SAD EXPERIMENT NO: 10

Aim: Understanding the concepts of cryptography and guidelines for using encryption

To do:

1. What types of cryptography are symmetric and asymmetric?
2. What are the cryptographic best practices according to OWASP?

Theory:

Cryptography is the study of encrypting and decrypting data to prevent unauthorized access. The ciphertext should be known by both the sender and the recipient. With the advancement of modern data security, we can now change our data such that only the intended recipient can understand it. Cryptography allows for the secure transmission of digital data between willing parties. It is used to safeguard company secrets, secure classified information, and sensitive information from fraudulent activity, among other things. Crypto means hidden and graph means writing.

Encryption is a fundamental component of cryptography, as it jumbles up data using various algorithms. Data encryption is the method of undoing the work done by encrypting data so that it can be read again. Cryptography is dependent on both of these methods.

A **symmetric key** is one that may be used to encrypt and decode data. This implies that in order to decrypt information, the same key that was used to encrypt it must be utilized. In practice, the keys represent a shared secret shared by two or more people that may be utilized to maintain a confidential information link

- **Data Encryption Standard (DES)**: An encryption algorithm that encrypts data with a 56-bit, randomly generated symmetric key. DES is not a secure encryption algorithm and it was cracked many times. Data Encryption Standard (DES) was developed by IBM and the U.S. Government together. DES is a block encryption algorithm.

- **Triple DES (3DES)**: Triple DES was developed from DES, uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. In 3DES, DES encryption is applied three times to the plaintext. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C. 3DES is a block encryption algorithm.

- **Advanced Encryption Standard**:- developed in 2001. As triple-DES was found to be slow, AES was created and is six times faster than the triple DES. It is one of the most widely used symmetric block cipher algorithm used nowadays. It works on bytes rather than bits.

- **Data Encryption Standard** :- developed in 1977. It is a multi-round cipher that divides the full text into 2 parts and then work on each part individually. It includes various functionality such as Expansion, Permutation, and Substitution, XOR operation with a round key.

Asymmetric keys are the cornerstone of Public Key Infrastructure (PKI), an encryption technique that requires two keys, one to lock or encrypt the plaintext and another to unlock or decrypt the ciphertext. Neither key performs both functions.

- **Rivest Shamir Adleman (RSA):-** RSA, which was patented in 1983 and still the most widely-used system for digital security, was released the same year as Diffie-Hellman. RSA gets much of its added security by combining two algorithms: one is applied to asymmetric cryptography, or PKI (Public Key Infrastructure), and the other algorithm provides for secure digital signatures. While the essential mathematics of both components is similar, and the output keys are of the same format.

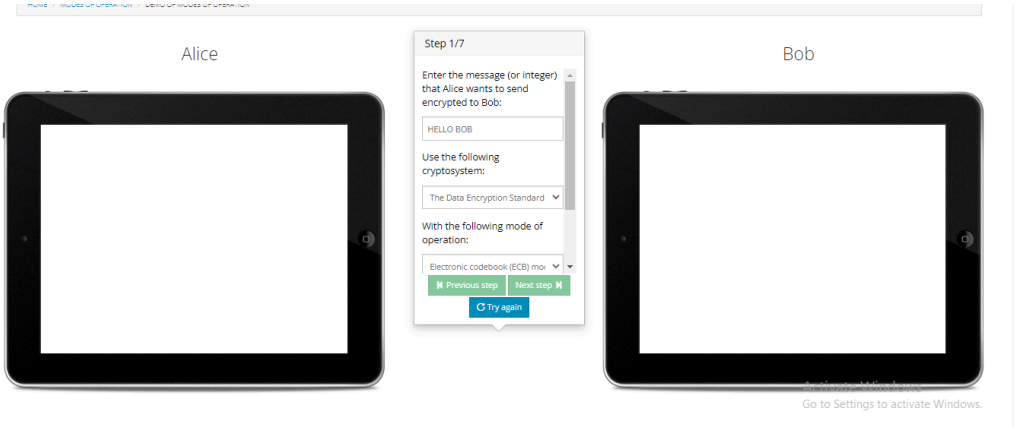
- **Digital Signature Algorithm (DSA):-**
  In 1991, the National Security Agency (NSA) developed the Digital Signature Algorithm (DSA) as an alternative to the RSA algorithm. Like RSA, DSA is an asymmetric encryption scheme, or PKI, which generates a pair of keys, one public and one private. The signature is created privately, though it can be identified publicly; the benefit of this is that only one authority can create the signature, but any other party can validate the signature using the public key. DSA, as a result, is faster in signing, but slower in verifying.

