**CNS Exp 5**

**Shashwat Tripathi  
D15A 64**

**Batch C**

**AIM: To understand how to Encrypt long messages using various modes of operation using AES or DES**

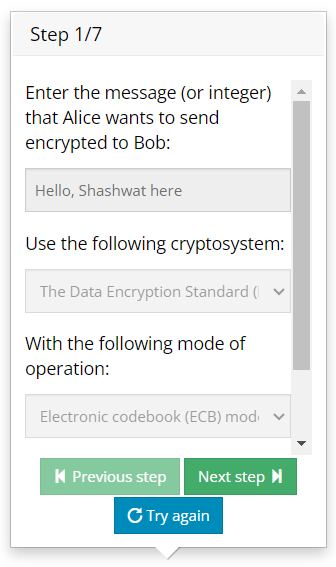
**Theory:**

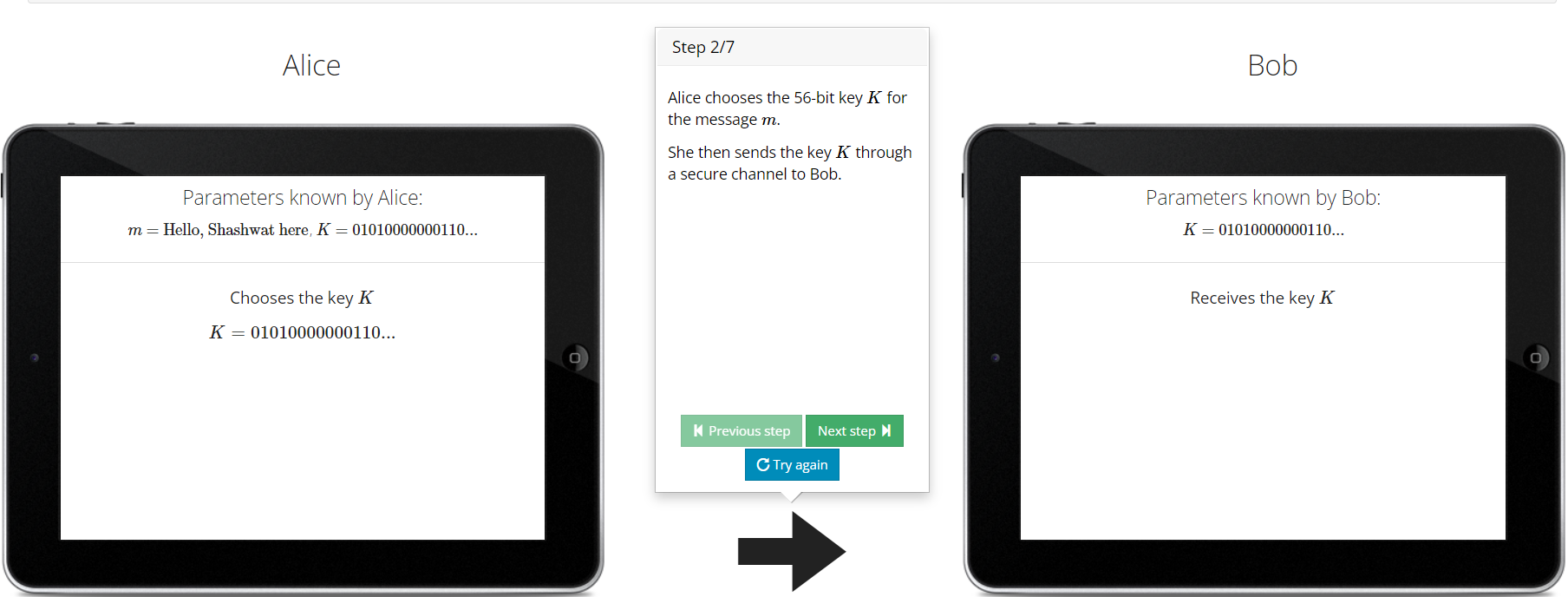
DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are two widely used symmetric-key encryption algorithms that serve to protect data confidentiality by converting plaintext data into ciphertext using a secret key. Here's a brief overview of both:

