**Practical No : 4** Name : Roshan Naicker

**Block Cipher and modes**  Roll No : 5021137

**of operation**

**Aim :** Encrypt messages using various modes of operation using AES or DES.

**Objectives :** To know how to break Mono-alphabetic Substitution Cipher using frequency

analysis method.

**Theory :**

A block cipher mode of operation is a particular way to use a block cipher, such as DES or AES, by combining it with some simple operations and feedback mechanism.

The modes considered here are the Electronic Code Book (ECB) mode, the Cipher Block Chaining (CBC) mode, the Output Feedback (OFB) mode, the Cipher Feedback

(CFB) mode, and the Counter (CTR) mode.

**DES (*Data Encryption Standard)***

The DES Algorithm is a block cipher that uses symmetric keys to convert 64-bit plaintext blocks into 48-bit ciphertext blocks. The (DES) Data Encryption Standard Algorithm was developed by the IBM team in the 1970s. It has since been accepted by the National Institute of Standards and Technology (NSIT). The DES encryption algorithm uses symmetric keys, which means that the same key is used for encrypting and decrypting the data.

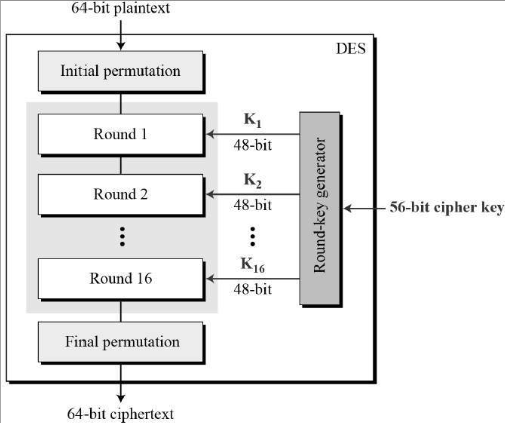
## **DES Algorithm Steps**

* The initial permutation (IP) function receives the 64-bit plaintext block.
* The IP is performed on plaintext.
* The IP then makes two halves of the block that has been permutated. The two halves are known as left plan text (LPT) and right text (RPT).
* All LPTs and RPTs are encrypted 16 times.
* The LPT and RPT are joined, and then the final permutation (FP) is performed on this block.
* The 64-bit ciphertext is now ready.

**In the encryption process (step 4), there are five stages:**

* Key transformation
* Expansion permutation
* S-Box permutation
* P-Box permutation
* XOR, and swap

In the decryption process, the same algorithm is used with the order of the 16 keys reversed. Expansions, permutations, and substitutions are some of the functions used in the rounds, as well as an XOR operation with a round key. Although DES was regarded to be less safe for encrypting highly confidential data of government because it uses a smaller shared key, triples-DES was invented to counter this. Still, it was also not considered a good algorithm because it encrypts data very slowly. In DES, even a minor change in the input text results in a completely new ciphertext.

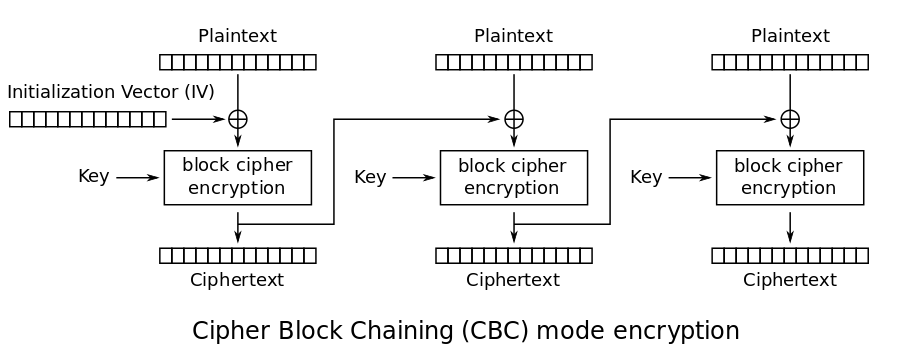


**AES (Advanced Encryption Standard)**

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that was established as a federal standard in the United States in 2001. It is used to secure sensitive data by encrypting it, making it unreadable to unauthorized parties. AES operates on blocks of data and is particularly well-suited for encrypting large amounts of data efficiently.

