The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)

November 15, 2002

Lawrence E. Bassham III

National Institute of Standards and Technology
Information Technology Laboratory
Computer Security Division

Table of Contents

1 Introduction

This document specifies the procedures involved in validating implementations of the Advanced Encryption Standard (AES) algorithm in FIPS 197 : *Advanced Encryption Standard* [1]. The AESAVS is designed to perform automated testing on Implementations Under Test (IUTs). This publication provides the basic design and configuration of the AESAVS. It includes the specifications for the three categories of tests that make up the AESAVS, i.e., the Known Answer Test (KAT), the Multi-block Message Test (MMT), and the Monte Carlo Test (MCT). The requirements and administrative procedures specific to those seeking formal validation of an implementation of the Advanced Encryption Standard algorithm are presented. The requirements described include the specific protocols for communication between the IUT and the AESAVS, the types of tests that the IUT must pass for formal validation, and general instructions for accessing and interfacing with the AESAVS. Several appendices with tables of KAT values are also provided.

2 Scope

This document specifies the tests required to validate IUTs for conformance to the AES algorithm as specified in FIPS 197: *Advanced Encryption Standard*. When applied to IUTs that implement the AES algorithm, the AESAVS provides testing to determine the correctness of the algorithm implementation. In addition to determining conformance, the AESAVS is structured to detect implementation flaws including pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the AES algorithm implementation.

3 Conformance

The successful completion of the tests contained within the AESAVS is required to claim conformance to the Advanced Encryption Standard as specified in FIPS 197: *Advanced Encryption Standard*. Testing for the cryptographic module in which AES is implemented is defined in FIPS 140-2: *Security Requirements for Cryptographic Modules* [2].

4 Organization

Section 5 outlines the design of the AESAVS. Section 6 provides an overview of the tests that make up the AESAVS. Appendices A through E provide tables of sample values for the three types of tests that comprise the AESAVS.

5 Design Philosophy Of The AESAVS

The AESAVS is designed to test conformance to FIPS197, *Advanced Encryption Standard*, rather than provide a measure of a product's security. The validation tests are designed to assist in the detection of accidental implementation errors, and are not designed to detect intentional attempts to misrepresent conformance. Thus, validation should not be interpreted as an evaluation or endorsement of overall product security. The AESAVS has the following design philosophy:

1. The AESAVS is designed to allow the testing of an IUT at locations remote to the AESAVS. The AESAVS and the IUT communicate data via *REQUEST* and *RESPONSE* files.
2. The testing performed within the AESAVS utilizes statistical sampling (i.e., only a small number of the possible cases are tested); hence, the successful validation of a device does not imply 100% conformance with the standard.

6 The AESAVS Tests Description

The AESVS is designed to test the following Modes of Operation:

- ECB
- CBC
- OFB
- CFB1 (CFB where the length of the data segment is 1 bit, s=1)
- CFB8 (CFB where the length of the data segment is 8 bits, s=8)
- CFB128 (CFB where the length of the data segment is 128 bits, s=128)
- Counter (Counter mode is tested by selecting the ECB mode)

For each mode implemented, selections are available for the key sizes (i.e., 128-bit, 192-bit, and 256-bit) supported as well as the ciphering direction (i.e., encryption and decryption). It is not necessary for every mode implemented to support the same key sizes and ciphering directions. For example, an implementation may support all three key sizes for CBC for both encryption and decryption, but only the 128-bit key size for CFB1 for decryption only.

Once configuration information has been provided, appropriate *REQUEST* files will be generated. *REQUEST* files are the means by which test data is communicated to the Implementation Under Test (IUT). The IUT is used to process the data in the *REQUEST* file, and the resulting data is placed in a *RESPONSE* file. The data in the *RESPONSE* file is then verified.

6.1 Configuration Information

To initiate the validation process of the AESAVS, a vendor submits an application to an accredited laboratory requesting the validation of their implementation of the algorithm

specified in FIPS 197, *Advanced Encryption Standard*. The vendor's implementation is referred to as the Implementation Under Test (IUT). The request for validation includes background information describing the IUT along with information needed by the AESAVS to perform the specific tests. More specifically, the request for validation should include:

1. Vendor Name;
2. Product Name;
3. Product Version;
4. Implementation in software, firmware, or hardware;
5. Processor and Operating System with which the IUT was tested if the IUT is implemented in software or firmware;
6. Brief description of the IUT or the product/product family in which the IUT is implemented by the vendor (2-3 sentences); and
7. Specific information about the IUT necessary to configure the tests:
   - a. The modes supported: ECB, CBC, CFB (1-bit, 8-bit, and/or 128-bit), OFB, and/or Counter;
   - b. The states supported: Encryption and/or Decryption; and
   - c. The key sizes supported: 128-bit, 192-bit, and/or 256-bit.

6.2 The Known Answer Tests

There are four types of Known Answer Test:

- GFSbox
- KeySbox
- Variable Key
- Variable Text

The *REQUEST* file for each of these KAT tests contains a series of data sets consisting of a key, an initialization vector (IV) (for all modes except ECB), and a plaintext for encryption (or a ciphertext for decryption). The following is a sample data set:

```
KEY = 00000000000000000000000000000000
IV = 00000000000000000000000000000000
PLAINTEXT = 6a84867cd77e12ad07ea1be895c53fa3
```

The *RESPONSE* file for the KAT tests contains the same data as the *REQUEST* file with the addition of the ciphertext for encryption (or plaintext for decryption). The following is a sample data set:

```
KEY = 00000000000000000000000000000000
IV = 00000000000000000000000000000000
PLAINTEXT = 6a84867cd77e12ad07ea1be895c53fa3
CIPHERTEXT = 732281c0a0aab8f7a54a0c67a0c45ecf
```

Appendices B through E contain the values for each of the four types of Known Answer Test.

6.3 The Multi-block Message Test

The Multi-block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which may require chaining of information from one block to the next. The test supplies the IUT with messages that are integral numbers of blocks in length. For ECB, CBC, OFB, and CFB128 the block length is 128 bits, for CFB1 the block length is 1 bit, and for CFB8 the block length is 8 bits. For each supported mode 10 messages are supplied with lengths of i * *blocklength*, where $1 \leq i \leq 10$.

The *REQUEST* file for the MMT test contains a series of data sets consisting of a key, an initialization vector (IV) (for all modes except ECB), and a plaintext for encryption (or a ciphertext for decryption). The following is a sample data set:

```
KEY = 4278b840fb44aaa757c1bf04acbe1a3e
IV = 57f02a5c5339daeb0a2908a06ac6393f
PLAINTEXT = 3c888bbbb1a8eb9f3e9b87acaad986c4
            66e2f7071c83083b8a557971918850e5
```

The *RESPONSE* file for the MMT test contains the same data as the *REQUEST* file with the addition of the ciphertext for encryption (or plaintext for decryption). The following is a sample data set:

```
KEY = 4278b840fb44aaa757c1bf04acbe1a3e
IV = 57f02a5c5339daeb0a2908a06ac6393f
PLAINTEXT = 3c888bbbb1a8eb9f3e9b87acaad986c4
            66e2f7071c83083b8a557971918850e5
CIPHERTEXT = 479c89ec14bc98994e62b2c705b5014e
             175bd7832e7e60a1e92aac568a861eb7
```

6.4 The Monte Carlo Test

Each Monte Carlo Test ciphers 100 pseudorandom texts. These texts are generated using the algorithm specified in the section below pertaining to the mode of operation being tested. For modes that use an IV, the IV is used at the beginning of each pseudorandom text. Within each text, values are chained as specified in the description of the modes of operation found in SP 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.*

The *REQUEST* file for the MCT test contains a set of pseudorandomly generated initial values for the Monte Carlo function described below. The initial values consist of a key, an IV (for all modes except ECB), and a plaintext for encryption (or a ciphertext for decryption). The following is a sample data set:

```
KEY = 9dc2c84a37850c11699818605f47958c
IV = 256953b2feab2a04ae0180d8335bbed6
PLAINTEXT = 2e586692e647f5028ec6fa47a55a2aab
```

The *RESPONSE* file for the MCT test contains a series of data sets consisting of a key, an IV (for all modes except ECB), a plaintext for encryption (or ciphertext for decryption), and a ciphertext for encryption (or a plaintext for decryption). The following is a sample data set:

```
KEY = 9dc2c84a37850c11699818605f47958c
IV = 256953b2feab2a04ae0180d8335bbed6
PLAINTEXT = 2e586692e647f5028ec6fa47a55a2aab
CIPHERTEXT = 1b1ebd1fc45ec43037fd4844241a437f
```

The following subsections contain pseudocode for encryption. The pseudocode for decryption can be obtained by replacing all PT's with CT's and all CT's with PT's.

6.4.1 Monte Carlo Test - ECB

REQUEST file:

```
KEY = 8d2e60365f17c7df1040d7501b4a7b5a
PLAINTEXT = 59b5088e6dadc3ad5f27a460872d5929
```

Monte Carlo Algorithm:

```
Key[0] = Key
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output PT[0]
     For j = 0 to 999
          CT[j] = AES(Key[i], PT[j])
          PT[j+1] = CT[j]
     Output CT[j]
     If ( keylen = 128 )
          Key[i+1] = Key[i] xor CT[j]
     If ( keylen = 192 )
          Key[i+1] = Key[i] xor (last 64-bits of
                     CT[j-1] || CT[j])
     If ( keylen = 256 )
          Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
```

```
PT[0] = CT[j]
```

The first three entries of the *RESPONSE* file are:

```
KEY = 8d2e60365f17c7df1040d7501b4a7b5a
PLAINTEXT = 59b5088e6dadc3ad5f27a460872d5929
CIPHERTEXT = a02600ecb8ea77625bba6641ed5f5920

KEY = 2d0860dae7fdb0bd4bfab111f615227a
PLAINTEXT = a02600ecb8ea77625bba6641ed5f5920
CIPHERTEXT = 5241ead9a89ca31a7147f53a5bf6d96a

KEY = 7f498a034f6113a73abd442bade3fb10
PLAINTEXT = 5241ead9a89ca31a7147f53a5bf6d96a
CIPHERTEXT = 22f09171bc67d0661d1c25f181a69f33
```

6.4.2 Monte Carlo Test - CBC

REQUEST file:

```
KEY = 9dc2c84a37850c11699818605f47958c
IV = 256953b2feab2a04ae0180d8335bbed6
PLAINTEXT = 2e586692e647f5028ec6fa47a55a2aab
```

Monte Carlo Algorithm:

```
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output IV[i]
     Output PT[0]
     For j = 0 to 999
          If ( j=0 )
               CT[j] = AES(Key[i], IV[i], PT[j])
               PT[j+1] = IV[i]
          Else
               CT[j] = AES(Key[i], PT[j])
               PT[j+1] = CT[j-1]
     Output CT[j]
     If ( keylen = 128 )
          Key[i+1] = Key[i] xor CT[j]
     If ( keylen = 192 )
          Key[i+1] = Key[i] xor (last 64-bits of
                     CT[j-1] || CT[j])
```

```
        If ( keylen = 256 )
             Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
        IV[i+1] = CT[j]
        PT[0] = CT[j-1]
```

Note: The IV value is only used on the first cipher function per text string.