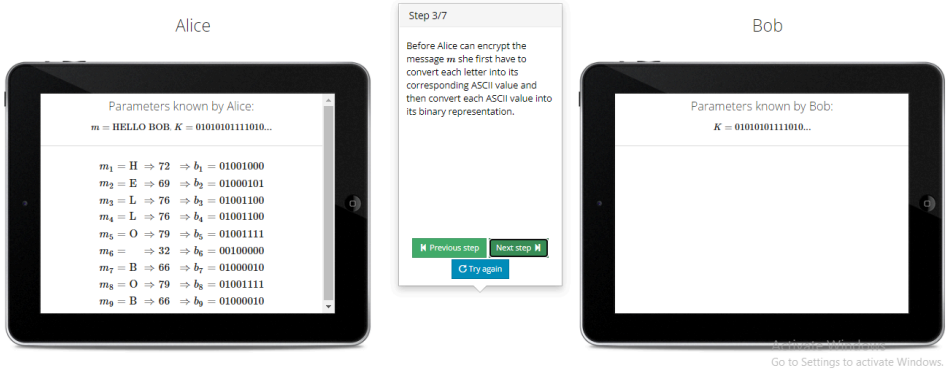
- **Diffie-Hellman:**
  The first prime-number, security-key algorithm was named Diffie-Hellman algorithm and patented in 1977. The Diffie-Hellman algorithm is non-authenticated protocol, but does require the sharing of a “secret” key between the two communicating parties. The two parties agree on an arbitrary starting number that they share, then each selects a number to be kept private.

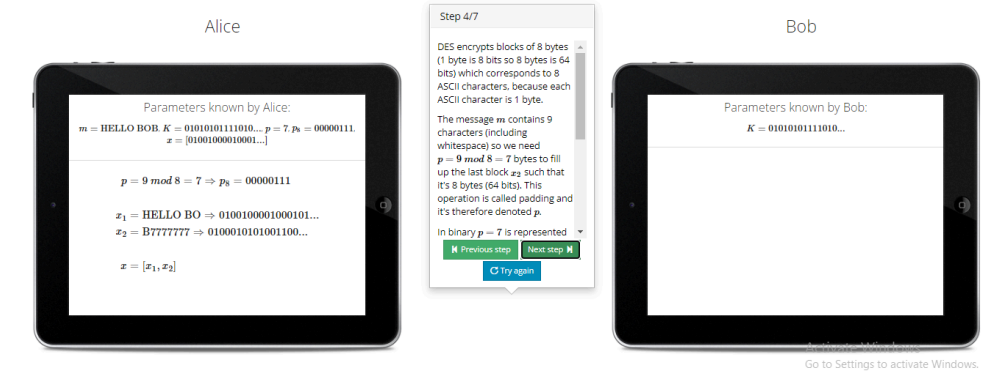
Implementation:

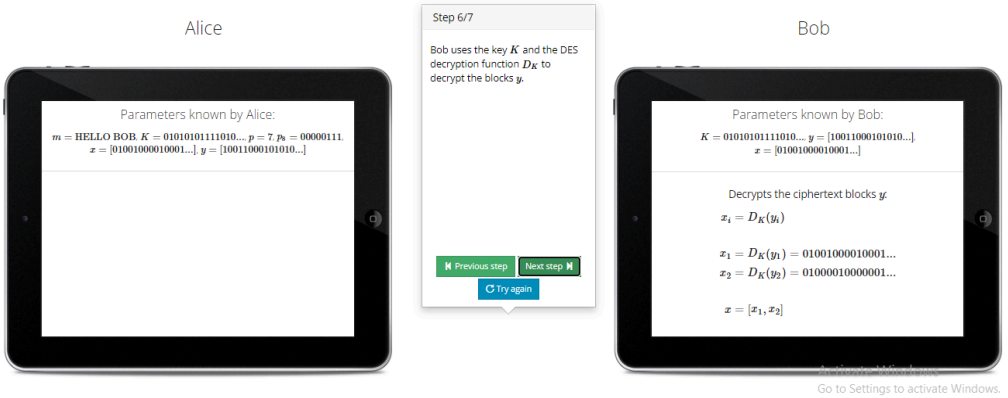
Link: https://cryptographyacademy.com/modes-of-operation/protocol/

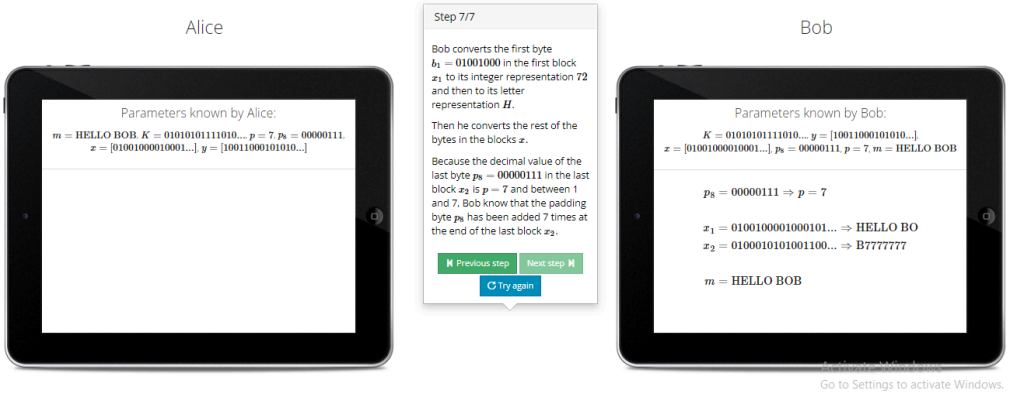
DES: Data encryption standard (DES) has been found vulnerable to very powerful attacks DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext.



