CTF Challenge Group: 2020Fireteam

Challenge Name: Two cats in one house

Background:

Tom and Jerry –Two cats (Tom and Butch) are living in the same house. Their fed up host threatens to get rid of one of her lazy cats when she's tired of dealing with all the mice problems.

To deal with Jerry together, they communicated using AES-CBC mode so as to come up with a plan. Jerry found out the files they left in the computer and wanted to decrypt the messages between them.

Handling two cats is too difficult for Jerry without knowing their plan.

If Jerry decrypt the message successfully, he can play tricks when they are chasing him and sow discord between them.

If so, the host will end up finding her cats wrestling with each other without solving the mice issue and Jerry will be able to escape from their chase.

Tom and Butch initiate their communication using RSA protocol with a pre-shared public key. Tom has the public key of the RSA key (The public key can be found here), and Butch has the private key of the RSA.

In order to remember the key more easily, Butch transforms his private key into English[1] (which is a couple of words). He still cannot remember such a long English version of private key. So he came up with an idea. He encrypted the English version of the private key using a substitution cipher [2], To prevent from making careless mistakes when decrypting, he also calculated the MD5 sum [3] of the original English version of private key. Then he wrote the Encrypted private key and the MD5 sum down on a paper and put it into his pocket. Jerry accidentally finds the paper and copies everything down. (The encrypted private key can be found here) **(The MD5 sum on the paper is fbad4a66f5934fa8f4784f15f1bd7925)**

Tom initiates the communication by sharing an AES key (encrypted using PKCS1_OAEP) to Butch encrypted using the RSA public key (The message for sending the key can be found here).

After Butch received the key. Tom and Butch start to communicate using AES-CBC mode to discuss the plan.

Jerry wants to eavesdrop on Tom and Butch's communication. He already got the encrypted private key and the MD5 sum, so he wants to decrypt the message, get the session key and know the plan between Tom and Butch. Besides, he carefully records all the messages sent between Tom and Butch.

Moreover, Jerry knows that Tom and Butch always use the same IV[6] for AES-CBC, which is a hash of a simple word selected from a book (book).[4]

Additionally, Jerry also accidentally found the MAC of the password[5] the salt added to the MAC is two printable characters one character at the begin of the password, another character at the end of the password. MAC: (**34bedb439ebe86ac90e60b43f033dcd6**).

Now you are Jerry and you want to find the plan sent between Tom and Butch.
Please find the flag in the format "flag-{}"

Appendix:
[1]: The private key is transformed into english using:
Key_english = key_to_english(str(private_key.d).encode('utf-8'))
You can use **Crypto.Util.RFC1751.key_to_english(key) to recover the private_key**

[2]: The Substitution Cipher is a random mapping between capital letters only.

[3]: The list of words as a string, then the MD5 sum is calculated using:
MD5.new(data=private_key_english.encode("utf-8")).hexdigest()

[4]: The IV here is given by **MD5.new(data=password.encode()).digest()**

[5]: This hash is the hash of the original word with two different single-char salts, at the start and end of the original word. Both salts are characters from string.printable. The hash is defined as the **MD5.new(data=(salt1 + word + salt2).encode("utf-8")).hexdigest().**

[6]: IV= MD5.new(data=word.encode()).digest()

Frequency of letters:
('A', '10.83%'), ('B', '2.13%'), ('C', '4.02%'), ('D', '4.63%'), ('E', '11.50%'), ('F', '1.95%'), ('G', '2.68%'), ('H', '7.12%'), ('I', '2.98%'), ('J', '0.37%'), ('K', '1.64%'), ('L', '5.90%'), ('M', '4.32%'), ('N', '4.32%'), ('O', '8.03%'), ('P', '3.29%'), ('Q', '0.12%'), ('R', '6.76%'), ('S', '3.16%'), ('T', '3.59%'), ('U', '4.32%'), ('V', '0.73%'), ('W', '2.68%'), ('Y', '2.92%'), ('Z', '0.00%')

Links for origin Tom and Jerry episode:
Tom and Jerry – A mouse in the house
https://www.dailymotion.com/video/x7d1e98
Tom and Jerry- A mouse in the house Wikipedia
https://tomandjerry.fandom.com/wiki/A_Mouse_in_the_House