The first three entries of the *RESPONSE* file are:

```
KEY = 9dc2c84a37850c11699818605f47958c
IV = 256953b2feab2a04ae0180d8335bbed6
PLAINTEXT = 2e586692e647f5028ec6fa47a55a2aab
CIPHERTEXT = 1b1ebd1fc45ec43037fd4844241a437f

KEY = 86dc7555f3dbc8215e6550247b5dd6f3
IV = 1b1ebd1fc45ec43037fd4844241a437f
PLAINTEXT = c1b77ed52521525f0a4ba341bdaf51d9
CIPHERTEXT = bf43583a665fa45fdee831243a16ea8f

KEY = 399f2d6f95846c7e808d6100414b3c7c
IV= bf43583a665fa45fdee831243a16ea8f
PLAINTEXT = 7cbeea19157ec7bbf6289e2dff5e8ee4
CIPHERTEXT = 5464e1900f81e06f67139456da25fc09
```

6.4.3 Monte Carlo Test – OFB

REQUEST file:

```
KEY = b11e4ecae2e71e14145dd7db2635652f
IV = add32bf8204c33339c54cd5858ee0d13
PLAINTEXT = 732049e89d74fce7c5a4966404868fa6
```

Monte Carlo Algorithm:

```
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output IV[i]
     Output PT[0]
     For j = 0 to 999
          If ( j=0 )
          CT[j] = AES(Key[i], IV[i], PT[j])
          PT[j+1] = IV[i]
          Else
               CT[j] = AES(Key[i], PT[j])
```

```
            PT[j+1] = CT[j-1]
        Output CT[j]
        If ( keylen = 128 )
            Key[i+1] = Key[i] xor CT[j]
        If ( keylen = 192 )
            Key[i+1] = Key[i] xor (last 64-bits of
                        CT[j-1] || CT[j])
        If ( keylen = 256 )
            Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
        IV[i+1] = CT[j]
        PT[0] = CT[j-1]
```

Note: The IV value is only used on the first cipher function per text string.

The first three entries of the *RESPONSE* file are:

```
KEY = b11e4ecae2e71e14145dd7db2635652f
IV = add32bf8204c33339c54cd5858ee0d13
PLAINTEXT = 732049e89d74fce7c5a4966404868fa6
CIPHERTEXT = 12bacd0509a0eb7e961944c77e64a0a6

KEY = a3a483cfeb47f56a8244931c5851c589
IV = 12bacd0509a0eb7e961944c77e64a0a6
PLAINTEXT = 31c58d58a2d1391a1943ce0406da85bd
CIPHERTEXT = d633e4f2baafee8ceee15778a8578dc0

KEY = 7597673d51e81be66ca5c464f0064849
IV = d633e4f2baafee8ceee15778a8578dc0
PLAINTEXT = 46d65190e96e2b300f47afe6e73502fb
CIPHERTEXT = ec66bf35224887db0fa947caf7d0a795
```

6.4.4 Monte Carlo Test – CFB1

REQUEST file:

```
KEY = 17de6f7dc48e81237e940edf5dfefcd4
IV = a4360b5489d5aa41d3c4252fa4409923
PLAINTEXT = 1
```

Monte Carlo Algorithm:

```
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output IV[i]
     Output PT[0]
```

```
        For j = 0 to 999
             If ( j=0 )
                  CT[j] = AES(Key[i], IV[i], PT[j])
                  PT[j+1] = BitJ(IV[i])
             Else
                  CT[j] = AES(Key[i], PT[j])
                  If ( j<128 )
                       PT[j+1] = BitJ(IV[i])
                  Else
                       PT[j+1] = CT[j-128]
        Output CT[j]
        If ( keylen = 128 )
             Key[i+1] = Key[i] xor (CT[j-127] || CT[j-126]
                        || … || CT[j])
        If ( keylen = 192 )
             Key[i+1] = Key[i] xor (CT[j-191] || CT[j-190]
                        || … || CT[j])
        If ( keylen = 256 )
             Key[i+1] = Key[i] xor (CT[j-255] || CT[j-254]
                        || … || CT[j])
        IV[i+1] = (CT[j-127] || CT[j-126]  || … || CT[j])
        PT[0] = CT[j-128]
```

Note1: The IV value is only used on the first cipher function per text string.
Note2: `BitJ(IV[i])` means the j^{th} bit of `IV[i]`, labeled left to right starting at 0.

The first three entries of the *RESPONSE* file are:

```
KEY = 17de6f7dc48e81237e940edf5dfefcd4
IV = a4360b5489d5aa41d3c4252fa4409923
PLAINTEXT = 1
CIPHERTEXT = 1

KEY = 698f194c33e5c94d4f7dfa7d3d50c3b9
IV = 7e517631f76b486e31e9f4a260ae3f6d
PLAINTEXT = 1
CIPHERTEXT = 0

KEY = 8deacd5d4ae4c1f80b1663e7c29f803b
IV = e465d411790108b5446b999affcf4382
PLAINTEXT = 1
CIPHERTEXT = 0
```

6.4.5 Monte Carlo Test – CFB8

REQUEST file:

```
Key = b616bd26c39592efca8faeb953856025
```

```
IV = 47a70a39ba519210e9bc4f70d812b886
PLAINTEXT = c6
```

Monte Carlo Algorithm:

```
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output IV[i]
     Output PT[0]
     For j = 0 to 999
          If ( j=0 )
               CT[j] = AES(Key[i], IV[i], PT[j])
               PT[j+1] = ByteJ(IV[i])
          Else
               CT[j] = AES(Key[i], PT[j])
               If ( j<16 )
                    PT[j+1] = ByteJ(IV[i])
               Else
                    PT[j+1] = CT[j-16]
     Output CT[j]
     If ( keylen = 128 )
          Key[i+1] = Key[i] xor (CT[j-15] || CT[j-14]
                     || … || CT[j])
     If ( keylen = 192 )
          Key[i+1] = Key[i] xor (CT[j-23] || CT[j-22]
                     || … || CT[j])
     If ( keylen = 256 )
          Key[i+1] = Key[i] xor (CT[j-31] || CT[j-30]
                     || … || CT[j])
     IV[i+1] = (CT[j-15] || CT[j-14]  || … || CT[j])
     PT[0] = CT[j-16]
```

Note1: The IV value is only used on the first cipher function per text string.
Note2: `ByteJ(IV[i])` means the j^{th} byte of `IV[i]`, labeled left to right starting at 0.

The first three entries of the *RESPONSE* file are:

```
KEY = b616bd26c39592efca8faeb953856025
IV = 47a70a39ba519210e9bc4f70d812b886
PLAINTEXT = c6
CIPHERTEXT = 76

KEY = 41ba244b9eb55e5e47f8c8795e4d0b53
IV = f7ac996d5d20ccb18d7766c00dc86b76
PLAINTEXT = 15
```

```
CIPHERTEXT = dd

KEY = 2e42e126683e89c91f63260dce91b48e
IV = 6ff8c56df68bd797589bee7490dcbfdd
PLAINTEXT = 97
CIPHERTEXT = d1
```

6.4.6 Monte Carlo Test – CFB128

REQUEST file:

```
KEY = 711511931a1562ea73290a8b0a37a3b4
IV = 9dce23fd2df5360f799cf17984e47c8d
PLAINTEXT = f066be4bd671ebc1c4cf3c008ef2cf18
```

Monte Carlo Algorithm:

```
Key[0] = Key
IV[0] = IV
PT[0] = PT
For i = 0 to 99
     Output Key[i]
     Output IV[i]
     Output PT[0]
     For j = 0 to 999
          If ( j=0 )
               CT[j] = AES(Key[i], IV[i], PT[j])
               PT[j+1] = IV[i]
          Else
               CT[j] = AES(Key[i], PT[j])
               PT[j+1] = CT[j-1]
     Output CT[j]
     If ( keylen = 128 )
          Key[i+1] = Key[i] xor CT[j]
     If ( keylen = 192 )
          Key[i+1] = Key[i] xor (last 64-bits of
                     CT[j-1] || CT[j])
     If ( keylen = 256 )
          Key[i+1] = Key[i] xor (CT[j-1] || CT[j])
     IV[i+1] = CT[j]
     PT[0] = CT[j-1]
```

Note: The IV value is only used on the first cipher function per text string.

The first three entries of the *RESPONSE* file are:

```
KEY = 711511931a1562ea73290a8b0a37a3b4
IV = 9dce23fd2df5360f799cf17984e47c8d
```

```
PLAINTEXT = f066be4bd671ebc1c4cf3c008ef2cf18
CIPHERTEXT = 4a51a519c76d2f5bebf2413cec54d007

KEY = 3b44b48add784db198db4bb7e66373b3
IV = 4a51a519c76d2f5bebf2413cec54d007
PLAINTEXT = 5e24a81fd125bd1974ea5f2b70b90f1f
CIPHERTEXT = 3fa5d0d921f53060568b43184d8a259d

KEY = 04e16453fc8d7dd1ce5008afabe9562e
IV = 3fa5d0d921f53060568b43184d8a259d
PLAINTEXT = 7f91f72b353e834fee55a34b8363fe6f
CIPHERTEXT = 0c6ef16c0fd28584e9eee565c299059b
```

Appendix A. Counter Mode Requirements

It is a requirement of the Counter Mode that a unique counter block be used for each plaintext block that is ever encrypted with a given key, across all messages. Due to the fact that Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. Also, since the tests in this document are only a statistical sampling, additional assurances are needed that the counter blocks used are in fact unique. Therefore, if the module being tested derives counter values internally, the testing lab shall conduct a design review of the internal counter mechanism used to ensure that it provides unique counter block values as well as a code review of the implementation of the counter mechanism to ensure that it properly implements the design. In addition, the tests for ECB Mode shall be performed on the encryption engine used for the counter mode.