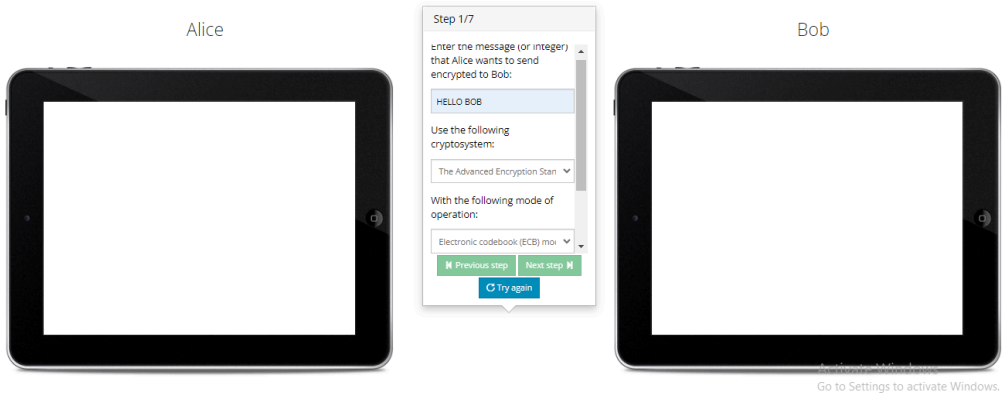


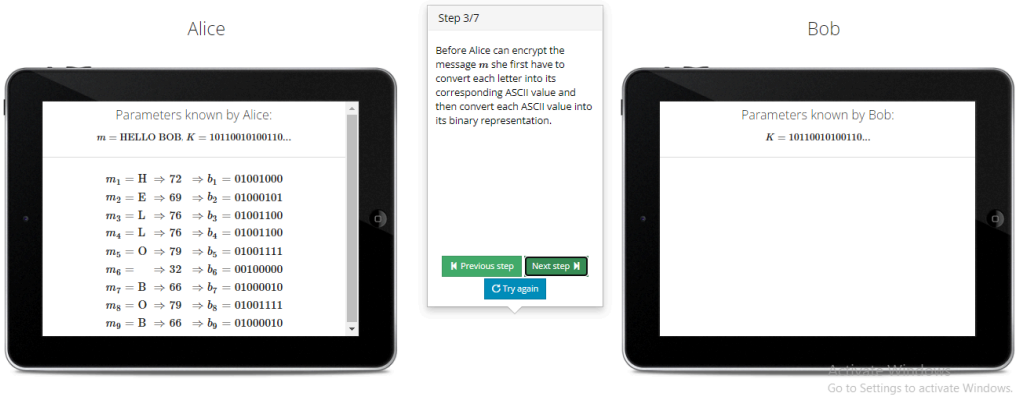


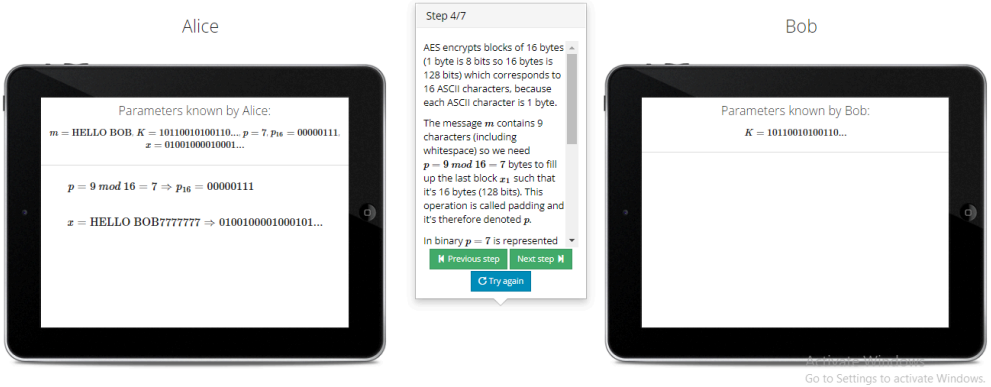


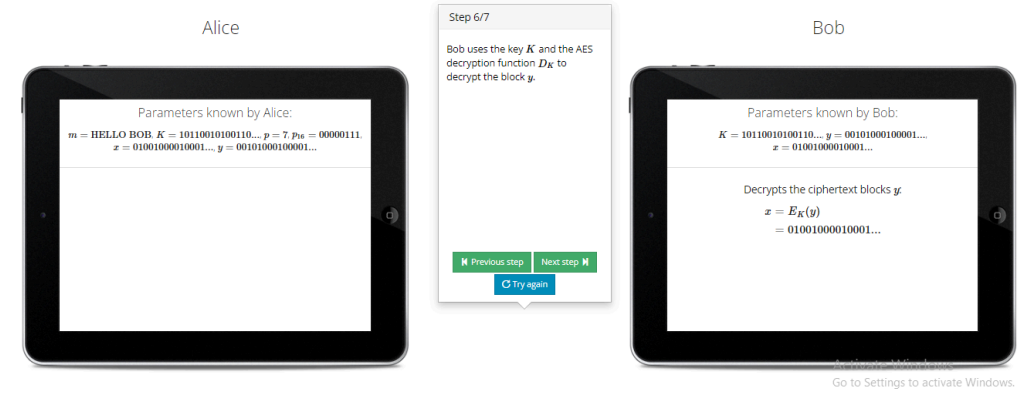


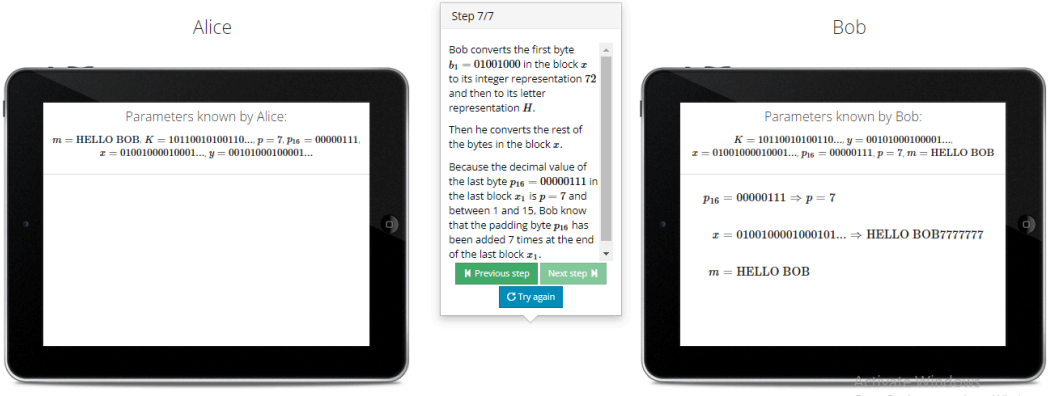
AES: AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.




Alice
Parameters known by Alice:
m = HELLO BOB, $K = 10110010100110...$
m_1 = H ⇒ 72 ⇒ b_1 = 01001000
m_2 = E ⇒ 69 ⇒ b_2 = 01000101
m_3 = L ⇒ 76 ⇒ b_3 = 01001100
m_4 = L ⇒ 76 ⇒ b_4 = 01001100
m_5 = O ⇒ 79 ⇒ b_5 = 01001111
m_6 = ⇒ 32 ⇒ b_6 = 00100000
m_7 = B ⇒ 66 ⇒ b_7 = 01000010
m_8 = O ⇒ 79 ⇒ b_8 = 01001111
m_9 = B ⇒ 66 ⇒ b_9 = 01000010
Step 3/7
Before Alice can encrypt the message m she first have to convert each letter into its corresponding ASCII value and then convert each ASCII value into its binary representation.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10110010100110...$


Alice
Parameters known by Alice:
m = HELLO BOB, $K = 10110010100110...$, $p = 7$, $p_{16} = 00000111$, $x = 01001000010001...$
$p = 9 \ mod \ 16 = 7 \Rightarrow p_{16} = 00000111$
x = HELLO BOB7777777 ⇒ 0100100001000101...
Step 4/7
AES encrypts blocks of 16 bytes (1 byte is 8 bits so 16 bytes is 128 bits) which corresponds to 16 ASCII characters, because each ASCII character is 1 byte.
The message m contains 9 characters (including whitespace) so we need $p = 9 \ mod \ 16 = 7$ bytes to fill up the last block x_1 such that it's 16 bytes (128 bits). This operation is called padding and it's therefore denoted p.
In binary $p = 7$ is represented
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10110010100110...$

