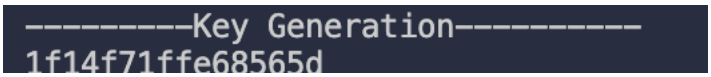
Chelsea Gantt
10.7.20
AES Report

OS – Mac
Language - Python 3.8.5

I used VSCode to build my project. In order to have it run, go into the src folder and select the app.py file. If you are in VSCode, you will need to select run at the top of your screen and click the dropdown either run w/ or w/o debugging. From there the program should run as desired. It will automatically run each function, with the last one being decryption. All of my txt files are in the data folder.

KeyGen Function

The keyGen() uses the *binascii* import to create a random hex variable, using urandom(), then decoding it to UTF-8. From there the key is written to key.txt file and printed to the console



Encryption Function

The encryption () reads from the key.txt and plaintext.txt to get the values in the AES encryption. From there we generate a random initialization vector, which is generated in the same fashion the secret key was created. In order to do the encryption, I leverage the pycrypto library. During the encryption I multiply the plaintext by 16 to ensure we have 16 byte sized boxes. This is then converted to hex and written to the ciphertext.txt file and printed in the console.

Decryption Function

The decryption() reads from the key.txt, iv.txt, and ciphertext.txt to get the values for the AES decryption. Prior to decryption I unhexlify the ciphertext, once the decryption is completed, I revert the length back to its original, then decode it so it does not have the leading 'b' prefix. Thereafter the final result is printed to the console and written to the result.txt.

Different Encryption Modes

Upon reviewing each of the ciphertexts for CBC & EBC Mode I wasn't able to find any obvious differences other than the fact that it was two different ciphertexts generated.