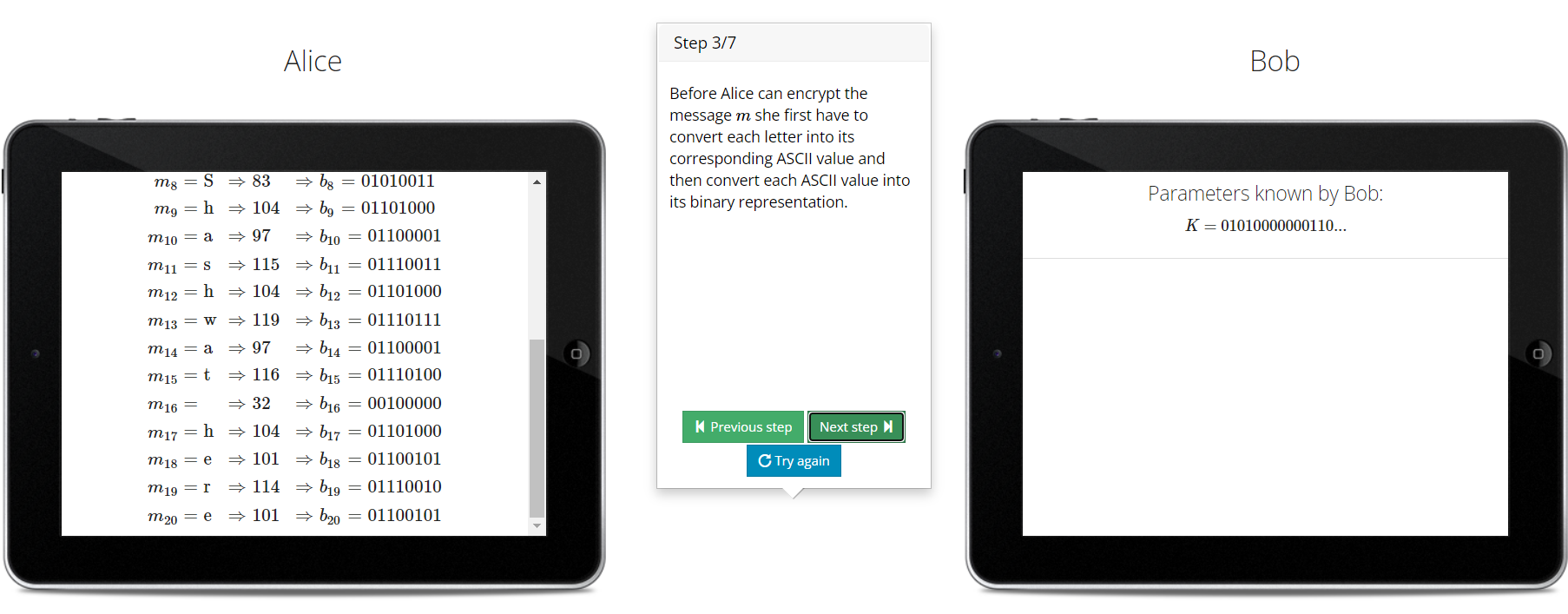
**1. DES (Data Encryption Standard):**

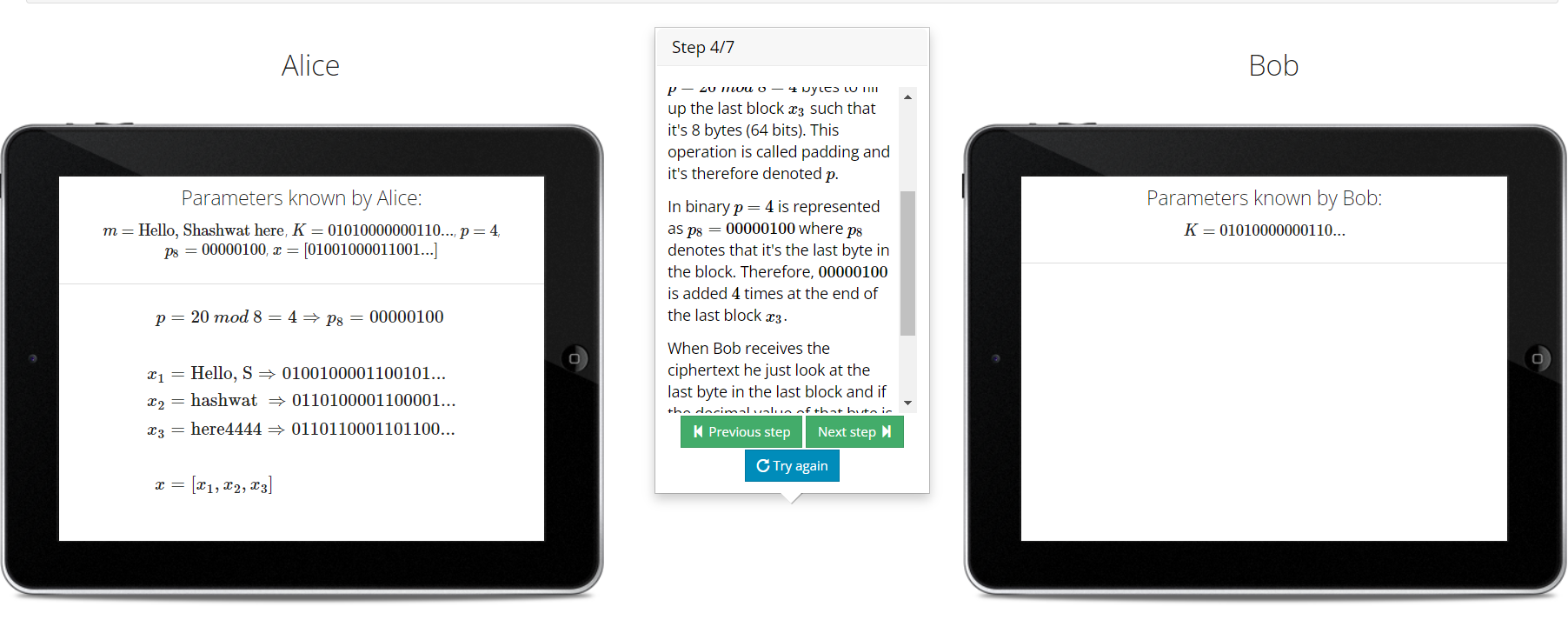
* Key Length: DES uses a 56-bit encryption key. This relatively short key length is one of the primary reasons why DES is no longer considered secure against modern attacks.
* Block Size: DES operates on 64-bit blocks of plaintext data.
* Encryption Process: DES uses a Feistel network structure. The encryption process involves multiple rounds (typically 16 rounds). During each round, the plaintext block is divided into two halves, and various mathematical operations, including substitution (S-boxes), permutation (P-boxes), and bitwise operations, are applied to each half using a round-specific subkey derived from the main encryption key. The results from each round are mixed and swapped, creating the ciphertext.
* Security Concerns: DES is no longer considered secure against modern cryptographic attacks, primarily due to its short key length. It can be vulnerable to brute-force attacks where an attacker tries all possible 2^56 keys to decrypt the data.