Appendix B. GFSbox Know Answer Test Values

B.1. Keysize = 128

KEY = 00000000000000000000000000000000
IV or PLAINTEXT = 00000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
f34481ec3cc627bacd5dc3fb08f273e6	0336763e966d92595a567cc9ce537f5e
9798c4640bad75c7c3227db910174e72	a9a1631bf4996954ebc093957b234589
96ab5c2ff612d9dfaae8c31f30c42168	ff4f8391a6a40ca5b25d23bedd44a597
6a118a874519e64e9963798a503f1d35	dc43be40be0e53712f7e2bf5ca707209
cb9fceec81286ca3e989bd979b0cb284	92beedab1895a94faa69b632e5cc47ce
b26aeb1874e47ca8358ff22378f09144	459264f4798f6a78bacb89c15ed3d601
58c8e00b2631686d54eab84b91f0aca1	08a4e2efec8a8e3312ca7460b9040bbf

B.2. Keysize = 192

KEY = 000000000000000000000000000000000000000000000000
IV or PLAINTEXT = 00000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
1b077a6af4b7f98229de786d7516b639	275cfc0413d8ccb70513c3859b1d0f72
9c2d8842e5f48f57648205d39a239af1	c9b8135ff1b5adc413dfd053b21bd96d
bff52510095f518ecca60af4205444bb	4a3650c3371ce2eb35e389a171427440
51719783d3185a535bd75adc65071ce1	4f354592ff7c8847d2d0870ca9481b7c
26aa49dcfe7629a8901a69a9914e6dfd	d5e08bf9a182e857cf40b3a36ee248cc
941a4773058224e1ef66d10e0a6ee782	067cd9d3749207791841562507fa9626

B.3. Keysize = 256

KEY = 0000000000000000000000000000000000000000000000000000000000000000
IV or PLAINTEXT = 00000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
014730f80ac625fe84f026c60bfd547d	5c9d844ed46f9885085e5d6a4f94c7d7
0b24af36193ce4665f2825d7b4749c98	a9ff75bd7cf6613d3731c77c3b6d0c04
761c1fe41a18acf20d241650611d90f1	623a52fcea5d443e48d9181ab32c7421
8a560769d605868ad80d819bdba03771	38f2c7ae10612415d27ca190d27da8b4
91fbef2d15a97816060bee1feaa49afe	1bc704f1bce135ceb810341b216d7abe

Appendix C. KeySbox Know Answer Test Values

C.1. Keysize = 128

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
10a58869d74be5a374cf867cfb473859	6d251e6944b051e04eaa6fb4dbf78465
caea65cdbb75e9169ecd22ebe6e54675	6e29201190152df4ee058139def610bb
a2e2fa9baf7d20822ca9f0542f764a41	c3b44b95d9d2f25670eee9a0de099fa3
b6364ac4e1de1e285eaf144a2415f7a0	5d9b05578fc944b3cf1ccf0e746cd581
64cf9c7abc50b888af65f49d521944b2	f7efc89d5dba578104016ce5ad659c05
47d6742eefcc0465dc96355e851b64d9	0306194f666d183624aa230a8b264ae7
3eb39790678c56bee34bbcdeccf6cdb5	858075d536d79ccee571f7d7204b1f67
64110a924f0743d500ccadae72c13427	35870c6a57e9e92314bcb8087cde72ce
18d8126516f8a12ab1a36d9f04d68e51	6c68e9be5ec41e22c825b7c7affb4363
f530357968578480b398a3c251cd1093	f5df39990fc688f1b07224cc03e86cea
da84367f325d42d601b4326964802e8e	bba071bcb470f8f6586e5d3add18bc66
e37b1c6aa2846f6fdb413f238b089f23	43c9f7e62f5d288bb27aa40ef8fe1ea8
6c002b682483e0cabcc731c253be5674	3580d19cff44f1014a7c966a69059de5
143ae8ed6555aba96110ab58893a8ae1	806da864dd29d48deafbe764f8202aef
b69418a85332240dc82492353956ae0c	a303d940ded8f0baff6f75414cac5243
71b5c08a1993e1362e4d0ce9b22b78d5	c2dabd117f8a3ecabfbb11d12194d9d0
e234cdca2606b81f29408d5f6da21206	fff60a4740086b3b9c56195b98d91a7b
13237c49074a3da078dc1d828bb78c6f	8146a08e2357f0caa30ca8c94d1a0544
3071a2a48fe6cbd04f1a129098e308f8	4b98e06d356deb07ebb824e5713f7be3
90f42ec0f68385f2ffc5dfc03a654dce	7a20a53d460fc9ce0423a7a0764c6cf2
febd9a24d8b65c1c787d50a4ed3619a9	f4a70d8af877f9b02b4c40df57d45b17

C.2. Keysize = 192

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
e9f065d7c13573587f7875357dfbb16c53489f6a4bd0f7cd	0956259c9cd5cfd0181cca53380cde0653489f6a4bd0f7cd
15d20f6ebc7e649fd95b76b107e6daba967c8a9484797f29	8e4e18424e591a3d5b6f0876f16f8594967c8a9484797f29
a8a282ee31c03fae4f8e9b8930d5473c2ed695a347e88b7c	93f3270cfc877ef17e106ce938979cb02ed695a347e88b7c
cd62376d5ebb414917f0c78f05266433dc9192a1ec943300	7f6c25ff41858561bb62f36492e93c29dc9192a1ec943300
502a6ab36984af268bf423c7f509205207fc1552af4a91e5	8e06556dcbb00b809a025047cff2a94007fc1552af4a91e5
25a39dbfd8034f71a81f9ceb55026e4037f8f6aa30ab44ce	3608c344868e94555d23a120f8a5502d37f8f6aa30ab44ce

e08c15411774ec4a908b64eadc6ac4199c7cd453f3aaef53	77da2021935b840b7f5dcc39132da9e5
3b375a1ff7e8d44409696e6326ec9dec86138e2ae010b980	3b7c24f825e3bf9873c9f14d39a0e6f4
950bb9f22cc35be6fe79f52c320af93dec5bc9c0c2f9cd53	64ebf95686b353508c90ecd8b6134316
7001c487cc3e572cfc92f4d0e697d982e8856fdcc957da40	ff558c5d27210b7929b73fc708eb4cf1
f029ce61d4e5a405b41ead0a883cc6a737da2cf50a6c92ae	a2c3b2a818075490a7b4c14380f02702
61257134a518a0d57d9d244d45f6498cbc32f2bafc522d79	cfe4d74002696ccf7d87b14a2f9cafc9
b0ab0a6a818baef2d11fa33eac947284fb7d748cfb75e570	d2eafd86f63b109b91f5dbb3a3fb7e13
ee053aa011c8b428cdcc3636313c54d6a03cac01c71579d6	9b9fdd1c5975655f539998b306a324af
d2926527e0aa9f37b45e2ec2ade5853ef807576104c7ace3	dd619e1cf204446112e0af2b9afa8f8c
982215f4e173dfa0fcffe5d3da41c4812c7bcc8ed3540f93	d4f0aae13c8fe9339fbf9e69ed0ad74d
98c6b8e01e379fbd14e61af6af891596583565f2a27d59e9	19c80ec4a6deb7e5ed1033dda933498f
b3ad5cea1dddc214ca969ac35f37dae1a9a9d1528f89bb35	3cf5e1d21a17956d1dffad6a7c41c659
45899367c3132849763073c435a9288a766c8b9ec2308516	69fd12e8505f8ded2fdcb197a121b362
ec250e04c3903f602647b85a401a1ae7ca2f02f67fa4253e	8aa584e2cc4d17417a97cb9a28ba29c8
d077a03bd8a38973928ccafe4a9d2f455130bd0af5ae46a9	abc786fb1edb504580c4d882ef29a0c7
d184c36cf0dddfec39e6541950060222 37871a47c33d3198	2e19fb60a3e1de0166f483c97824a978
4c6994ffa9dcdc805b60c2c0095334c42d95a8fc0ca5b080	7656709538dd5fec41e0ce6a0f8e207d
c88f5b00a4ef9a6840e2acaf33f00a3bdc4e25895303fa72	a67cf333b314d411d3c0ae6e1cfcd8f5

C.3. Keysize = 256

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
c47b0294dbbbee0fec4757f22ffeee3587ca4730c3d33b691df38bab076bc558	46f2fb342d6f0ab477476fc501242c5f
28d46cffa158533194214a91e712fc2b45b518076675affd910edeca5f41ac64	4bf3b0a69aeb6657794f2901b1440ad4

c1cc358b449909a19436cfbb3f852ef8bcb5ed12ac7058325f56e6099aab1a1c	352065272169abf9856843927d0674fd
984ca75f4ee8d706f46c2d98c0bf4a45f5b00d791c2dfeb191b5ed8e420fd627	4307456a9e67813b452e15fa8fffe398
b43d08a447ac8609baadae4ff12918b9f68fc1653f1269222f123981ded7a92f	4663446607354989477a5c6f0f007ef4
1d85a181b54cde51f0e098095b2962fdc93b51fe9b88602b3f54130bf76a5bd9	531c2c38344578b84d50b3c917bbb6e1
dc0eba1f2232a7879ded34ed8428eeb8769b056bbaf8ad77cb65c3541430b4cf	fc6aec906323480005c58e7e1ab004ad
f8be9ba615c5a952cabbca24f68f8593039624d524c816acda2c9183bd917cb9	a3944b95ca0b52043584ef02151926a8
797f8b3d176dac5b7e34a2d539c4ef367a16f8635f6264737591c5c07bf57a3e	a74289fe73a4c123ca189ea1e1b49ad5
6838d40caf927749c13f0329d331f448e202c73ef52c5f73a37ca635d4c47707	b91d4ea4488644b56cf0812fa7fcf5fc
ccd1bc3c659cd3c59bc437484e3c5c724441da8d6e90ce556cd57d0752663bbc	304f81ab61a80c2e743b94d5002a126b
13428b5e4c005e0636dd338405d173ab135dec2a25c22c5df0722d69dcc43887	649a71545378c783e368c9ade7114f6c
07eb03a08d291d1b07408bf3512ab40c91097ac77461aad4bb859647f74f00ee	47cb030da2ab051dfc6c4bf6910d12bb
90143ae20cd78c5d8ebdd6cb9dc1762427a96c78c639bccc41a61424564eafe1	798c7c005dee432b2c8ea5dfa381ecc3
b7a5794d52737475d53d5a377200849be0260a67a2b22ced8bbef12882270d07	637c31dc2591a07636f646b72daabbe7
fca02f3d5011cfc5c1e23165d413a049d4526a991827424d896fe3435e0bf68e	179a49c712154bbffbe6e7a84a18e220