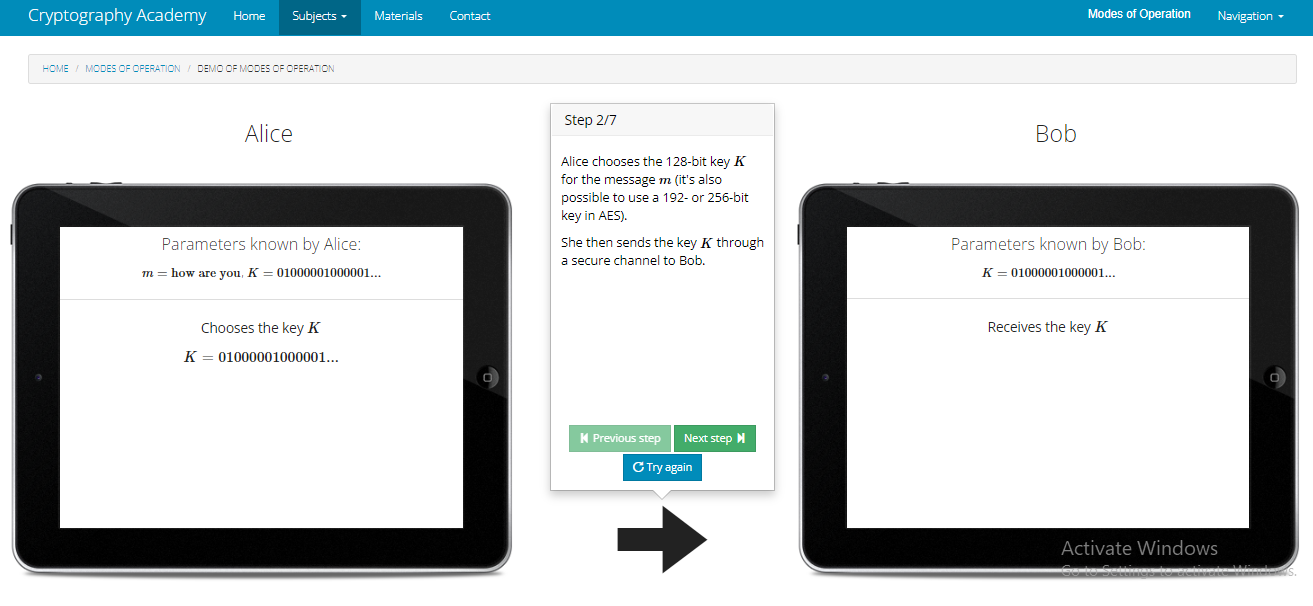
Here are some key features and aspects of the AES algorithm:

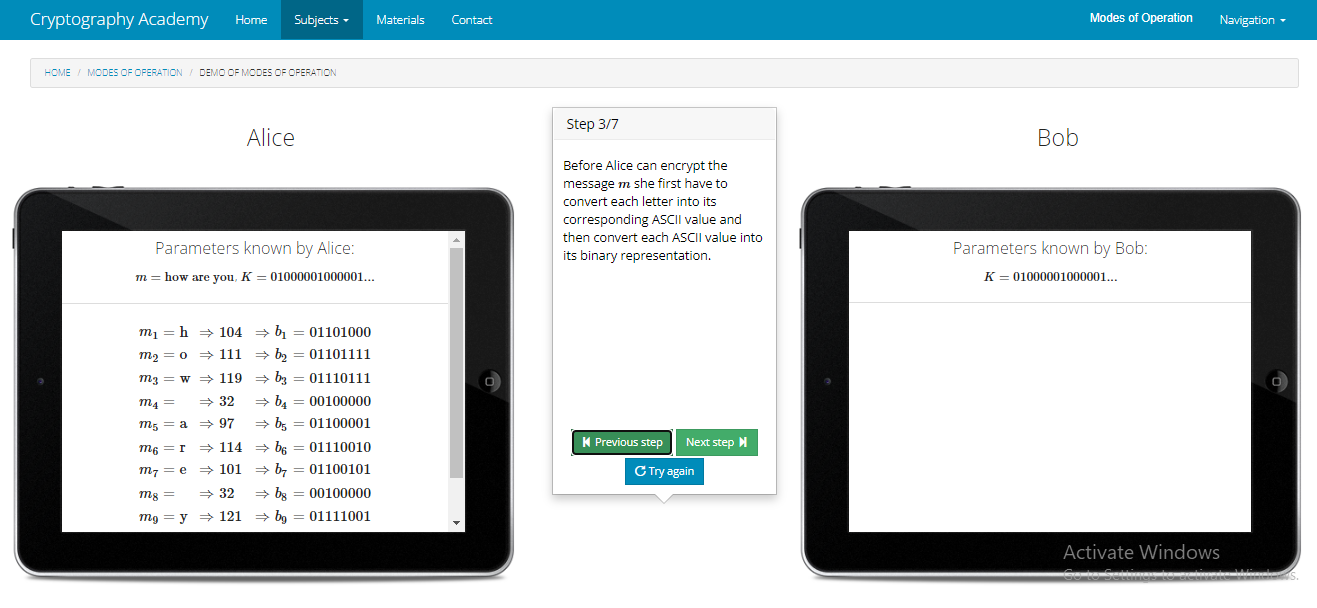
* Symmetric Encryption: AES is a symmetric encryption algorithm, which means the same key is used for both encryption and decryption. This requires that both the sender and the receiver have access to the same secret key.
* Block Cipher: AES operates on fixed-size blocks of data. The block size for AES is 128 bits (16 bytes).
* Key Lengths: AES supports key lengths of 128, 192, or 256 bits. The strength of the encryption increases with longer key lengths, but longer keys also require more computational resources.
* Substitution-Permutation Network (SPN): AES employs a series of transformations, including byte substitution (SubBytes), shift rows (ShiftRows), mix columns (MixColumns), and add round key (AddRoundKey), which are applied in multiple rounds to the input data.
* Key Expansion: AES uses a key expansion process to generate round keys for each round of encryption. These round keys are derived from the original encryption key using a combination of operations.
* Security: AES is considered highly secure and resistant to various types of attacks, such as brute force, differential, and linear attacks. The security of AES is based on the complexity of its mathematical operations and the number of rounds it employs.
* Modes of Operation: AES can be used in various modes of operation, such as Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), Galois/Counter Mode (GCM), and others, which determine how the algorithm processes data blocks and handles issues like data integrity and confidentiality.
* Wide Adoption: AES has become the de facto standard for symmetric encryption and is used in a wide range of applications, including secure communications, data protection, file encryption, disk encryption, and more.

