Cheat sheet for using Cryptography library on Python 3.5

1. Encryption modes need keys as bytes

cipher = Cipher(algorithms.AES(aesKey), modes.ECB(), backend=backend)

aesKey has to be bytes

1. Encryption needs data in bytes as well

message = b'Try this for a change'

1. Output of decryption is in bytes

textOut = decryptor.update(ct) + decryptor.finalize() #output is in bytes

textOut is in bytes

1. Padding needs to be done manually else you’ll get an error

padder = padding.PKCS7(128).padder()  
padded\_data = padder.update(message) + padder.finalize()

If you don’t finalize the last block will be missing

Data must be in bytes.