I did notice on decryption I did not have to decode the results to remove the leading 'b' prefix. It was already done in the encryption.

```
----------Encryption CBC Mode----------
059a1dc9a84d18bf69567386d829acb326087ca3e181c0d32934fa305f217761cc7e9ab0ff15097744c7d8d8321be9967f427fec279b8171999514b24d96eee6617aa3b2ea9d5ce7a7b050b0092b28a1248ef7f54364f6c4fbbf8176c0337d0b59c7e3ba8ff8b59bc5
8290c214dd2aab09ba178161e03806966c61497eccead544564b77c689e9da0bd5e8c064e1c36f752f7e74da018db13779a3dcacaeee69c1abf5813955576f4007b62ecec ffbe3dc40dbc81c712acb8ef4b63f5675b8200ca764122924e671d5a61fbe9a0f86d27fc68b
1f6a9fa62cb236d30f78b3ce7928de422bf1ccee71cc964e283c8c83453f19494a38119785aefc61fadbbf819d664872a13d983a675ab03d2225149e349f6e9c9c7dd4fa8542cae0cb54916a69af0dbc07e4db2b45f25fba1f97d6cb89d66ee92a530171104db20f65
f137f2f2e261b721c105dafac22c09e0c436c6e074
----------Encryption ECB Mode----------
4fce73213303c6c9ecd57555a659dfbaa021e1bfedd0a3fab98b5f032c979c38e46437c75a9f3ad4a51b88111c2193c9e0f898c7764b3b6cefd3e48f73ca7ae1e8170c32dd2880d6b69049b225172f31ffe049ce1d6b3a2eff359fe4586888b0376d3fe1b26d3faf7e
b75feefabe5844e3682d6369293642e3a3b1807f61c5b3b2cd58dc8916d0e956c2e2ec02dd2a776e03da4c4db9fb8475e85c9780d75ff8bfff2b6c6f9fd46b1dddfdd71c74162395500e21381c69414ec23472e908ad7ddda7c8e3e924bda08212fd294a1d4cb7c337
490c4b5584741c5148a0ebb313e4df62120554c46766ab61147fca8bafd0608a97e3707ce4438b87e5e07096c57232dba81034355d261b6f8374c3a7bc9e0b9667d69bdedf5c7703f88c794f675914d04cfcd5693a127fac388eafdbead8c9089635dbe792256f3621
4cc0e4b409431a9e62c78d0428be1d641132ca380c
chelseaaliece@aliece aes.m08812601 %  cd "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601" ; /usr/bin/env /usr/local/bin/python3 /Users/chelseaaliece/.vscode/extensions/ms-python.python-202
0.9.114305/pythonFiles/lib/python/debugpy/launcher 55791 -- "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601/src/app.py"
----------Encryption CBC Mode----------
ea60ba0a30adf77c656427caa29bf0eb319cf05093325bf1e0ae962d105c24ad13521c2f965276a1fbc576a49e11a7dcba536aaf9f83154c046adea08063a48cb7586fa97aaf312f1f0d058ed18fffdf4fd03b52fd60f8fb3b5b65aca2961f49339734bb6123c23f3a
ba3be3e1524bf9ce20f6ae09159a57b06dd2d3a65da545d6c1b0e80fbdef9eb6402cbacffc1434ac4ef2fa0a7e240c72688fa1a5e96349acb60612166cc5a8bbe9c2342a599c2bb126b6a3c6f1e9a4149d6797416573123ffd2d53ce7daad4d53a76f896237a0b4eda
bcd8400b357cbe5be738885e25a05c312cdb4cc140f3c7a0ae63859a96f26a6fac078c8b8332586b002840876139f925d202e71459a1bf4bf4322fc239a8a129c00a5cbe126d2e3e7c9800bb5991e1370aafcf966a79360a83e6bc2cd608f7b02d851cbbae77a04843
a469a3b5616e769aa03e42114beee54853b56a7b8e
----------Encryption ECB Mode----------
4fce73213303c6c9ecd57555a659dfbaa021e1bfedd0a3fab98b5f032c979c38e46437c75a9f3ad4a51b88111c2193c9e0f898c7764b3b6cefd3e48f73ca7ae1e8170c32dd2880d6b69049b225172f31ffe049ce1d6b3a2eff359fe4586888b0376d3fe1b26d3faf7e
b75feefabe5844e3682d6369293642e3a3b1807f61c5b3b2cd58dc8916d0e956c2e2ec02dd2a776e03da4c4db9fb8475e85c9780d75ff8bfff2b6c6f9fd46b1dddfdd71c74162395500e21381c69414ec23472e908ad7ddda7c8e3e924bda08212fd294a1d4cb7c337
490c4b5584741c5148a0ebb313e4df62120554c46766ab61147fca8bafd0608a97e3707ce4438b87e5e07096c57232dba81034355d261b6f8374c3a7bc9e0b9667d69bdedf5c7703f88c794f675914d04cfcd5693a127fac388eafdbead8c9089635dbe792256f3621
4cc0e4b409431a9e62c78d0428be1d641132ca380c
chelseaaliece@aliece aes.m08812601 %  cd "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601" ; /usr/bin/env /usr/local/bin/python3 /Users/chelseaaliece/.vscode/extensions/ms-python.python-202
0.9.114305/pythonFiles/lib/python/debugpy/launcher 55795 -- "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601/src/app.py"
----------Encryption CBC Mode----------
e874475e8d2bab99324010343ec6233eca8375d84df566347929d2938ade7464c3fde6afa8311766ff9a5c02a0569845ce0bfe3f5733a337676640ea8335446c5721cd7627d4c9c278acdce7a03af81ad47d50fb9690b12554f69058df32dbb12ba7ab71b4f58d1baf
a2d550c1aecb1926b0e7fd5fec7ae759a741f2e34a7f8a58743cbce13e721f7ae2b5469669baa31ed5b64dab5e40f4439ec46ab02a6e1ad693478ae6325ffe4eccd1991b8a8e5ed8a4251b4b240b70c0ccc435458f1db6aa80f64846a9ea74326519b48b768e68cdd2
59c1604674bcc206b99df4dac5ba3af5c03211b788a6ace5bc546c962f3776219e36ccdb70810cf9858d478c4c70eec042bb147c2d712992ba2aac69cb7eaa45659118313b75ef4a42a4ea2503939790c355a57353e93b41a6cb332cbbac62415e6853869aef8d9eea
810117c54827652aea771ca4a98c961fa3e0fb834b
----------Encryption ECB Mode----------