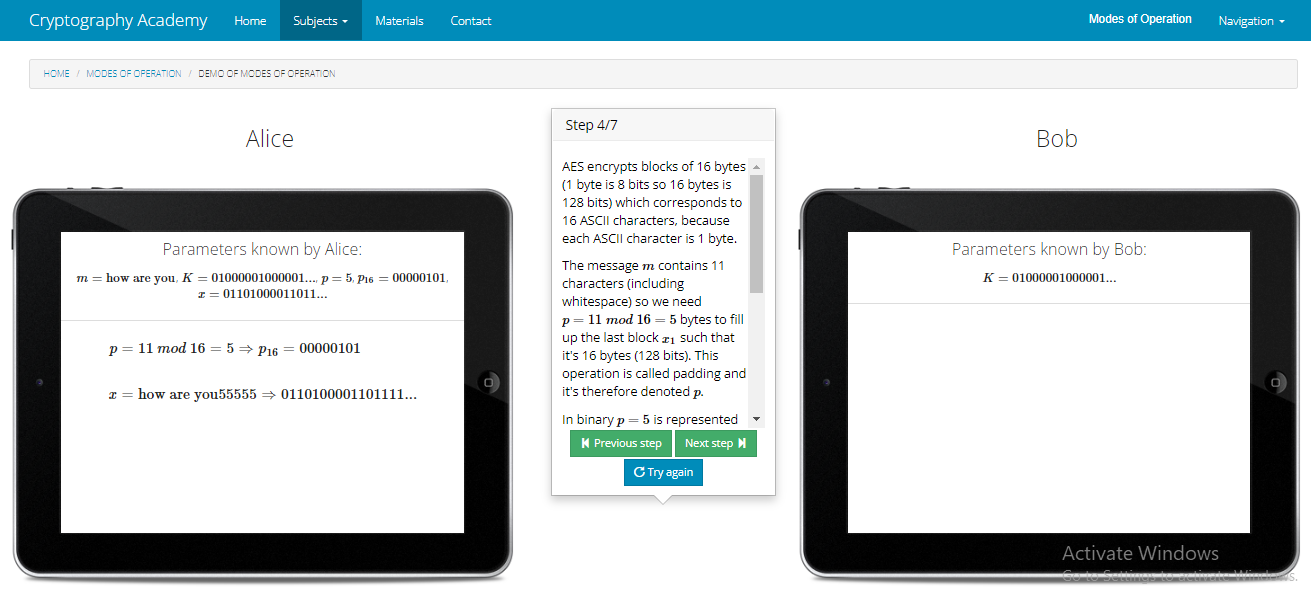


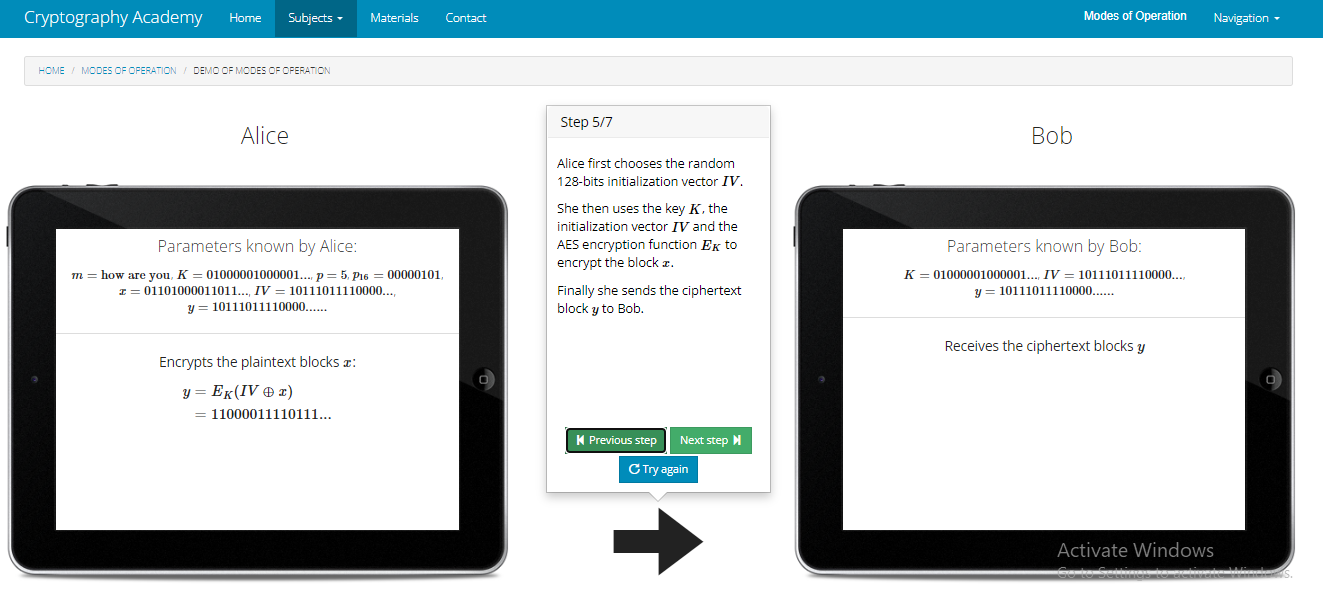
**Results:**