Appendix D. VarTxt Known Answer Test Values

D.1. Keysize = 128

KEY = 00000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
80000000000000000000000000000000	3ad78e726c1ec02b7ebfe92b23d9ec34
c0000000000000000000000000000000	aae5939c8efdf2f04e60b9fe7117b2c2
e0000000000000000000000000000000	f031d4d74f5dcbf39daaf8ca3af6e527
f0000000000000000000000000000000	96d9fd5cc4f07441727df0f33e401a36
f8000000000000000000000000000000	30ccdb044646d7e1f3ccea3dca08b8c0
fc000000000000000000000000000000	16ae4ce5042a67ee8e177b7c587ecc82
fe000000000000000000000000000000	b6da0bb11a23855d9c5cb1b4c6412e0a
ff000000000000000000000000000000	db4f1aa530967d6732ce4715eb0ee24b
ff800000000000000000000000000000	a81738252621dd180a34f3455b4baa2f
ffc00000000000000000000000000000	77e2b508db7fd89234caf7939ee5621a
ffe00000000000000000000000000000	b8499c251f8442ee13f0933b688fcd19
fff00000000000000000000000000000	965135f8a81f25c9d630b17502f68e53
fff80000000000000000000000000000	8b87145a01ad1c6cede995ea3670454f
fffc0000000000000000000000000000	8eae3b10a0c8ca6d1d3b0fa61e56b0b2
fffe0000000000000000000000000000	64b4d629810fda6bafdf08f3b0d8d2c5
ffff0000000000000000000000000000	d7e5dbd3324595f8fdc7d7c571da6c2a
ffff8000000000000000000000000000	f3f72375264e167fca9de2c1527d9606
ffffc000000000000000000000000000	8ee79dd4f401ff9b7ea945d86666c13b
ffffe000000000000000000000000000	dd35cea2799940b40db3f819cb94c08b
fffff000000000000000000000000000	6941cb6b3e08c2b7afa581ebdd607b87
fffff800000000000000000000000000	2c20f439f6bb097b29b8bd6d99aad799
fffffc000000000000000000000000000	625d01f058e565f77ae86378bd2c49b3
fffffe000000000000000000000000000	c0b5fd98190ef45fbb4301438d095950
ffffff000000000000000000000000000	13001ff5d99806efd25da34f56be854b
ffffff800000000000000000000000000	3b594c60f5c8277a5113677f94208d82
ffffffc000000000000000000000000000	e9c0fc1818e4aa46bd2e39d638f89e05
ffffffe000000000000000000000000000	f8023ee9c3fdc45a019b4e985c7e1a54
fffffff000000000000000000000000000	35f40182ab4662f3023baec1ee796b57
fffffff800000000000000000000000000	3aebbad7303649b4194a6945c6cc3694
fffffffc000000000000000000000000000	a2124bea53ec2834279bed7f7eb0f938
fffffffe000000000000000000000000000	b9fb4399fa4facc7309e14ec98360b0a
ffffffff000000000000000000000000000	c26277437420c5d634f715aea81a9132
ffffffff800000000000000000000000000	171a0e1b2dd424f0e089af2c4c10f32f
ffffffffc000000000000000000000000000	7cadbe402d1b208fe735edce00aee7ce
ffffffffe000000000000000000000000000	43b02ff929a1485af6f5c6d6558baa0f
fffffffff000000000000000000000000000	092faacc9bf43508bf8fa8613ca75dea
fffffffff800000000000000000000000000	cb2bf8280f3f9742c7ed513fe802629c
fffffffffc000000000000000000000000000	215a41ee442fa992a6e323986ded3f68

fffffffffe0000000000000000000000	f21e99cf4f0f77cea836e11a2fe75fb1
fffffffffe0000000000000000000000	95e3a0ca9079e646331df8b4e70d2cd6
fffffffffe8000000000000000000000	4afe7f120ce7613f74fc12a01a828073
fffffffffe8000000000000000000000	827f000e75e2c8b9d479beed913fe678
fffffffffe8000000000000000000000	35830c8e7aaefe2d30310ef381cbf691
fffffffffe8000000000000000000000	191aa0f2c8570144f38657ea4085ebe5
fffffffffe8000000000000000000000	85062c2c909f15d9269b6c18ce99c4f0
fffffffffe8000000000000000000000	678034dc9e41b5a560ed239eeab1bc78
fffffffffe8000000000000000000000	c2f93a4ce5ab6d5d56f1b93cf19911c1
fffffffffe8000000000000000000000	1c3112bcb0c1dcc749d799743691bf82
fffffffffe8000000000000000000000	00c55bd75c7f9c881989d3ec1911c0d4
fffffffffe8000000000000000000000	ea2e6b5ef182b7dff3629abd6a12045f
fffffffffe8000000000000000000000	22322327e01780b17397f24087f8cc6f
fffffffffe8000000000000000000000	c9cacb5cd11692c373b2411768149ee7
fffffffffe8000000000000000000000	a18e3dbbca577860dab6b80da3139256
fffffffffe8000000000000000000000	79b61c37bf328ecca8d743265a3d425c
fffffffffe8000000000000000000000	d2d99c6bcc1f06fda8e27e8ae3f1ccc7
fffffffffe8000000000000000000000	1bfd4b91c701fd6b61b7f997829d663b
fffffffffe8000000000000000000000	11005d52f25f16bdc9545a876a63490a
fffffffffe8000000000000000000000	3a4d354f02bb5a5e47d39666867f246a
fffffffffe8000000000000000000000	d451b8d6e1e1a0ebb155fbbf6e7b7dc3
fffffffffe8000000000000000000000	6898d4f42fa7ba6a10ac05e87b9f2080
fffffffffe8000000000000000000000	b611295e739ca7d9b50f8e4c0e754a3f
fffffffffe8000000000000000000000	7d33fc7d8abe3ca1936759f8f5deaf20
fffffffffe8000000000000000000000	3b5e0f566dc96c298f0c12637539b25c
fffffffffe8000000000000000000000	f807c3e7985fe0f5a50e2cdb25c5109e
fffffffffe8000000000000000000000	41f992a856fb278b389a62f5d274d7e9
fffffffffe8000000000000000000000	10d3ed7a6fe15ab4d91acbc7d0767ab1
fffffffffe8000000000000000000000	21feecd45b2e675973ac33bf0c5424fc
fffffffffe8000000000000000000000	1480cb3955ba62d09eea668f7c708817
fffffffffe8000000000000000000000	66404033d6b72b609354d5496e7eb511
fffffffffe8000000000000000000000	1c317a220a7d700da2b1e075b00266e1
fffffffffe8000000000000000000000	ab3b89542233f1271bf8fd0c0f403545
fffffffffe8000000000000000000000	d93eae966fac46dca927d6b114fa3f9e
fffffffffe8000000000000000000000	1bdec521316503d9d5ee65df3ea94ddf
fffffffffe8000000000000000000000	eef456431dea8b4acf83bdae3717f75f
fffffffffe8000000000000000000000	06f2519a2fafaa596bfef5cfa15c21b9
fffffffffe8000000000000000000000	251a7eac7e2fe809e4aa8d0d7012531a
fffffffffe8000000000000000000000	3bffc16e4c49b268a20f8d96a60b4058
fffffffffe8000000000000000000000	e886f9281999c5bb3b3e8862e2f7c988
fffffffffe8000000000000000000000	563bf90d61beef39f48dd625fcef1361
fffffffffe8000000000000000000000	4d37c850644563c69fd0acd9a049325b
fffffffffe8000000000000000000000	b87c921b91829ef3b13ca541ee1130a6
fffffffffe8000000000000000000000	2e65eb6b6ea383e109accce8326b0393
fffffffffe8000000000000000000000	9ca547f7439edc3e255c0f4d49aa8990