**Steps:**



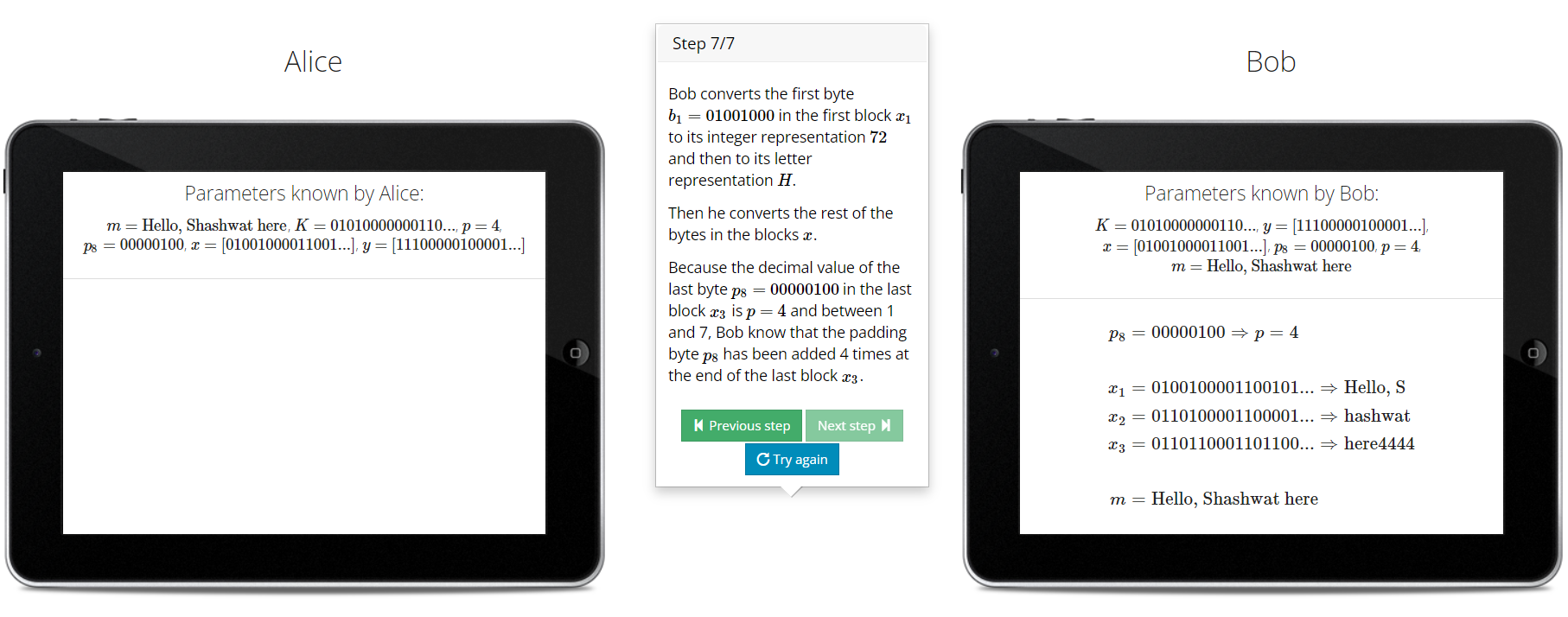






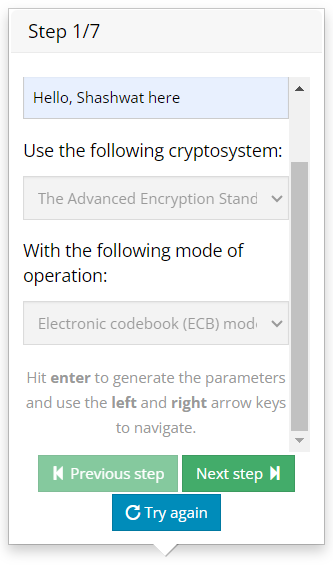




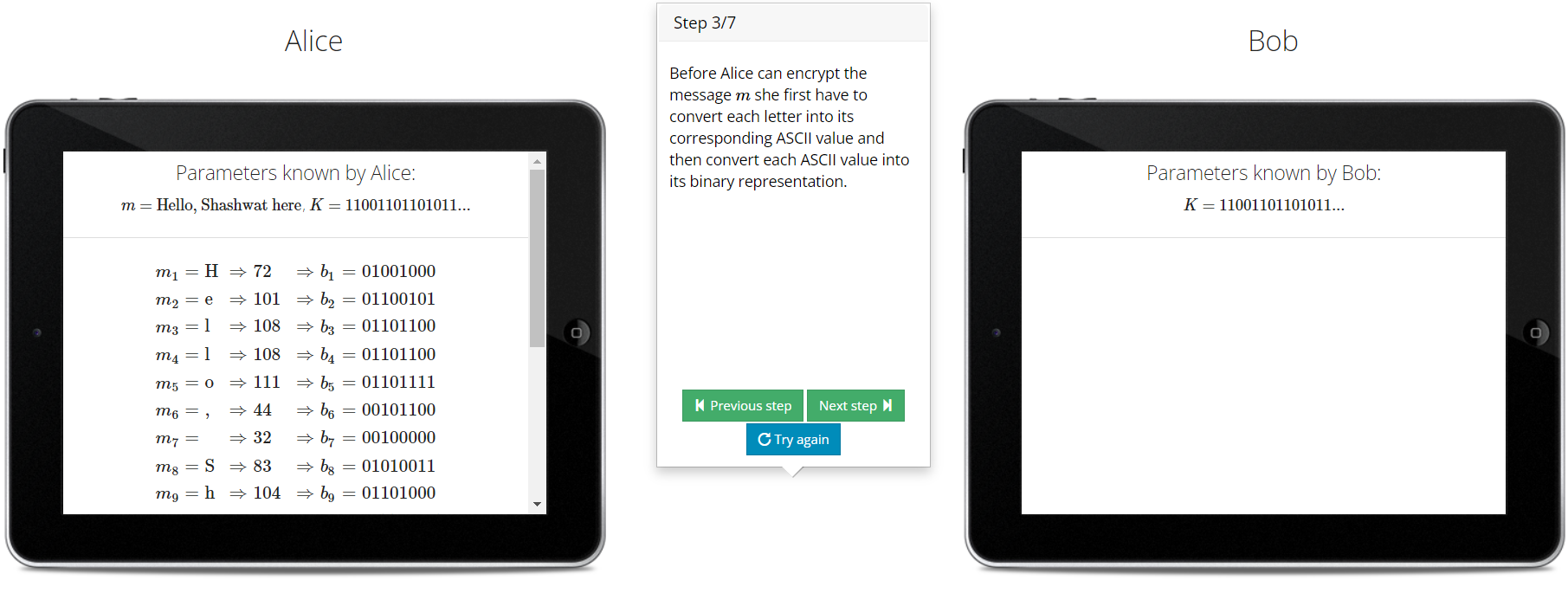


**2.** **AES (Advanced Encryption Standard):**

* Key Length: AES supports multiple key lengths, including 128-bit, 192-bit, and 256-bit keys. Longer key lengths provide higher security.
* Block Size:AES operates on 128-bit blocks of plaintext data.
* Encryption Process: AES uses a substitution-permutation network (SPN) structure. The encryption process involves several rounds, with the number of rounds depending on the key length (10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys). Each round consists of several operations, including a substitution step (SubBytes), permutation step (ShiftRows), mixing step (MixColumns), and adding a round key (XOR with a round-specific key derived from the main encryption key).