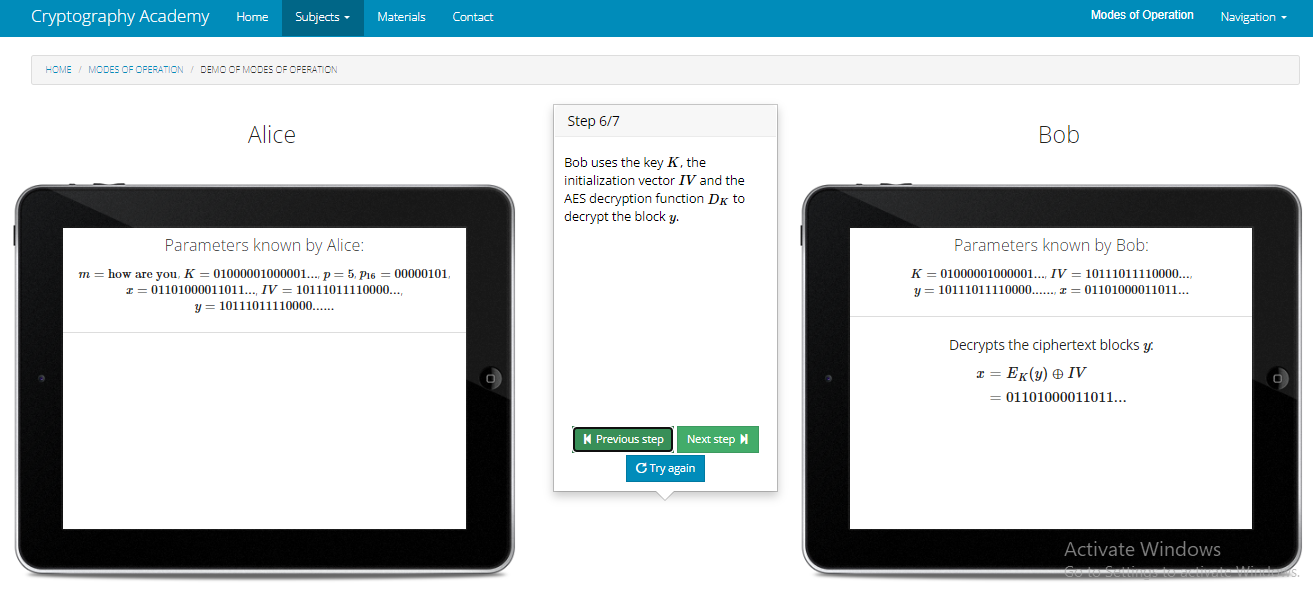
Advanced encryption standard

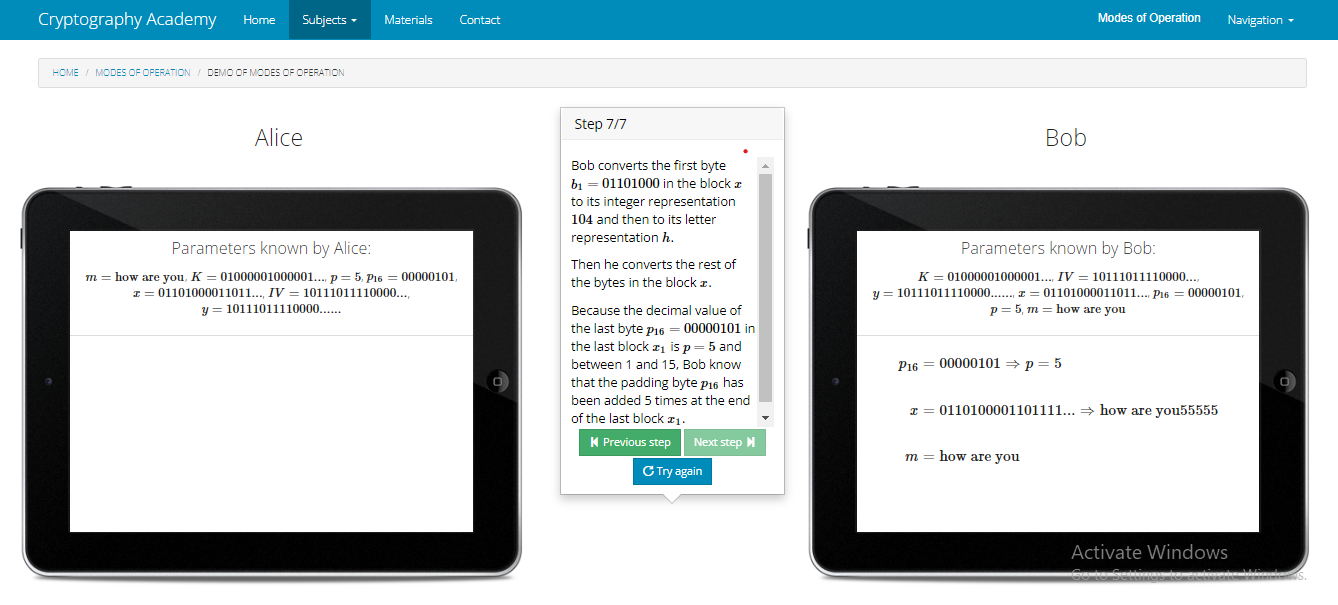




