**Enter the CTF through this link:** [**http://flask-env.dy2nh6w2mr.ap-southeast-1.elasticbeanstalk.com**](http://flask-env.dy2nh6w2mr.ap-southeast-1.elasticbeanstalk.com)

**Part I: Shattered**

*Hash Value = “b7a875fc1ea228b9061041b7cec4bd3c52ab3ce3”*

Find the password to enter the website using the hash value given above.

**Part II: RSA**

*Ciphertext* ***(in binary)*** *= “110000101011001011110001111000100000010000101000110101010101000000111110011111010010001111100011000101010101000110011111011100000010111100100110010011011111100011101000011100101100010000000011110110101110101101011000100101100100101011”*

With only the public key (public\_key.pem) given and the knowledge that the encryption is using RSA. Get the plaintext from cipher text.

**Part III: AES key derivation**

*passwordSalt=b'\x7f\x8a\x91\xab\xc2\x0c\xe6\x8d\xc0\xd7\xba! \xd2\x80\xa1M'*

Using the pyaes and pbkdf2 libraries, password derived from part II and salt given, get the AES encryption key!

**Part III: Read the Bytes**

Using the text file given, analyse the byte distribution of each line.

Out of all the strings in the text file, there are 4 strings that will stand out.

**Part IV: AES Decryption (CTR Block mode)**

*IV=57116448576878005380785937564945681393249968307171981972 903895716101015138040*

Using the IV given and AES encryption key derived in part II, decrypt the 4 strings you singled out from the entire text file.

**Part V: Final Stage to Decipher**

*Ciphertext= “IYTNANDTLRTRSEEDSENRLIFOAPHLUISWSOTGLDSGAEIDSTANAPSVANTSNASH IRIELHTAINARIUATCAOHVENHAETAYSOAOFFAPRD”*

Using the decrypted text, decrypted the final cipher text!