ffffffffffffffffffff00000000000	a5e652614c9300f37816b1f9fd0c87f9
ffffffffffffffffffff80000000000	14954f0b4697776f44494fe458d814ed
fffffffffffffffffffffc0000000000	7c8d9ab6c2761723fe42f8bb506cbcf7
fffffffffffffffffffffe0000000000	db7e1932679fdd99742aab04aa0d5a80
ffffffffffffffffffffff0000000000	4c6a1c83e568cd10f27c2d73ded19c28
ffffffffffffffffffffff8000000000	90ecbe6177e674c98de412413f7ac915
fffffffffffffffffffffffc000000000	90684a2ac55fe1ec2b8ebd5622520b73
fffffffffffffffffffffffe000000000	7472f9a7988607ca7970779599103 5e6
ffffffffffffffffffffffff000000000	56aff089878bf3352f8df172a3ae47d8
ffffffffffffffffffffffff800000000	65c0526cbe40161b8019a2a3171abd23
fffffffffffffffffffffffc00000000	377be0be33b4e3e310b4aabda173f84f
fffffffffffffffffffffffe00000000	9402e9aa6f69de6504da8d20c4fcaa2f
ffffffffffffffffffffffff00000000	123c1f4af313ad8c2ce648b2e71fb6e1
ffffffffffffffffffffffff80000000	1ffc626d30203dcdb0019fb80f726cf4
fffffffffffffffffffffffffc0000000	76da1fbe3a50728c50fd2e621b5ad885
fffffffffffffffffffffffffe0000000	082eb8be35f442fb52668e16a591d1d6
ffffffffffffffffffffffffff0000000	e656f9ecf5fe27ec3e4a73d00c282fb3
ffffffffffffffffffffffffff8000000	2ca8209d63274cd9a29bb74bcd77683a
fffffffffffffffffffffffffffc000000	79bf5dce14bb7dd73a8e3611de7ce026
fffffffffffffffffffffffffffe000000	3c849939a5d29399f344c4a0eca8a576
ffffffffffffffffffffffffffff000000	ed3c0a94d59bece98835da7aa4f07ca2
ffffffffffffffffffffffffffff800000	63919ed4ce10196438b6ad09d99cd795
fffffffffffffffffffffffffffffc00000	7678f3a833f19fea95f3c6029e2bc610
fffffffffffffffffffffffffffffe00000	3aa426831067d36b92be7c5f81c13c56
fffffffffffffffffffffffffffff00000	9272e2d2cdd11050998c845077a30ea0
fffffffffffffffffffffffffffff80000	088c4b53f5ec0ff814c19adae7f6246c
fffffffffffffffffffffffffffffc0000	4010a5e401fdf0a0354ddbcc0d012b17
fffffffffffffffffffffffffffffe0000	a87a385736c0a6189bd6589bd8445a93
ffffffffffffffffffffffffffffff0000	545f2b83d9616dccf60fa9830e9cd287
ffffffffffffffffffffffffffffff8000	4b706f7f92406352394037a6d4f4688d
fffffffffffffffffffffffffffffffc000	b7972b3941c44b90afa7b264bfba7387
fffffffffffffffffffffffffffffffe000	6f45732cf10881546f0fd23896d2bb60
ffffffffffffffffffffffffffffffff000	2e3579ca15af27f64b3c955a5bfc30ba
ffffffffffffffffffffffffffffffff800	34a2c5a91ae2aec99b7d1b5fa6780447
fffffffffffffffffffffffffffffffc00	a4d6616bd04f87335b0e53351227a9ee
fffffffffffffffffffffffffffffffe00	7f692b03945867d16179a8cefc83ea3f
ffffffffffffffffffffffffffffffff00	3bd141ee84a0e6414a26e7a4f281f8a2
ffffffffffffffffffffffffffffffff80	d1788f572d98b2b16ec5d5f3922b99bc
fffffffffffffffffffffffffffffffc0	0833ff6f61d98a57b288e8c3586b85a6
fffffffffffffffffffffffffffffffe0	8568261797de176bf0b43becc6285afb
ffffffffffffffffffffffffffffffff0	f9b0fda0c4a898f5b9e6f661c4ce4d07
ffffffffffffffffffffffffffffffff8	8ade895913685c67c5269f8aae42983e
fffffffffffffffffffffffffffffffc	39bde67d5c8ed8a8b1c37eb8fa9f5ac0
fffffffffffffffffffffffffffffffe	5c005e72c1418c44f569f2ea33ba54f3
ffffffffffffffffffffffffffffffff	3f5b8cc9ea855a0afa7347d23e8d664e

D.2. Keysize = 192

KEY = 000000000000000000000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
80000000000000000000000000000000	6cd02513e8d4dc986b4afe087a60bd0c
c0000000000000000000000000000000	2ce1f8b7e30627c1c4519eada44bc436
e0000000000000000000000000000000	9946b5f87af446f5796c1fee63a2da24
f0000000000000000000000000000000	2a560364ce529efc21788779568d5555
f8000000000000000000000000000000	35c1471837af446153bce55d5ba72a0a
fc000000000000000000000000000000	ce60bc52386234f158f84341e534cd9e
fe000000000000000000000000000000	8c7c27ff32bcf8dc2dc57c90c2903961
ff000000000000000000000000000000	32bb6a7ec84499e166f936003d55a5bb
ff800000000000000000000000000000	a5c772e5c62631ef660ee1d5877f6d1b
ffc00000000000000000000000000000	030d7e5b64f380a7e4ea5387b5cd7f49
ffe00000000000000000000000000000	0dc9a2610037009b698f11bb7e86c83e
fff00000000000000000000000000000	0046612c766d1840c226364f1fa7ed72
fff80000000000000000000000000000	4880c7e08f27befe78590743c05e698b
fffc0000000000000000000000000000	2520ce829a26577f0f4822c4ecc87401
fffe0000000000000000000000000000	8765e8acc169758319cb46dc7bcf3dca
ffff0000000000000000000000000000	e98f4ba4f073df4baa116d011dc24a28
ffff8000000000000000000000000000	f378f68c5dbf59e211b3a659a7317d94
ffffc000000000000000000000000000	283d3b069d8eb9fb432d74b96ca762b4
ffffe000000000000000000000000000	a7e1842e8a87861c221a500883245c51
fffff000000000000000000000000000	77aa270471881be070fb52c7067ce732
fffff800000000000000000000000000	01b0f476d484f43f1aeb6efa9361a8ac
fffffc000000000000000000000000000	1c3a94f1c052c55c2d8359aff2163b4f
fffffe000000000000000000000000000	e8a067b604d5373d8b0f2e05a03b341b
ffffff000000000000000000000000000	a7876ec87f5a09bfea42c77da30fd50e
ffffff800000000000000000000000000	0cf3e9d3a42be5b854ca65b13f35f48d
ffffffc000000000000000000000000000	6c62f6bbcab7c3e821c9290f08892dda
ffffffe000000000000000000000000000	7f5e05bd2068738196fee79ace7e3aec
fffffff000000000000000000000000000	440e0d733255cda92fb46e842fe58054
fffffff800000000000000000000000000	aa5d5b1c4ea1b7a22e5583ac2e9ed8a7
fffffffc000000000000000000000000000	77e537e89e8491e8662aae3bc809421d
fffffffe000000000000000000000000000	997dd3e9f1598bfa73f75973f7e93b76
ffffffff000000000000000000000000000	1b38d4f7452afefcb7fc721244e4b72e
ffffffff800000000000000000000000000	0be2b18252e774dda30cdda02c6906e3
fffffffffc000000000000000000000000	d2695e59c20361d82652d7d58b6f11b2
fffffffffe000000000000000000000000	902d88d13eae52089abd6143cfe394e9
ffffffffff000000000000000000000000	d49bceb3b823fedd602c305345734bd2
ffffffffff800000000000000000000000	707b1dbb0ffa40ef7d95def421233fae
fffffffffffc000000000000000000000000	7ca0c1d93356d9eb8aa952084d75f913
fffffffffffe000000000000000000000000	f2cbf9cb186e270dd7bdb0c28febc57d

fffffffff000000000000000000000	c94337c37c4e790ab45780bd9c3674a0
fffffffff800000000000000000000	8e3558c135252fb9c9f367ed609467a1
ffffffffc000000000000000000000	1b72eeaee4899b443914e5b3a57fba92
ffffffffe000000000000000000000	011865f91bc56868d051e52c9efd59b7
fffffffff000000000000000000000	e4771318ad7a63dd680f6e583b7747ea
fffffffff800000000000000000000	61e3d194088dc8d97e9e6db37457eac5
ffffffffc000000000000000000000	36ff1ec9ccfbc349e5d356d063693ad6
ffffffffe000000000000000000000	3cc9e9a9be8cc3f6fb2ea24088e9bb19
fffffffff000000000000000000000	1ee5ab003dc8722e74905d9a8fe3d350
fffffffff800000000000000000000	245339319584b0a412412869d6c2eada
ffffffffc000000000000000000000	7bd496918115d14ed5380852716c8814
ffffffffe000000000000000000000	273ab2f2b4a366a57d582a339313c8b1
fffffffff000000000000000000000	113365a9ffbe3b0ca61e98507554168b
fffffffff800000000000000000000	afa99c997ac478a0dea4119c9e45f8b1
ffffffffc000000000000000000000	9216309a7842430b83ffb98638011512
ffffffffe000000000000000000000	62abc792288258492a7cb45145f4b759
fffffffff000000000000000000000	534923c169d504d7519c15d30e756c50
fffffffff800000000000000000000	fa75e05bcdc7e00c273fa33f6ee441d2
ffffffffc000000000000000000000	7d350fa6057080f1086a56b17ec240db
ffffffffe000000000000000000000	f34e4a6324ea4a5c39a661c8fe5ada8f
fffffffff000000000000000000000	0882a16f44088d42447a29ac090ec17e
fffffffff800000000000000000000	3a3c15bfc11a9537c130687004e136ee
ffffffffc000000000000000000000	22c0a7678dc6d8cf5c8a6d5a9960767c
ffffffffe000000000000000000000	b46b09809d68b9a456432a79bdc2e38c
fffffffff000000000000000000000	93baaffb35fbe739c17c6ac22eecf18f
fffffffff800000000000000000000	c8aa80a7850675bc007c46df06b49868
ffffffffc000000000000000000000	12c6f3877af421a918a84b775858021d
ffffffffe000000000000000000000	33f123282c5d633924f7d5ba3f3cab11
fffffffff000000000000000000000	a8f161002733e93ca4527d22c1a0c5bb
fffffffff800000000000000000000	b72f70ebf3e3fda23f508eec76b42c02
ffffffffc000000000000000000000	6a9d965e6274143f25afdcfc88ffd77c
ffffffffe000000000000000000000	a0c74fd0b9361764ce91c5200b095357
fffffffff000000000000000000000	091d1fdc2bd2c346cd5046a8c6209146
fffffffff800000000000000000000	e2a37580116cfb71856254496ab0aca8
ffffffffc000000000000000000000	e0b3a00785917c7efc9adba322813571
ffffffffe000000000000000000000	733d41f4727b5ef0df4af4cf3cffa0cb
fffffffff000000000000000000000	a99ebb030260826f981ad3e64490aa4f
fffffffff800000000000000000000	73f34c7d3eae5e80082c1647524308ee
ffffffffc000000000000000000000	40ebd5ad082345b7a2097ccd3464da02
ffffffffe000000000000000000000	7cc4ae9a424b2cec90c97153c2457ec5
fffffffff000000000000000000000	54d632d03aba0bd0f91877ebdd4d09cb
fffffffff800000000000000000000	d3427be7e4d27cd54f5fe37b03cf0897
ffffffffc000000000000000000000	b2099795e88cc158fd75ea133d7e7fbe
ffffffffe000000000000000000000	a6cae46fb6fadfe7a2c302a34242817b
fffffffff000000000000000000000	026a7024d6a902e0b3ffccbaa910cc3f

