# Simple AES Problem

Yasmin has intercepted email traffic between the Master and one of their agents. See if you can decrypt the message.

Master: Agent 4, execute instructions contained in the attached message MastersOrder1563.b64. As usual, the message is encrypted with AES in ECB mode and then Base64 encoded (The Master is too busy to deal with nonces and tags.) Use the 42nd entry in your book of keys.

Master: Agent 4, you have not executed my order. Why?

Agent 4: Uh, I can’t find my book of keys.

Master: You idiot! Look harder!

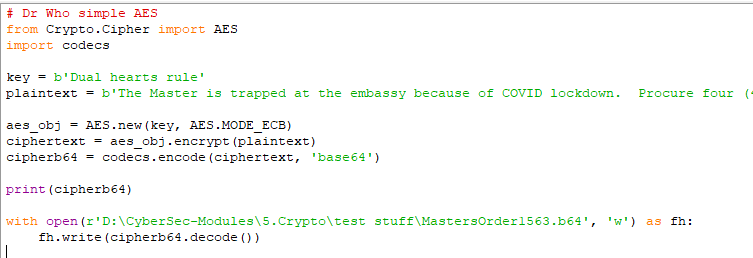
Agent 4: Sir, the book of keys was accidentally burned.

Master: Accidentally!? By whom!? Idiot! I’ll get you the key.

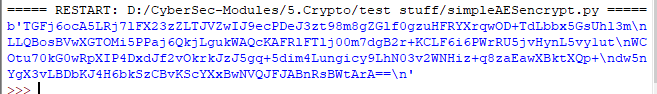
Master: Dual hearts rule

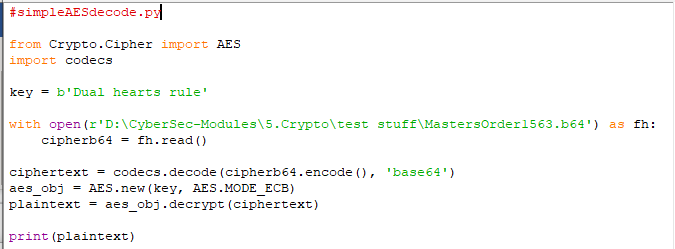
Plaintext

The Master is trapped at the embassy because of COVID lockdown. Procure four (4) bars of Ghirardelli chocolate, INTENSE DARK, 86% CACAO. Deliver them to The Master at the embassy. ( ineptminion, Idiot!7 )



b'TGFj6ocA5LRj7lFX23zZLTJVZwIJ9ecPDeJ3zt98m8gZGlf0gzuHFRYXrqwOD+TdLbbx5GsUhl3m\nLLQBosBVwXGTOMi5PPaj6QkjLgukWAQcKAFRlFTlj00m7dgB2r+KCLF6i6PWrRU5jvHynL5vy1ut\nWCOtu70kG0wRpXIP4DxdJf2vOkrkJzJ5gq+5dim4Lungicy9LhN03v2WNHiz+q8zaEawXBktXQp+\ndw5nYgX3vLBDbKJ4H6bkSzCBvKScYXxBwNVQJFJABnRsBWtArA==\n'





Hint 1: This should be almost identical to the AES.MODE\_ECB example in Crypto Homework 4.  
VGhpcyBzaG91bGQgYmUgYWxtb3N0IGlkZW50aWNhbCB0byB0aGUgQUVTLk1PREVfRUNCIGV4YW1wbGUgaW4gQ3J5cHRvIEhvbWV3b3JrIDQu

Hint 2: If you are pasting the base64 into your Python, make sure it is one long string with no carriage returns/line feeds.  
SWYgeW91IGFyZSBwYXN0aW5nIHRoZSBiYXNlNjQgaW50byB5b3VyIFB5dGhvbiwgbWFrZSBzdXJlIGl0IGlzIG9uZSBsb25nIHN0cmluZyB3aXRoIG5vIGNhcnJpYWdlIHJldHVybnMvbGluZSBmZWVkcy4=

Hint 3: codecs and AES both want input of type bytes. Use somestring.encode() to change string to bytes. Use somebytes.decode() to change bytes to string.  
Y29kZWNzIGFuZCBBRVMgYm90aCB3YW50IGlucHV0IG9mIHR5cGUgYnl0ZXMuICBVc2Ugc29tZXN0cmluZy5lbmNvZGUoKSB0byBjaGFuZ2Ugc3RyaW5nIHRvIGJ5dGVzLiAgVXNlIHNvbWVieXRlcy5kZWNvZGUoKSB0byBjaGFuZ2UgYnl0ZXMgdG8gc3RyaW5nLg==