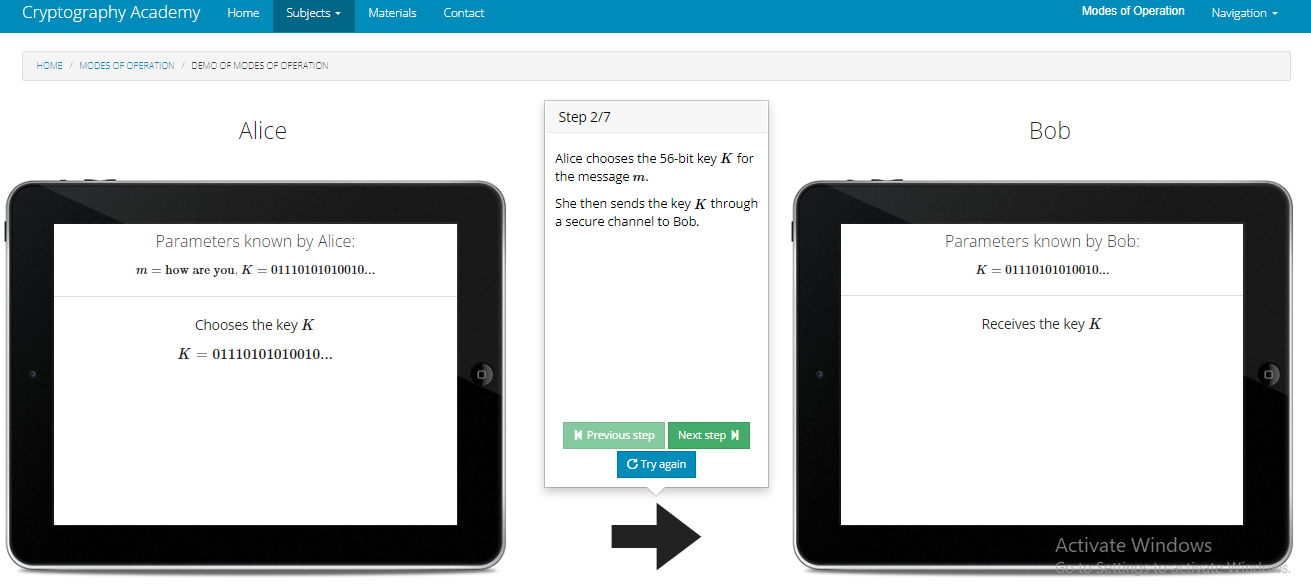


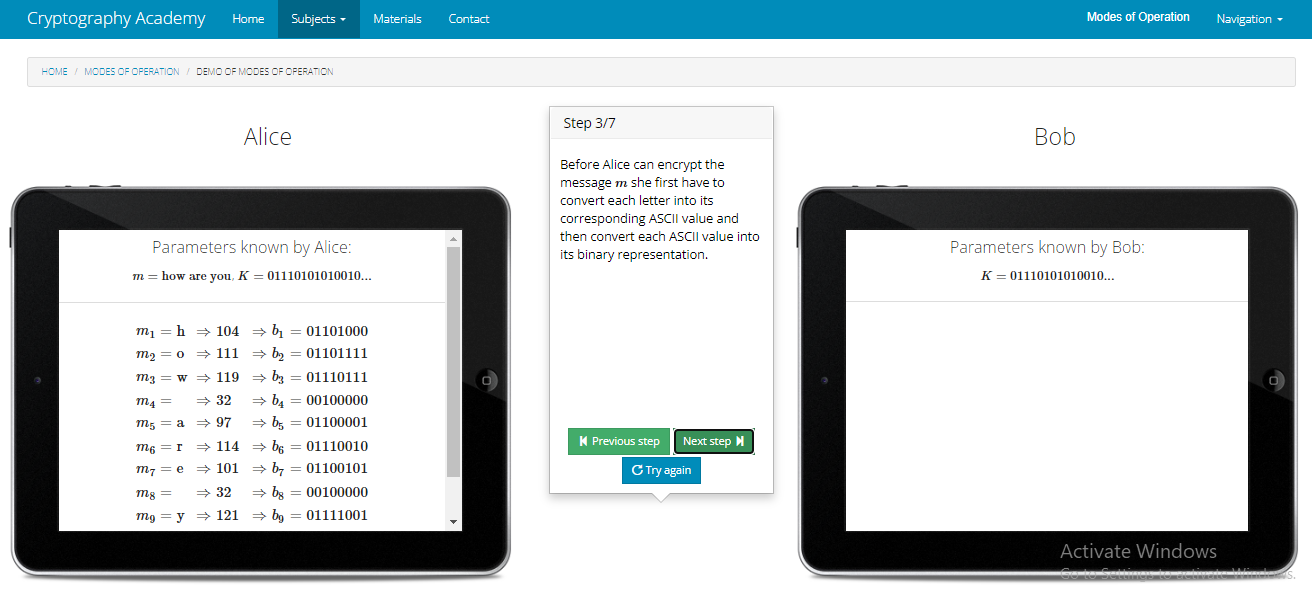