ffffffffffffffffffff80000000000	156f07767a85a4312321f63968338a01
ffffffffffffffffffffc0000000000	15eec9ebf42b9ca76897d2cd6c5a12e2
ffffffffffffffffffffe0000000000	db0d3a6fdcc13f915e2b302ceeb70fd8
fffffffffffffffffffff0000000000	71dbf37e87a2e34d15b20e8f10e48924
fffffffffffffffffffff8000000000	c745c451e96ff3c045e4367c833e3b54
fffffffffffffffffffffc000000000	340da09c2dd11c3b679d08ccd27dd595
fffffffffffffffffffffe000000000	8279f7c0c2a03ee660c6d392db025d18
fffffffffffffffffffffff000000000	a4b2c7d8eba531ff47c5041a55fbd1ec
fffffffffffffffffffffff800000000	74569a2ca5a7bd5131ce8dc7cbfbf72f
fffffffffffffffffffffffc00000000	3713da0c0219b63454035613b5a403dd
fffffffffffffffffffffffe00000000	8827551ddcc9df23fa72a3de4e9f0b07
ffffffffffffffffffffffff00000000	2e3febfd625bfcd0a2c06eb460da1732
ffffffffffffffffffffffff80000000	ee82e6ba488156f76496311da6941deb
ffffffffffffffffffffffffc0000000	4770446f01d1f391256e85a1b30d89d3
ffffffffffffffffffffffffe0000000	af04b68f104f21ef2afb4767cf74143c
fffffffffffffffffffffffff0000000	cf3579a9ba38c8e43653173e14f3a4c6
fffffffffffffffffffffffff8000000	b3bba904f4953e09b54800af2f62e7d4
fffffffffffffffffffffffffc000000	fc4249656e14b29eb9c44829b4c59a46
fffffffffffffffffffffffffe000000	9b31568febe81cfc2e65af1c86d1a308
ffffffffffffffffffffffffff000000	9ca09c25f273a766db98a480ce8dfedc
ffffffffffffffffffffffffff800000	b909925786f34c3c92d971883c9fbedf
ffffffffffffffffffffffffffc00000	82647f1332fe570a9d4d92b2ee771d3b
ffffffffffffffffffffffffffe00000	3604a7e80832b3a99954bca6f5b9f501
fffffffffffffffffffffffffff00000	884607b128c5de3ab39a529a1ef51bef
fffffffffffffffffffffffffff80000	670cfa093d1dbdb23170414041024 35e
fffffffffffffffffffffffffffc0000	7a867195f3ce8769cbd336502fbb5130
fffffffffffffffffffffffffffe0000	52efcf64c72b2f7ca5b3c836b1078c15
ffffffffffffffffffffffffffff0000	4019250f6eefb2ac5ccbcae044e75c7e
ffffffffffffffffffffffffffff8000	022c4f6f5a017d292785627667ddef24
ffffffffffffffffffffffffffffc000	e9c21078a2eb7e03250f71000fa9e3ed
ffffffffffffffffffffffffffffe000	a13eaeeb9cd391da4e2b09490b3e7fad
fffffffffffffffffffffffffffff000	c958a171dca1d4ed53e1af1d380803a9
fffffffffffffffffffffffffffff800	21442e07a110667f2583eaeeee44dc8c
fffffffffffffffffffffffffffffc00	59bbb353cf1dd867a6e33737af655e99
fffffffffffffffffffffffffffffe00	43cd3b25375d0ce41087ff9fe2829639
ffffffffffffffffffffffffffffff00	6b98b17e80d1118e3516bd768b285a84
ffffffffffffffffffffffffffffff80	ae47ed3676ca0c08deea02d95b81db58
ffffffffffffffffffffffffffffffc0	34ec40dc20413795ed53628ea748720b
ffffffffffffffffffffffffffffffe0	4dc68163f8e9835473253542c8a65d46
fffffffffffffffffffffffffffffff0	2aabb999f43693175af65c6c612c46fb
fffffffffffffffffffffffffffffff8	e01f94499dac3547515c5b1d756f0f58
fffffffffffffffffffffffffffffffc	9d12435a46480ce00ea349f71799df9a
fffffffffffffffffffffffffffffffe	cef41d16d266bdfe46938ad7884cc0cf
ffffffffffffffffffffffffffffffff	b13db4da1f718bc6904797c82bcf2d32

D.3. Keysize = 256

KEY = 0000000000000000000000000000000000000000000000000000000000000000

PLAINTEXT or IV	CIPHERTEXT
8000000000000000000000000000000000000000000000000000000000000000	ddc6bf790c15760d8d9aeb6f9a75fd4e
c0000000000000000000000000000000000000000000000000000000000000000	0a6bdc6d4c1e6280301fd8e97ddbe601
e0000000000000000000000000000000000000000000000000000000000000000	9b80eefb7ebe2d2b16247aa0efc72f5d
f0000000000000000000000000000000000000000000000000000000000000000	7f2c5ece07a98d8bee13c51177395ff7
f8000000000000000000000000000000000000000000000000000000000000000	7818d800dcf6f4be1e0e94f403d1e4c2
fc0000000000000000000000000000000000000000000000000000000000000000	e74cd1c92f0919c35a0324123d6177d3
fe0000000000000000000000000000000000000000000000000000000000000000	8092a4dcf2da7e77e93bdd371dfed82e
ff0000000000000000000000000000000000000000000000000000000000000000	49af6b372135acef10132e548f217b17
ff8000000000000000000000000000000000000000000000000000000000000000	8bcd40f94ebb63b9f7909676e667f1e7
ffc0000000000000000000000000000000000000000000000000000000000000000	fe1cffb83f45dcfb38b29be438dbd3ab
ffe0000000000000000000000000000000000000000000000000000000000000000	0dc58a8d886623705aec15cb1e70dc0e
fff0000000000000000000000000000000000000000000000000000000000000000	c218faa16056bd0774c3e8d79c35a5e4
fff8000000000000000000000000000000000000000000000000000000000000000	047bba83f7aa841731504e012208fc9e
fffc0000000000000000000000000000000000000000000000000000000000000000	dc8f0e4915fd81ba70a331310882f6da
fffe0000000000000000000000000000000000000000000000000000000000000000	1569859ea6b7206c30bf4fd0cbfac33c
ffff0000000000000000000000000000000000000000000000000000000000000000	300ade92f88f48fa2df730ec16ef44cd
ffff8000000000000000000000000000000000000000000000000000000000000000	1fe6cc3c05965dc08eb0590c95ac71d0
fffffc0000000000000000000000000000000000000000000000000000000000000000	59e858eaaa97fec38111275b6cf5abc0
fffffe0000000000000000000000000000000000000000000000000000000000000000	2239455e7afe3b0616100288cc5a723b
fffff00000000000000000000000000000000000000000000000000000000000000000	3ee500c5c8d63479717163e55c5c4522
fffff80000000000000000000000000000000000000000000000000000000000000000	d5e38bf15f16d90e3e214041d774daa8
fffffc0000000000000000000000000000000000000000000000000000000000000000	b1f4066e6f4f187dfe5f2ad1b17819d0
fffffe0000000000000000000000000000000000000000000000000000000000000000	6ef4cc4de49b11065d7af2909854794a
ffffff0000000000000000000000000000000000000000000000000000000000000000	ac86bc606b6640c309e782f232bf367f
ffffff8000000000000000000000000000000000000000000000000000000000000000	36aff0ef7bf3280772cf4cac80a0d2b2
ffffffc0000000000000000000000000000000000000000000000000000000000000000	1f8eedea0f62a1406d58cfc3ecea72cf
ffffffe0000000000000000000000000000000000000000000000000000000000000000	abf4154a3375a1d3e6b1d454438f95a6
fffffff0000000000000000000000000000000000000000000000000000000000000000	96f96e9d607f6615fc192061ee648b07
fffffff8000000000000000000000000000000000000000000000000000000000000000	cf37cdaaa0d2d536c71857634c792064
fffffffc0000000000000000000000000000000000000000000000000000000000000000	fbd6640c80245c2b805373f130703127
fffffffe0000000000000000000000000000000000000000000000000000000000000000	8d6a8afe55a6e481badae0d146f436db
ffffffff0000000000000000000000000000000000000000000000000000000000000000	6a4981f2915e3e68af6c22385dd06756
ffffffff8000000000000000000000000000000000000000000000000000000000000000	42a1136e5f8d8d21d3101998642d573b
fffffffffc0000000000000000000000000000000000000000000000000000000000000000	9b471596dc69ae1586cee6158b0b0181
fffffffffe0000000000000000000000000000000000000000000000000000000000000000	753665c4af1eff33aa8b628bf8741cfd
fffffffff00000000000000000000000000000000000000000000000000000000000000000	9a682acf40be01f5b2a4193c9a82404d
fffffffff80000000000000000000000000000000000000000000000000000000000000000	54fafe26e4287f17d1935f87eb9ade01
fffffffffc0000000000000000000000000000000000000000000000000000000000000000	49d541b2e74cfe73e6a8e8225f7bd449
fffffffffe0000000000000000000000000000000000000000000000000000000000000000	11a45530f624ff6f76a1b3826626ff7b
ffffffffff0000000000000000000000000000000000000000000000000000000000000000	f96b0c4a8bc6c86130289f60b43b8fba