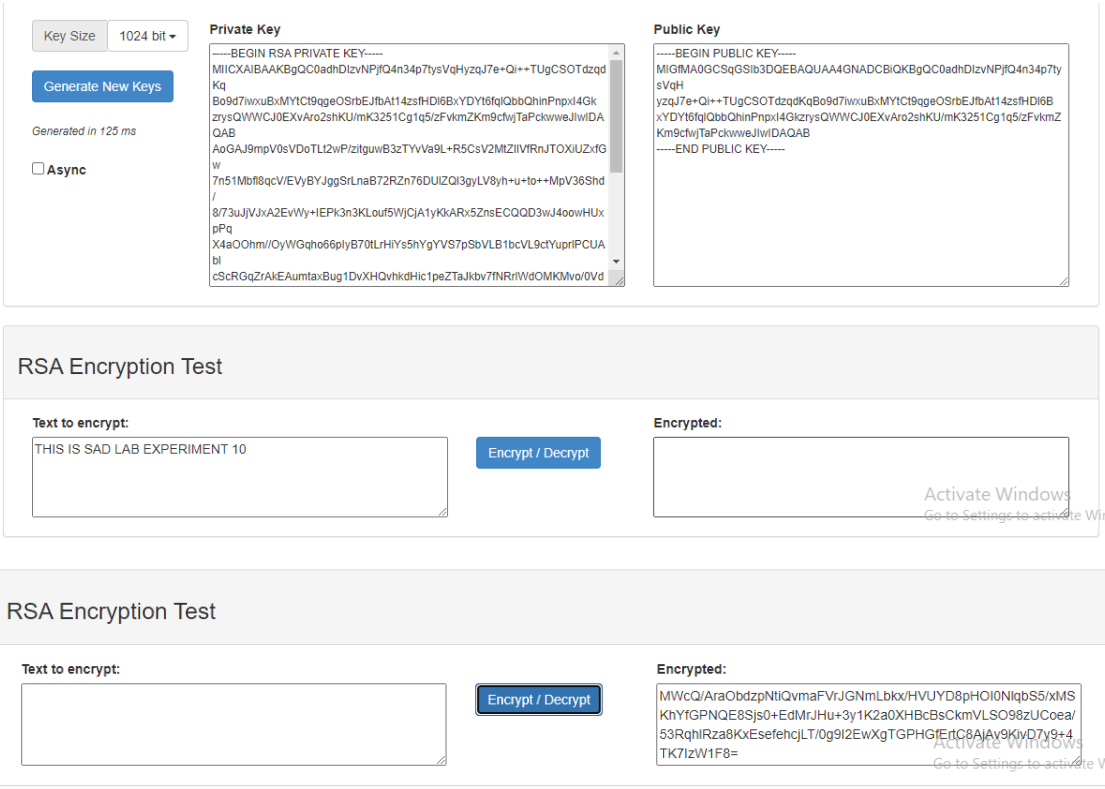

Alice
Parameters known by Alice:
m = HELLO BOB, $K = 10110010100110...$, $p = 7$, $p_{16} = 00000111$, $x = 01001000010001...$, $y = 00101000100001...$
Step 6/7
Bob uses the key K and the AES decryption function D_K to decrypt the block y.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10110010100110...$, $y = 00101000100001...$
$x = 01001000010001...$
Decrypts the ciphertext blocks y.
$x = E_K(y)$
$= 010010000010001...$


Alice
Parameters known by Alice:
m = HELLO BOB, $K = 10110010100110...$, $p = 7$, $p_{16} = 00000111$, $x = 01001000010001...$, $y = 00101000100001...$
Step 7/7
Bob converts the first byte $b_1 = 01001000$ in the block x to its integer representation 72 and then to its letter representation H.
Then he converts the rest of the bytes in the block x.
Because the decimal value of the last byte $p_{16} = 00000111$ in the last block x_1 is $p = 7$ and between 1 and 15, Bob know that the padding byte p_{16} has been added 7 times at the end of the last block x_1.
Previous step
Next step
Try again
Bob
Parameters known by Bob:
$K = 10110010100110...$, $y = 00101000100001...$
$x = 01001000010001...$, $p_{16} = 00000111$, $p = 7$, m = HELLO BOB
$p_{16} = 00000111 \Rightarrow p = 7$
$x = 0100100001000101... \Rightarrow$ HELLO BOB7777777
m = HELLO BOB

RSA: RSA is a public-key cryptosystem, one of the oldest, that is widely used for secure data transmission. The RSA public key is used for key encryption of DES or AES DATA keys and the RSA private key for key recovery.

Link: https://travistidwell.com/jsencrypt/demo/

Online RSA Key Generator:



Conclusion: Cryptography involves the practice of encrypting and decrypting information to ensure it is kept private and secure from unintended parties. We performed Encryption of data using Online Cryptographic platforms. Thus we successfully implemented symmetric and asymmetric cryptography, that is AES/DES and RSA Algorithm.