* Security: AES is widely regarded as highly secure against both brute-force and cryptographic attacks when used with sufficient key lengths. It has withstood extensive scrutiny and is widely adopted in various applications, including data encryption, secure communication protocols, and more.

****

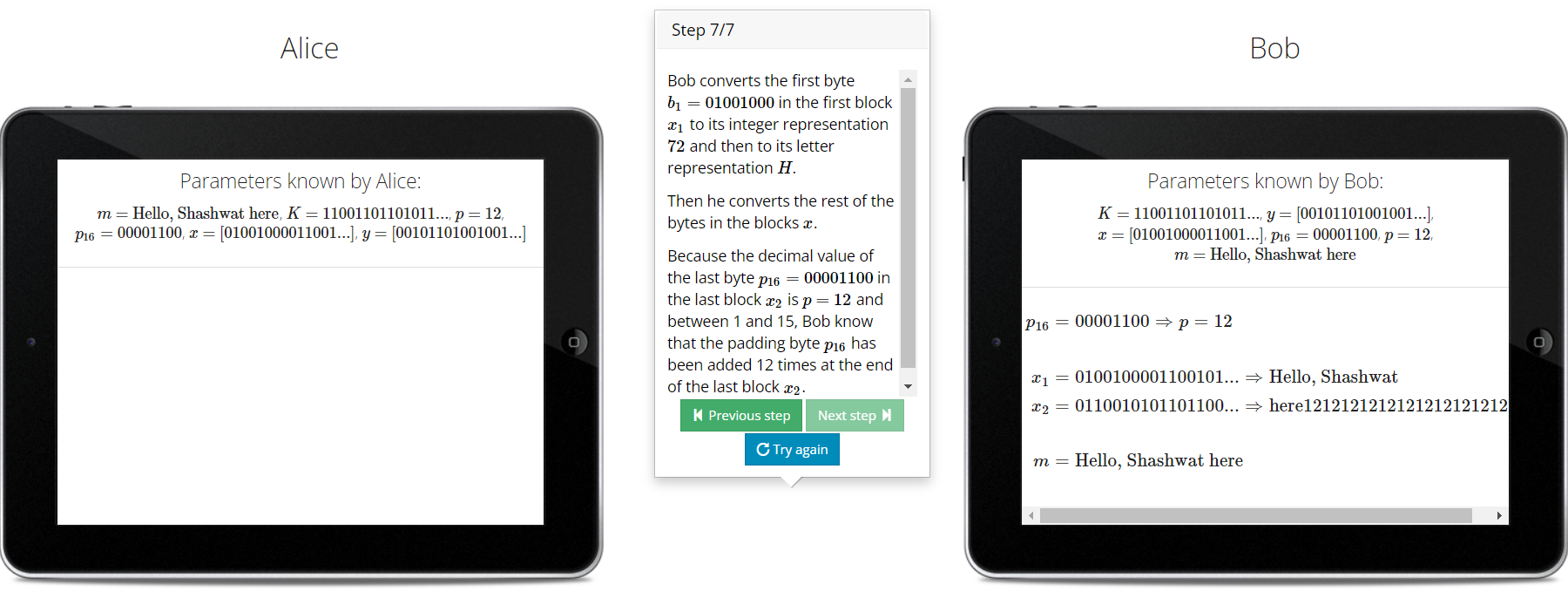
****

****

****

****

****

****

**CONCLUSION:**In summary,DES is no longer considered secure due to its short key length. AES, on the other hand, is a modern and widely accepted encryption standard that offers strong security with different key lengths and is suitable for various encryption applications.