fffffffff8000000000000000000	48c7d0e80834ebdc35b6735f76b46c8b
fffffffffc0000000000000000000	2463531ab54d66955e73edc4cb8eaa45
fffffffffe0000000000000000000	ac9bd8e2530469134b9d5b065d4f565b
ffffffffff0000000000000000000	3f5f9106d0e52f973d4890e6f37e8a00
ffffffffff8000000000000000000	20ebc86f1304d272e2e207e59db639f0
ffffffffffc0000000000000000000	e67ae6426bf9526c972cff072b52252c
ffffffffffe0000000000000000000	1a518dddaf9efa0d002cc58d107edfc8
fffffffffff0000000000000000000	ead731af4d3a2fe3b34bed047942a49f
fffffffffff8000000000000000000	b1d4efe40242f83e93b6c8d7efb5eae9
fffffffffffc0000000000000000000	cd2b1fec11fd906c5c7630099443610a
fffffffffffe0000000000000000000	a1853fe47fe29289d153161d06387d21
ffffffffffff0000000000000000000	4632154179a555c17ea604d0889fab14
ffffffffffff8000000000000000000	dd27cac6401a022e8f38f9f93e774417
ffffffffffffc0000000000000000000	c090313eb98674f35f3123385fb95d4d
ffffffffffffe0000000000000000000	cc3526262b92f02edce548f716b9f45c
fffffffffffff0000000000000000000	c0838d1a2b16a7c7f0dfcc433c399c33
fffffffffffff8000000000000000000	0d9ac756eb297695eed4d382eb126d26
ffffffffffffffc000000000000000000	56ede9dda3f6f141bff1757fa689c3e1
ffffffffffffffe000000000000000000	768f520efe0f23e61d3ec8ad9ce91774
fffffffffffffff000000000000000000	b1144ddfa75755213390e7c596660490
fffffffffffffff800000000000000000	1d7c0c4040b355b9d107a99325e3b050
ffffffffffffffffc00000000000000000	d8e2bb1ae8ee3dcf5bf7d6c38da82a1a
ffffffffffffffffe00000000000000000	faf82d178af25a9886a47e7f789b98d7
fffffffffffffffff00000000000000000	9b58dbfd77fe5aca9cfc190cd1b82d19
fffffffffffffffff80000000000000000	77f392089042e478ac16c0c86a0b5db5
ffffffffffffffffffc0000000000000000	19f08e3420ee69b477ca1420281c4782
ffffffffffffffffffe0000000000000000	a1b19beee4e117139f74b3c53fdcb875
fffffffffffffffffff0000000000000000	a37a5869b218a9f3a0868d19aea0ad6a
fffffffffffffffffff8000000000000000	bc3594e865bcd0261b13202731f33580
ffffffffffffffffffffc000000000000000	811441ce1d309eee7185e8c752c07557
ffffffffffffffffffffe000000000000000	959971ce4134190563518e700b9874d1
fffffffffffffffffffff000000000000000	76b5614a042707c98e2132e2e805fe63
fffffffffffffffffffff800000000000000	7d9fa6a57530d0f036fec31c230b0cc6
ffffffffffffffffffffffc00000000000000	964153a83bf6989a4ba80daa91c3e081
ffffffffffffffffffffffe00000000000000	a013014d4ce8054cf2591d06f6f2f176
fffffffffffffffffffffff00000000000000	d1c5f6399bf382502e385eee1474a869
fffffffffffffffffffffff80000000000000	0007e20b8298ec354f0f5fe7470f36bd
ffffffffffffffffffffffffc0000000000000	b95ba05b332da61ef63a2b31fcad9879
ffffffffffffffffffffffffe0000000000000	4620a49bd967491561669ab25dce45f4
fffffffffffffffffffffffff0000000000000	12e71214ae8e04f0bb63d7425c6f14d5
fffffffffffffffffffffffff8000000000000	4cc42fc1407b008fe350907c092e80ac
ffffffffffffffffffffffffffc000000000000	08b244ce7cbc8ee97fbba808cb146fda
ffffffffffffffffffffffffffe000000000000	39b333e8694f21546ad1edd9d87ed95b
fffffffffffffffffffffffffff000000000000	3b271f8ab2e6e4a20ba8090f43ba78f3
fffffffffffffffffffffffffff800000000000	9ad983f3bf651cd0393f0a73cccdea50

fffffffffffffffffffc0000000000	8f476cbff75c1f725ce18e4bbcd19b32
fffffffffffffffffffe0000000000	905b6267f1d6ab5320835a133f096f2a
ffffffffffffffffffff0000000000	145b60d6d0193c23f4221848a892d61a
ffffffffffffffffffff8000000000	55cfb3fb6d75cad0445bbc8dafa25b0f
fffffffffffffffffffc000000000	7b8e7098e357ef71237d46d8b075b0f5
fffffffffffffffffffe000000000	2bf27229901eb40f2df9d8398d1505ae
ffffffffffffffffffff000000000	83a63402a77f9ad5c1e931a931ecd706
ffffffffffffffffffff800000000	6f8ba6521152d31f2bada1843e26b973
fffffffffffffffffffc00000000	e5c3b8e30fd2d8e6239b17b44bd23bbd
fffffffffffffffffffe00000000	1ac1f7102c59933e8b2ddc3f14e94baa
ffffffffffffffffffff00000000	21d9ba49f276b45f11af8fc71a088e3d
ffffffffffffffffffff80000000	649f1cddc3792b4638635a392bc9bade
fffffffffffffffffffc0000000	e2775e4b59c1bc2e31a2078c11b5a08c
fffffffffffffffffffe0000000	2be1fae5048a25582a679ca10905eb80
ffffffffffffffffffff0000000	da86f292c6f41ea34fb2068df75ecc29
ffffffffffffffffffff8000000	220df19f85d69b1b562fa69a3c5beca5
fffffffffffffffffffc000000	1f11d5d0355e0b556ccdb6c7f5083b4d
fffffffffffffffffffe000000	62526b78be79cb384633c91f83b4151b
ffffffffffffffffffff000000	90ddbcb950843592dd47bbef00fdc876
ffffffffffffffffffff800000	2fd0e41c5b8402277354a7391d2618e2
fffffffffffffffffffc00000	3cdf13e72dee4c581bafec70b85f9660
fffffffffffffffffffe00000	afa2ffc137577092e2b654fa199d2c43
ffffffffffffffffffff00000	8d683ee63e60d208e343ce48dbc44cac
ffffffffffffffffffff80000	705a4ef8ba2133729c20185c3d3a4763
fffffffffffffffffffc0000	0861a861c3db4e94194211b77ed761b9
fffffffffffffffffffe0000	4b00c27e8b26da7eab9d3a88dec8b031
ffffffffffffffffffff0000	5f397bf03084820cc8810d52e5b666e9
ffffffffffffffffffff8000	63fafabb72c07bfbd3ddc9b1203104b8
fffffffffffffffffffc000	683e2140585b18452dd4ffbb93c95df9
fffffffffffffffffffe000	286894e48e537f8763b56707d7d155c8
ffffffffffffffffffff000	a423deabc173dcf7e2c4c53e77d37cd1
ffffffffffffffffffff800	eb8168313e1cfdfdb5e986d5429cf172
fffffffffffffffffffc00	27127daafc9accd2fb334ec3eba52323
fffffffffffffffffffe00	ee0715b96f72e3f7a22a5064fc592f4c
ffffffffffffffffffff00	29ee526770f2a11dcfa989d1ce88830f
ffffffffffffffffffff80	0493370e054b09871130fe49af730a5a
fffffffffffffffffffc0	9b7b940f6c509f9e44a4ee140448ee46
fffffffffffffffffffe0	2915be4a1ecfdcbe3e023811a12bb6c7
ffffffffffffffffffff0	7240e524bc51d8c4d440b1be55d1062c
ffffffffffffffffffff8	da63039d38cb4612b2dc36ba26684b93
fffffffffffffffffffc	0f59cb5a4b522e2ac56c1a64f558ad9a
fffffffffffffffffffe	7bfe9d876c6d63c1d035da8fe21c409d
ffffffffffffffffffff	acdace8078a32b1a182bfa4987ca1347

Appendix E. VarKey Known Answer Test Values

E.1. Keysize = 128

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
80000000000000000000000000000000	0edd33d3c621e546455bd8ba1418bec8
c0000000000000000000000000000000	4bc3f883450c113c64ca42e1112a9e87
e0000000000000000000000000000000	72a1da770f5d7ac4c9ef94d822affd97
f0000000000000000000000000000000	970014d634e2b7650777e8e84d03ccd8
f8000000000000000000000000000000	f17e79aed0db7e279e955b5f493875a7
fc000000000000000000000000000000	9ed5a75136a940d0963da379db4af26a
fe000000000000000000000000000000	c4295f83465c7755e8fa364bac6a7ea5
ff000000000000000000000000000000	b1d758256b28fd850ad4944208cf1155
ff800000000000000000000000000000	42ffb34c743de4d88ca38011c990890b
ffc00000000000000000000000000000	9958f0ecea8b2172c0c1995f9182c0f3
ffe00000000000000000000000000000	956d7798fac20f82a8823f984d06f7f5
fff00000000000000000000000000000	a01bf44f2d16be928ca44aaf7b9b106b
fff80000000000000000000000000000	b5f1a33e50d40d103764c76bd4c6b6f8
fffc0000000000000000000000000000	2637050c9fc0d4817e2d69de878aee8d
fffe0000000000000000000000000000	113ecbe4a453269a0dd26069467fb5b5
ffff0000000000000000000000000000	97d0754fe68f11b9e375d070a608c884
ffff8000000000000000000000000000	c6a0b3e998d05068a5399778405200b4
ffffc000000000000000000000000000	df556a33438db87bc41b1752c55e5e49
ffffe000000000000000000000000000	90fb128d3a1af6e548521bb962bf1f05
fffff000000000000000000000000000	26298e9c1db517c215fadfb7d2a8d691
fffff800000000000000000000000000	a6cb761d61f8292d0df393a279ad0380
fffffc000000000000000000000000000	12acd89b13cd5f8726e34d44fd486108
fffffe000000000000000000000000000	95b1703fc57ba09fe0c3580febdd7ed4
ffffff000000000000000000000000000	de11722d893e9f9121c381becc1da59a
ffffff800000000000000000000000000	6d114ccb27bf391012e8974c546d9bf2
ffffffc000000000000000000000000000	5ce37e17eb4646ecfac29b9cc38d9340
ffffffe000000000000000000000000000	18c1b6e2157122056d0243d8a165cddb
fffffff000000000000000000000000000	99693e6a59d1366c74d823562d7e1431
fffffff800000000000000000000000000	6c7c64dc84a8bba758ed17eb025a57e3
fffffffc000000000000000000000000000	e17bc79f30eaab2fac2cbbe3458d687a
fffffffe000000000000000000000000000	1114bc2028009b923f0b01915ce5e7c4
ffffffff000000000000000000000000000	9c28524a16a1e1c1452971caa8d13476
ffffffff800000000000000000000000000	ed62e16363638360fdd6ad62112794f0
ffffffffc000000000000000000000000000	5a8688f0b2a2c16224c161658ffd4044
ffffffffe000000000000000000000000000	23f710842b9bb9c32f26648c786807ca
fffffffff000000000000000000000000000	44a98bf11e163f632c47ec6a49683a89
fffffffff800000000000000000000000000	0f18aff94274696d9b61848bd50ac5e5
fffffffffc000000000000000000000000000	82408571c3e2424540207f833b6dda69