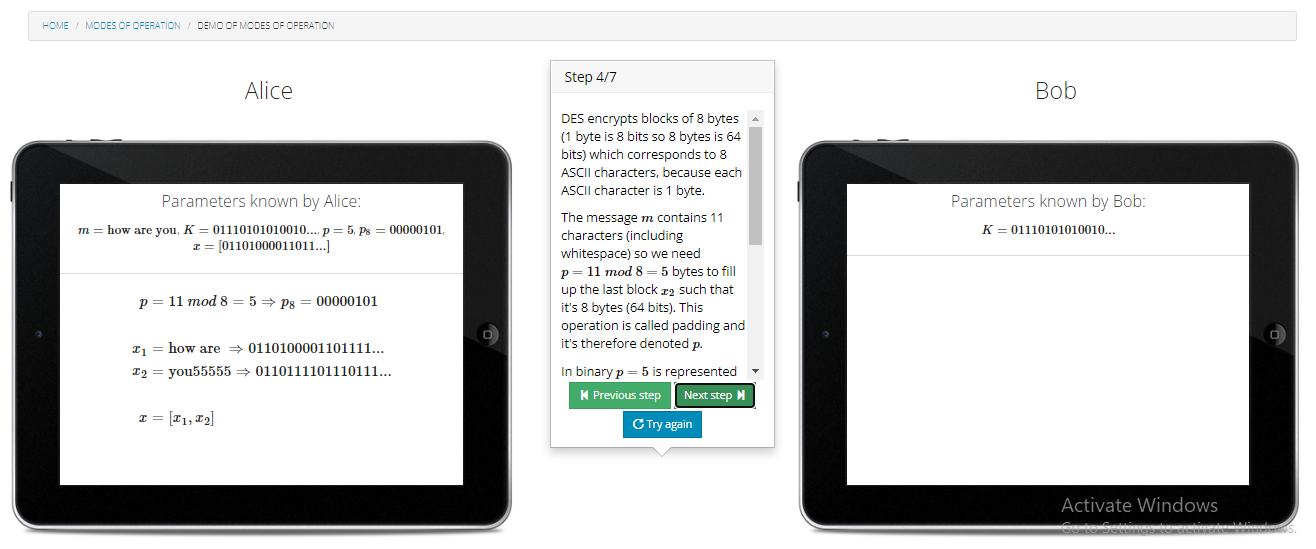


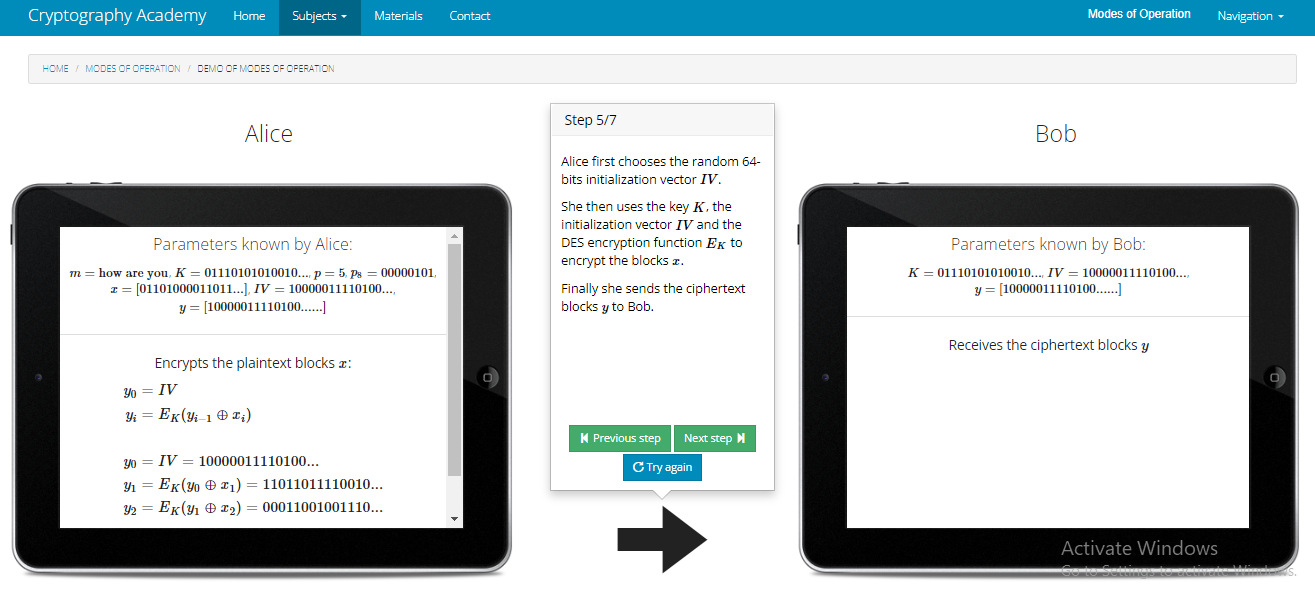


