**=============THE FOLLOWING GIVEN TO THE PARTICIPANTS=============**

## **The Alien Oracle**

## **Challenge Category:** Crypto

## **Challenge Description:**

*Once upon a time, you are stuck in an alien planet,*

*with your only means to return home hidden within the alien message:*

|  |
| --- |
|  |
| *b'P\xe2s\x14&o\xda\x04\x124\xb3\xf2\x8d\x97\xeaG\xa4H\n5}m\t.\xe1\xaf\xa7\x0f\xc3\x8d8\x04!\x06AP\x13\xa8[\x01#\xcao\xb9\xc6\xbf^\x97\*A\x92j)MfmEL\xa5\xef\xbc.(\xfe\xc2\xf1\xb3e@Z\x91=\x19\xba\xdc\xbb\x1a\x01Eu'* |
|  |

*You have only three clues:*

* *The message comes in 16-symbol blocks, and the answer is hidden in the centre block of the message.*
* *The message originated from the Cryogenic-Bezier-Curve and not the primitive version, Ectoplasmic-Cuckoo-Boogaloo.*
* *The message is padded with Planetary-Kebab-Cosmic-Solomon-7 and obviously protected from barbaric-mass-times-acceleration attacks.*

*Fortunately, there is an alien oracle that lives in the planet, but it only speaks in alien tongue.*

*It only will say "ree" if the padding of your alien message is valid, and "yon" if the padding is not.*

*A means of communicating with the alien oracle has been provided in client-challenge.py.*

*You have only 75 hours before nightfall in this alien planet, where you will freeze over in its subzero temperatures.*

*Will you be able to return home?*

**Challenge Source Files for participants:**

client-challenge.py (skeleton code for attack)

**Challenge Server running in LEET Lab:**

l2server.py (Code for running the server, **not given** to participants)

**=============THE FOLLOWING IS FOR PROF NILS EYES ONLY=============**

## **Team Reyon**

Members:

* Kenneth ,1001092
* Weihan ,1001003
* Wei Sheng ,1000978
* Lim Zhi Han Ryan ,1000985

Challenge Name: The Alien Oracle

Category: Crypto

Topics: Chain Block Cipher (CBC) & Padding Oracle Attack

## **Summary of Challenge:**

In this CTF, we will provide a ciphertext that attackers need to decrypt to obtain the flag, and a server that acts as an oracle which will take in a ciphertext, and outputs a positive result if the padding of the encrypted message is correct, and a negative result otherwise. The padding we are using will be PKCS7 and in the form of the following:

|  |  |  |  |
| --- | --- | --- | --- |
| … | … | … | 0x01 |
| … | … | 0x02 | 0x02 |
| … | 0x03 | 0x03 | 0x03 |

And so on…

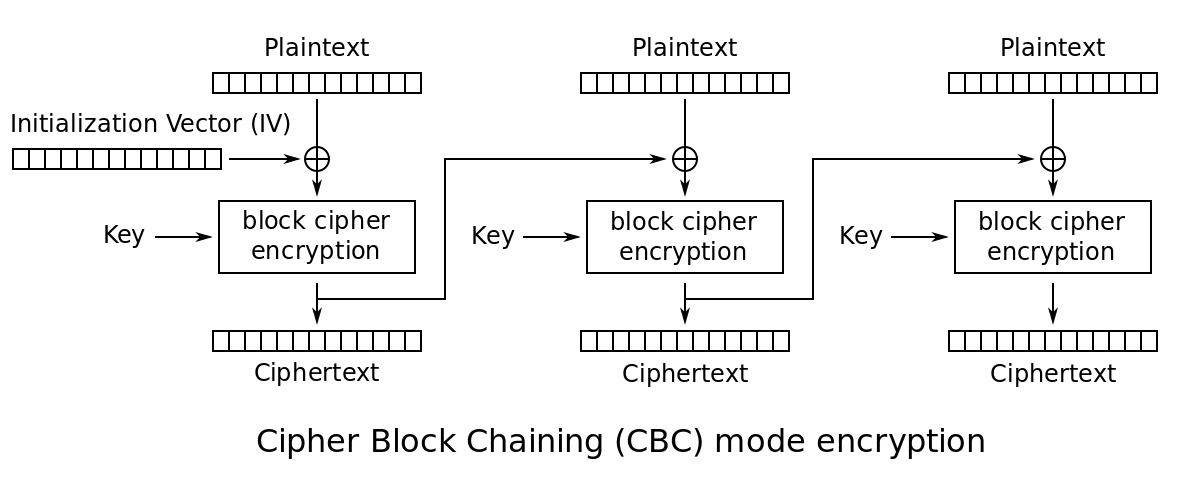
The objective of the challenge is to have attackers understand how CBC works and how the leakage of information (whether the padding of an encrypted message is correct) can lead to the confidentiality of the ciphertext being compromised.

