CS 490: Embedded Systems Security
Homework #01 Report
Dylan Williams

For this assignment, I developed a Python 2.7 implementation of the Rijndael encryption scheme (AES). The entire implementation and all unit tests and AES vector verification is contained within the single file *aes.py*. In its current implementation, all unit tests are ran to ensure each component of the encryption scheme produces the correct output. This is important as a single misplaced byte will result in either a weakened encrypted ciphertext or in the inability to retrieve the plaintext afterwards.

The final test "*Cipher*" actually tests the complete implementation by feeding various key/plaintext pairs through the application and comparing them to established, expected ciphertexts as provided in the AES Algorithm Validation Suite documentation.[1] If the *Cipher* test passes, it signifies that the encryption implementation is creating the correct ciphertext given the key/plaintext pair. The test vector inputs and outputs have been attached to this report.

Also attached to this report is the output from the *pylint* static code analysis tool when ran against *aes.py*. The majority of the warnings throughout are merely stylistic as I opted to follow the code style of the official AES pseudocode[2] rather than the established Python coding style. However, such warnings as produced by static code analysis tools can be helpful in discovering possible side-channel attacks against a particular implementation of an encryption scheme such as memory leaks, timing attacks, and other attack vectors.

[1] http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf
[2] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

AES NIST Validation Vectors and Implementation Ciphertext

key =
[0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f,
0x10,0x11,0x12,0x13,0x14,0x15,0x16,0x17,0x18,0x19,0x1a,0x1b,0x1c,0x1d,0x1e,0x1f]
plaintext =
[0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,0x88,0x99,0xaa,0xbb,0xcc,0xdd,0xee,0xff]
ciphertext =
[0x8e,0xa2,0xb7,0xca,0x51,0x67,0x45,0xbf,0xea,0xfc,0x49,0x90,0x4b,0x49,0x60,0x89]

key =
[0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00]
plaintext =
[0x01,0x47,0x30,0xf8,0x0a,0xc6,0x25,0xfe,0x84,0xf0,0x26,0xc6,0x0b,0xfd,0x54,0x7d]
ciphertext =
[0x5c,0x9d,0x84,0x4e,0xd4,0x6f,0x98,0x85,0x08,0x5e,0x5d,0x6a,0x4f,0x94,0xc7,0xd7]

key = same as above
plaintext =
[0x0b,0x24,0xaf,0x36,0x19,0x3c,0xe4,0x66,0x5f,0x28,0x25,0xd7,0xb4,0x74,0x9c,0x98]
ciphertext =
[0xa9,0xff,0x75,0xbd,0x7c,0xf6,0x61,0x3d,0x37,0x31,0xc7,0x7c,0x3b,0x6d,0x0c,0x04]

key = same as above
plaintext =
[0x76,0x1c,0x1f,0xe4,0x1a,0x18,0xac,0xf2,0x0d,0x24,0x16,0x50,0x61,0x1d,0x90,0xf1]
ciphertext=
[0x62,0x3a,0x52,0xfc,0xea,0x5d,0x44,0x3e,0x48,0xd9,0x18,0x1a,0xb3,0x2c,0x74,0x21]

key = same as above
plaintext =
[0x8a,0x56,0x07,0x69,0xd6,0x05,0x86,0x8a,0xd8,0x0d,0x81,0x9b,0xdb,0xa0,0x37,0x71]
ciphertext=
[0x38,0xf2,0xc7,0xae,0x10,0x61,0x24,0x15,0xd2,0x7c,0xa1,0x90,0xd2,0x7d,0xa8,0xb4]

key = same as above
plaintext =
[0x91,0xfb,0xef,0x2d,0x15,0xa9,0x78,0x16,0x06,0x0b,0xee,0x1f,0xea,0xa4,0x9a,0xfe]
ciphertext=
[0x1b,0xc7,0x04,0xf1,0xbc,0xe1,0x35,0xce,0xb8,0x10,0x34,0x1b,0x21,0x6d,0x7a,0xbe]

```
Report
======
238 statements analysed.

Statistics by type
------------------

+---------+-------+-----------+-----------+------------+---------+
|type     |number |old number |difference |%documented |%badname |
+=========+=======+===========+===========+============+=========+
|module   |1      |1          |=          |0.00        |0.00     |
+---------+-------+-----------+-----------+------------+---------+
|class    |0      |0          |=          |0           |0        |
+---------+-------+-----------+-----------+------------+---------+
|method   |0      |0          |=          |0           |0        |
+---------+-------+-----------+-----------+------------+---------+
|function |23     |23         |=          |0.00        |100.00   |
+---------+-------+-----------+-----------+------------+---------+



Messages by category
--------------------

+-----------+-------+---------+-----------+
|type       |number |previous |difference |
+===========+=======+=========+===========+
|convention |255    |255      |=          |
+-----------+-------+---------+-----------+
|refactor   |2      |2        |=          |
+-----------+-------+---------+-----------+
|warning    |3      |3        |=          |
+-----------+-------+---------+-----------+
|error      |0      |0        |=          |
+-----------+-------+---------+-----------+



Messages
--------

+--------------------+------------+
|message id          |occurrences |
+====================+============+
|bad-whitespace      |142         |
+--------------------+------------+
|invalid-name        |41          |
+--------------------+------------+
|line-too-long       |26          |
+--------------------+------------+
|missing-docstring   |24          |
+--------------------+------------+
|multiple-statements |18          |
+--------------------+------------+
|superfluous-parens  |4           |
+--------------------+------------+
|unused-variable     |2           |
+--------------------+------------+
|too-many-statements |1           |
+--------------------+------------+
|too-many-branches   |1           |
+--------------------+------------+
|redefined-builtin   |1           |
+--------------------+------------+




Global evaluation
-----------------
Your code has been rated at -0.92/10 (previous run: -0.92/10, +0.00)

Duplication
-----------

+-------------------------+------+---------+-----------+
|                         |now   |previous |difference |
+=========================+======+=========+===========+
|nb duplicated lines      |0     |0        |=          |
+-------------------------+------+---------+-----------+
|percent duplicated lines |0.000 |0.000    |=          |
+-------------------------+------+---------+-----------+



Raw metrics
-----------

+----------+-------+------+---------+-----------+
|type      |number |%     |previous |difference |
+==========+=======+======+=========+===========+
|code      |283    |97.25 |283      |=          |
+----------+-------+------+---------+-----------+
|docstring |0      |0.00  |0        |=          |
+----------+-------+------+---------+-----------+
|comment   |5      |1.72  |5        |=          |
+----------+-------+------+---------+-----------+
|empty     |3      |1.03  |3        |=          |
+----------+-------+------+---------+-----------+
```