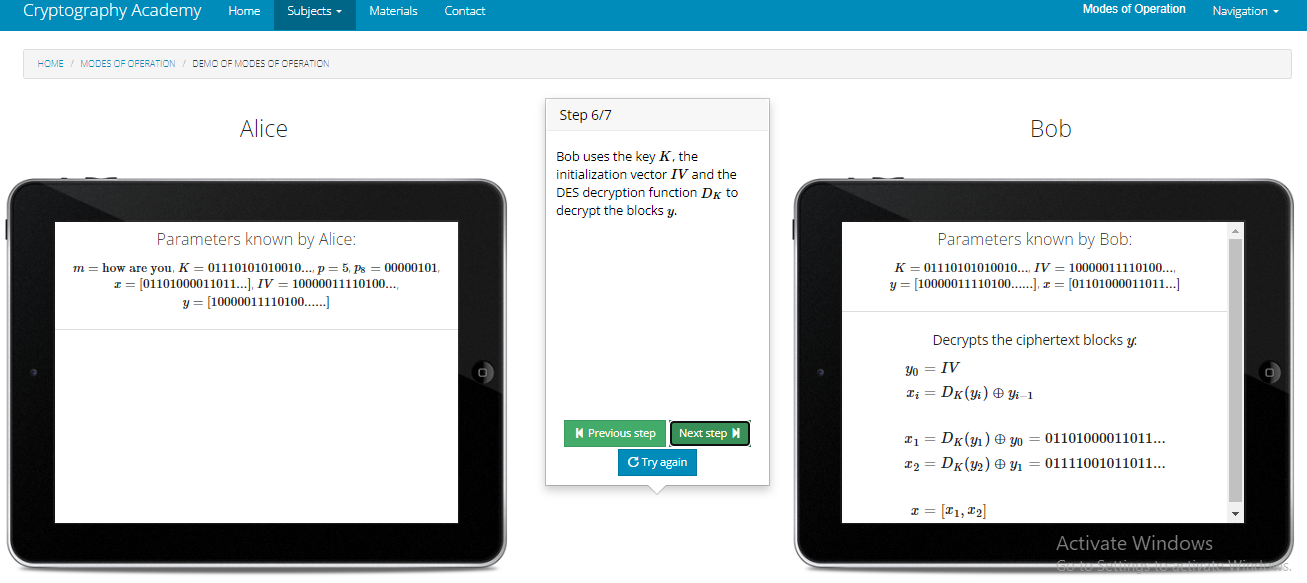
Data encryption standard

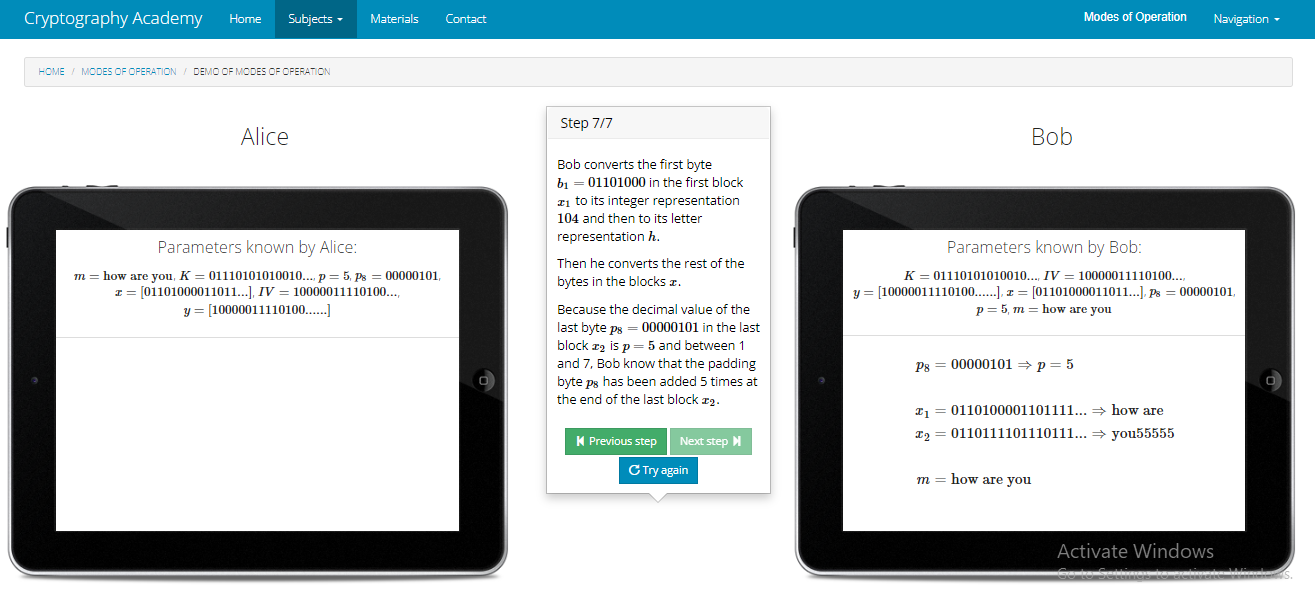












**Conclusion**: Observed the performance of different modes of operation using online tool.