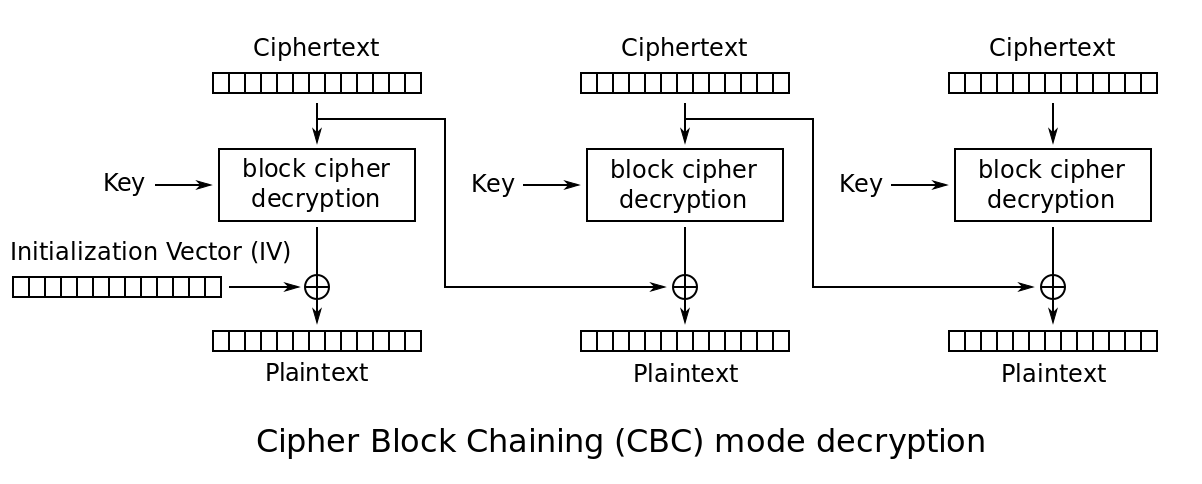
Users will perform a padding oracle attack on our system to obtain the flag. Details of an attacker’s approach and likely pseudocode are below.

## 

**Summary of Chain Block Cipher (CBC):**

In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all the plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.





## 

## **Summary of Attack:**

We can pass any ciphertext to the oracle, and the oracle will reply whether the decrypted ciphertext is a plaintext with a valid padding or not. We can use this padding information to exploit CBC.

To get the last byte of P2, we need to craft a malicious payload such that the decrypted message has a valid padding ending with 0x01.

We craft the payload C1’ + C2, where C1’ is a cipher block specially crafted by us, and C2 is the ciphertext block we are trying to decrypt.

We choose C1’[0 to 15] to be C1[0 to 15], and C1’[16] to be C1[16]^ guess^0x01.

If our guess is correct, during decryption for the last byte of plaintext,

P2[16] = I2[16] ^ C1[16] ^ guess ^ 0x01 = 0x01, as I2[16] ^ C1[16] ^ guess will be cancelled out.

This will result in a plaintext with a valid padding ending with 0x01. When C1’ + C2 is sent to the oracle, he will reply that the decrypted message has a correct padding. This is where we know the last byte of P2 is our guess.

However, if the oracle replies with a wrong padding, we know that we have made a wrong guess as the padding is wrong. We will then vary our guess from 0 to 255, until we receive a positive response from the oracle. The guess which gives a positive response in the loop will be the last byte of the P2. This correctly guessed byte is stored as b1.

To guess the second last byte of the plaintext, we need to make the decrypted plaintext padding 0x02 0x02.

Again, we craft a message C1’ + C2, where C1’ is,

C1’ = C1[0 to 14] + C1[15] ^ guess ^ 0x02 + C1[16] ^ b1 ^ 0x02

This message C1’ + C2 is passed to the oracle to be checked for the correct padding.

The last byte of the decrypted plaintext will always be decrypted to 0x02 as

I2[16] ^ C1[16] ^ b1 ^ 0x02 = 0x02, as I2[16] ^ C1[16] ^ b1 will cancel out.

We now need to change the second last byte of the P2 to 0x02.

Similarly, we loop our guess from a range of 0 to 255,

If our guess is correct, I2[15] ^ C1[15] ^ guess ^ 0x02 = 0x02, as I2[15] ^ C1[15] ^ guess will be cancelled out.

This will result in the oracle replying with a positive response as our message has a valid padding of 0x02 0x02, where this new guess is our second last byte of P2.

This is repeated until all the bytes of the plaintext is found.

**Note:** The first block of the plaintext cannot be decrypted as we did not provide the Initialisation Vector to the participants.

**Complexity:**

Since there are 256 possibilities per byte of ciphertext, enumerating all possibilities to find the intermediate and subsequently plaintext will take on average 128 iterations per byte, and given 16 bytes per block is will take 2048 iterations per block, which should not take very long. This attack essentially negates the need to find out what the key is or attacking the encryption algorithm(AES).

**Working Solution**:

* solution-client.py