4fce73213303c6c9ecd57555a659dfbaa021e1bfedd0a3fab98b5f032c979c38e46437c75a9f3ad4a51b88111c2193c9e0f898c7764b3b6cefd3e48f73ca7ae1e8170c32dd2880d6b69049b225172f31ffe049ce1d6b3a2eff359fe4586888b0376d3fe1b26d3faf7e
b75feefabe5844e3682d6369293642e3a3b1807f61c5b3b2cd58dc8916d0e956c2e2ec02dd2a776e03da4c4db9fb8475e85c9780d75ff8bfff2b6c6f9fd46b1dddfdd71c74162395500e21381c69414ec23472e908ad7ddda7c8e3e924bda08212fd294a1d4cb7c337
490c4b5584741c5148a0ebb313e4df62120554c46766ab61147fca8bafd0608a97e3707ce4438b87e5e07096c57232dba81034355d261b6f8374c3a7bc9e0b9667d69bdedf5c7703f88c794f675914d04cfcd5693a127fac388eafdbead8c9089635dbe792256f3621
4cc0e4b409431a9e62c78d0428be1d641132ca380c
chelseaaliece@aliece aes.m08812601 %  cd "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601" ; /usr/bin/env /usr/local/bin/python3 /Users/chelseaaliece/.vscode/extensions/ms-python.python-202
0.9.114305/pythonFiles/lib/python/debugpy/launcher 55799 -- "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601/src/app.py"
----------Encryption CBC Mode----------
7cccb4e38ccaf78ca119dda2f5a9a24069f378e5102d3ab6157121f7b5ec001ba3ba3d268dbd175f8b5046b03e74af406bcc43807b9ced449a2c47da96d647c927d83465afd2ad303c536c0ab0f4833fb099a9a1314972edec098080d0b12590450eccc50532aacde
45c8836394b0c4a807cf57929e4c5e50b2ec25e3d4dfb55a077f35e0f4fb82d4887d6aa2dbc49201c376d1bdec0422be78b72203f99eb0137aaac1d7906e18d4f724372ca43c80e72dc010f9e145e7ff9be8396739be9e520cfe0a950a43d9ebf64ceb86196a535a17
84a2222e4fcdfedf71ff87d575c27624ece75e1082168504b746d94488c0f1d78b133efae693f546fdf68234813bfcf5de5ed60b30168676169a760a914577f881cde6fcd7f5ad43c0d698aed3032b38e9419126b7f3b8dd2c6e05f36dbf752995bcf353ee83eff22
2724c2d560e7af298009dbf855b05d088466f1c00f
----------Encryption ECB Mode----------
4fce73213303c6c9ecd57555a659dfbaa021e1bfedd0a3fab98b5f032c979c38e46437c75a9f3ad4a51b88111c2193c9e0f898c7764b3b6cefd3e48f73ca7ae1e8170c32dd2880d6b69049b225172f31ffe049ce1d6b3a2eff359fe4586888b0376d3fe1b26d3faf7e
b75feefabe5844e3682d6369293642e3a3b1807f61c5b3b2cd58dc8916d0e956c2e2ec02dd2a776e03da4c4db9fb8475e85c9780d75ff8bfff2b6c6f9fd46b1dddfdd71c74162395500e21381c69414ec23472e908ad7ddda7c8e3e924bda08212fd294a1d4cb7c337
490c4b5584741c5148a0ebb313e4df62120554c46766ab61147fca8bafd0608a97e3707ce4438b87e5e07096c57232dba81034355d261b6f8374c3a7bc9e0b9667d69bdedf5c7703f88c794f675914d04cfcd5693a127fac388eafdbead8c9089635dbe792256f3621
4cc0e4b409431a9e62c78d0428be1d641132ca380c
chelseaaliece@aliece aes.m08812601 %  cd "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601" ; /usr/bin/env /usr/local/bin/python3 /Users/chelseaaliece/.vscode/extensions/ms-python.python-202
0.9.114305/pythonFiles/lib/python/debugpy/launcher 55804 -- "/Users/chelseaaliece/Documents/Data Security & Privacy/aes.m08812601/src/app.py"
----------Encryption CBC Mode----------
9554eb042cd09e837a6387b7e9ee031206632b122e2aec5f8edcc3204d8a81d01eb9d0d75bf8488bac2b649e2d4f7e0da2297db64ff7c81cf40fd846b97b3e447ef0de013da3698c6f8f12a898509e7ea2babf9b19577a62c237a5fb1d7c7c907bfa658030cc08e12
678e3fc162a038c01b0282laadd11e39a4ad2730eaac6494b17851912bdf9694aae42870a3d2390eb2236ed3f326977bfe1326c1fdd385fc645014d5755c807e31aeec1c5457620c941f428e46afbccbd33ab59df9a4e453e8be8eea40bbf0e78cb1b044988bf08672
eaee98384b6d988d9d0c267beccdbe73e7b4d398a7bfdeeaa3a4fe0822611d4f02f78515a4e50179a9cc4a7fa892aee9bed9bf8575adfa1e874b078407fb6dc20fcba00aa5fb0921495ea8d30fc46a123069a949bd2a4ea3d57fd9ac022642c775af80f9f33f2f6382
55b417cdf96982fef4f6afb60d259ac7c6fa0faaed
----------Encryption ECB Mode----------
4fce73213303c6c9ecd57555a659dfbaa021e1bfedd0a3fab98b5f032c979c38e46437c75a9f3ad4a51b88111c2193c9e0f898c7764b3b6cefd3e48f73ca7ae1e8170c32dd2880d6b69049b225172f31ffe049ce1d6b3a2eff359fe4586888b0376d3fe1b26d3faf7e
b75feefabe5844e3682d6369293642e3a3b1807f61c5b3b2cd58dc8916d0e956c2e2ec02dd2a776e03da4c4db9fb8475e85c9780d75ff8bfff2b6c6f9fd46b1dddfdd71c74162395500e21381c69414ec23472e908ad7ddda7c8e3e924bda08212fd294a1d4cb7c337
490c4b5584741c5148a0ebb313e4df62120554c46766ab61147fca8bafd0608a97e3707ce4438b87e5e07096c57232dba81034355d261b6f8374c3a7bc9e0b9667d69bdedf5c7703f88c794f675914d04cfcd5693a127fac388eafdbead8c9089635dbe792256f3621
4cc0e4b409431a9e62c78d0428be1d641132ca380c
```

Average time for Encryption to run: 0.0012 Seconds
Average time for Decryption to run: 0.0006 Seconds

Calculated using the time function. Available but commented out in code