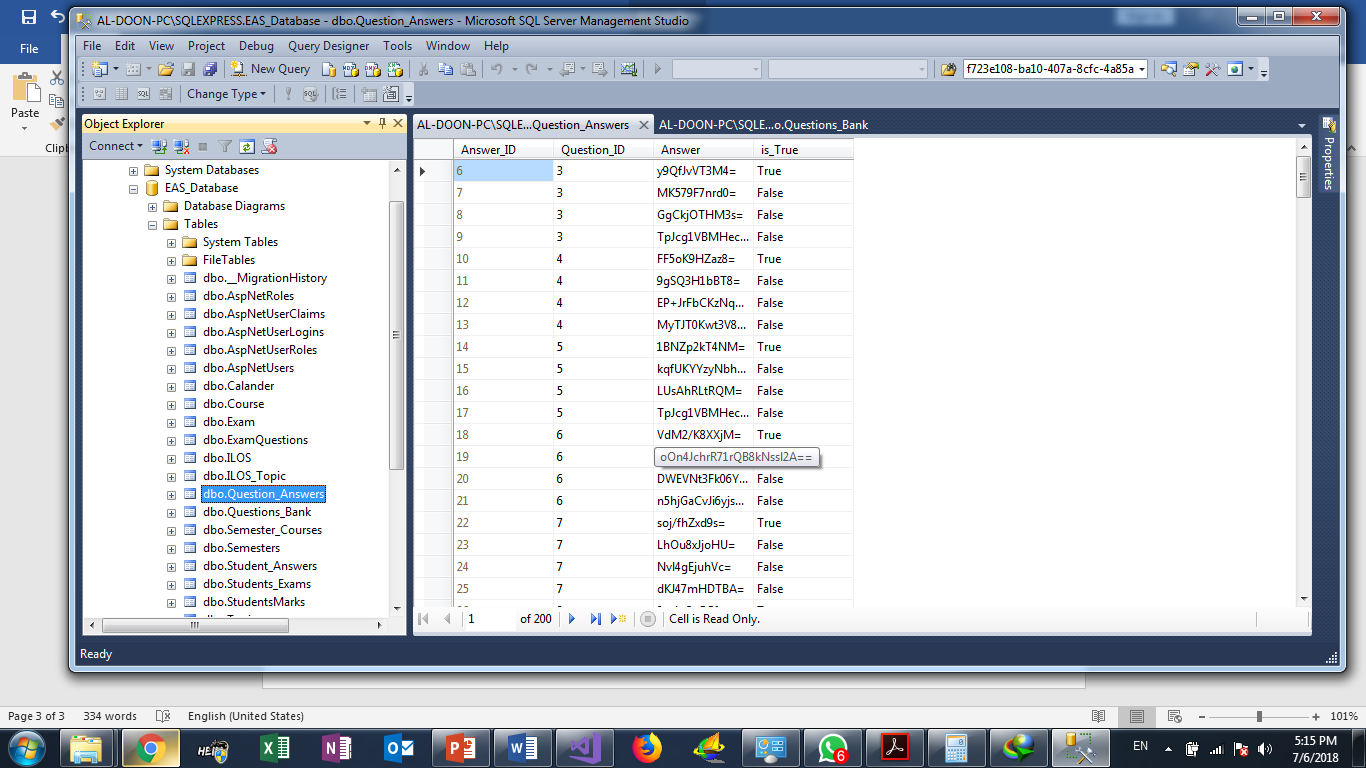
When the teacher wants to add a new question, the system applies Des. Encrypton on the question text and question answers before save it in the Database, these step is too important to protect Questions from hacking

To apply DES Algorithm we use ASP DESCryptoServiceProvider ,so the teacher insert question and his answer ,the system call Des. Encrypton For encryption



now in the Database the question was saved in encrypted form:





**When we use DES Decrypt?**

In the Exam. after Question algorithm Controller prepare exam question ,the system apply DES. Decrypt and display questions to students, so from save questions in database to Exam date ,questions Safely reserved