fffffffffe0000000000000000000000	303ff996947f0c7d1f43c8f3027b9b75
fffffffffe0000000000000000000000	7df4daf4ad29a3615a9b6ece5c99518a
fffffffffe8000000000000000000000	c72954a48d0774db0b4971c526260415
fffffffffe8000000000000000000000	1df9b76112dc6531e07d2cfda04411f0
fffffffffe8000000000000000000000	8e4d8e699119e1fc87545a647fb1d34f
fffffffffe8000000000000000000000	e6c4807ae11f36f091c57d9fb68548d1
fffffffffe8000000000000000000000	8ebf73aad49c82007f77a5c1ccec6ab4
fffffffffe8000000000000000000000	4fb288cc2040049001d2c7585ad123fc
fffffffffe8000000000000000000000	04497110efb9dceb13e2b13fb4465564
fffffffffe8000000000000000000000	75550e6cb5a88e49634c9ab69eda0430
fffffffffe8000000000000000000000	b6768473ce9843ea66a81405dd50b345
fffffffffe8000000000000000000000	cb2f430383f9084e03a653571e065de6
fffffffffe8000000000000000000000	ff4e66c07bae3e79fb7d210847a3b0ba
fffffffffe8000000000000000000000	7b90785125505fad59b13c186dd66ce3
fffffffffe8000000000000000000000	8b527a6aebdaec9eaef8eda2cb7783e5
fffffffffe8000000000000000000000	43fdaf53ebbc9880c228617d6a9b548b
fffffffffe8000000000000000000000	53786104b9744b98f052c46f1c850d0b
fffffffffe8000000000000000000000	b5ab3013dd1e61df06cbaf34ca2aee78
fffffffffe8000000000000000000000	7470469be9723030fdcc73a8cd4fbb10
fffffffffe8000000000000000000000	a35a63f5343ebe9ef8167bcb48ad122e
fffffffffe8000000000000000000000	fd8687f0757a210e9fdf181204c30863
fffffffffe8000000000000000000000	7a181e84bd5457d26a88fbae96018fb0
fffffffffe8000000000000000000000	653317b9362b6f9b9e1a580e68d494b5
fffffffffe8000000000000000000000	995c9dc0b689f03c45867b5faa5c18d1
fffffffffe8000000000000000000000	77a4d96d56dda398b9aabecfc75729fd
fffffffffe8000000000000000000000	84be19e053635f09f2665e7bae85b42d
fffffffffe8000000000000000000000	32cd652842926aea4aa6137bb2be2b5e
fffffffffe8000000000000000000000	493d4a4f38ebb337d10aa84e9171a554
fffffffffe8000000000000000000000	d9bff7ff454b0ec5a4a2a69566e2cb84
fffffffffe8000000000000000000000	3535d565ace3f31eb249ba2cc6765d7a
fffffffffe8000000000000000000000	f60e91fc3269eecf3231c6e9945697c6
fffffffffe8000000000000000000000	ab69cfadf51f8e604d9cc37182f6635a
fffffffffe8000000000000000000000	7866373f24a0b6ed56e0d96fcdafb877
fffffffffe8000000000000000000000	1ea448c2aac954f5d812e9d78494446a
fffffffffe8000000000000000000000	acc5599dd8ac02239a0fef4a36dd1668
fffffffffe8000000000000000000000	d8764468bb103828cf7e1473ce895073
fffffffffe8000000000000000000000	1b0d02893683b9f180458e4aa6b73982
fffffffffe8000000000000000000000	96d9b017d302df410a937dcdb8bb6e43
fffffffffe8000000000000000000000	ef1623cc44313cff440b1594a7e21cc6
fffffffffe8000000000000000000000	284ca2fa35807b8b0ae4d19e11d7dbd7
fffffffffe8000000000000000000000	f2e976875755f9401d54f36e2a23a594
fffffffffe8000000000000000000000	ec198a18e10e532403b7e20887c8dd80
fffffffffe8000000000000000000000	545d50ebd919e4a6949d96ad47e46a80
fffffffffe8000000000000000000000	dbdfb527060e0a71009c7bb0c68f1d44
fffffffffe8000000000000000000000	9cfa1322ea33da2173a024f2ff0d896d

ffffffffffffffffffff00000000000	8785b1a75b0f3bd958dcd0e29318c521
ffffffffffffffffffff80000000000	38f67b9e98e4a97b6df030a9fcdd0104
fffffffffffffffffffc0000000000	192afffb2c880e82b05926d0fc6c448b
fffffffffffffffffffe0000000000	6a7980ce7b105cf530952d74daaf798c
ffffffffffffffffffff0000000000	ea3695e1351b9d6858bd958cf513ef6c
ffffffffffffffffffff8000000000	6da0490ba0ba0343b935681d2cce5ba1
fffffffffffffffffffc000000000	f0ea23af08534011c60009ab29ada2f1
fffffffffffffffffffe000000000	ff13806cf19cc38721554d7c0fcdcd4b
ffffffffffffffffffff000000000	6838af1f4f69bae9d85dd188dcdf0688
ffffffffffffffffffff800000000	36cf44c92d550bfb1ed28ef583ddf5d7
fffffffffffffffffffc00000000	d06e3195b5376f109d5c4ec6c5d62ced
fffffffffffffffffffe00000000	c440de014d3d610707279b13242a5c36
ffffffffffffffffffff00000000	f0c5c6ffa5e0bd3a94c88f6b6f7c16b9
ffffffffffffffffffff80000000	3e40c3901cd7effc22bffc35dee0b4d9
fffffffffffffffffffc0000000	b63305c72bedfab97382c406d0c49bc6
fffffffffffffffffffe0000000	36bbaab22a6bd4925a99a2b408d2dbae
ffffffffffffffffffff0000000	307c5b8fcd0533ab98bc51e27a6ce461
ffffffffffffffffffff8000000	829c04ff4c07513c0b3ef05c03e337b5
fffffffffffffffffffc000000	f17af0e895dda5eb98efc68066e84c54
fffffffffffffffffffe000000	277167f3812afff1ffacb4a934379fc3
ffffffffffffffffffff000000	2cb1dc3a9c72972e425ae2ef3eb597cd
ffffffffffffffffffff800000	36aeaa3a213e968d4b5b679d3a2c97fe
fffffffffffffffffffc00000	9241daca4fdd034a82372db50e1a0f3f
fffffffffffffffffffe00000	c14574d9cd00cf2b5a7f77e53cd57885
ffffffffffffffffffff00000	793de39236570aba83ab9b737cb521c9
ffffffffffffffffffff80000	16591c0f27d60e29b85a96c33861a7ef
fffffffffffffffffffc0000	44fb5c4d4f5cb79be5c174a3b1c97348
fffffffffffffffffffe0000	674d2b61633d162be59dde04222f4740
ffffffffffffffffffff0000	b4750ff263a65e1f9e924ccfd98f3e37
ffffffffffffffffffff8000	62d0662d6eaeddedebae7f7ea3a4f6b6
fffffffffffffffffffc000	70c46bb30692be657f7eaa93ebad9897
fffffffffffffffffffe000	323994cfb9da285a5d9642e1759b224a
ffffffffffffffffffff000	1dbf57877b7b17385c85d0b54851e371
ffffffffffffffffffff800	dfa5c097cdc1532ac071d57b1d28d1bd
fffffffffffffffffffc00	3a0c53fa37311fc10bd2a9981f513174
fffffffffffffffffffe00	ba4f970c0a25c41814bdae2e506be3b4
ffffffffffffffffffff00	2dce3acb727cd13ccd76d425ea56e4f6
ffffffffffffffffffff80	5160474d504b9b3eefb68d35f245f4b3
fffffffffffffffffffc0	41a8a947766635dec37553d9a6c0cbb7
fffffffffffffffffffe0	25d6cfe6881f2bf497dd14cd4ddf445b
ffffffffffffffffffff0	41c78c135ed9e98c096640647265da1e
ffffffffffffffffffff8	5a4d404d8917e353e92a21072c3b2305
fffffffffffffffffffc	02bc96846b3fdc71643f384cd3cc3eaf
fffffffffffffffffffe	9ba4a9143f4e5d4048521c4f8877d88e
ffffffffffffffffffff	a1f6258c877d5fcd8964484538bfc92c

E.2. Keysize = 192

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
800000000000000000000000000000000000000000000000	de885dc87f5a92594082d02cc1e1b42c
c000000000000000000000000000000000000000000000000	132b074e80f2a597bf5febd8ea5da55e
e000000000000000000000000000000000000000000000000	6eccedf8de592c22fb81347b79f2db1f
f000000000000000000000000000000000000000000000000	180b09f267c45145db2f826c2582d35c
f800000000000000000000000000000000000000000000000	edd807ef7652d7eb0e13c8b5e15b3bc0
fc000000000000000000000000000000000000000000000000	9978bcf8dd8fd72241223ad24b31b8a4
fe000000000000000000000000000000000000000000000000	5310f654343e8f27e12c83a48d24ff81
ff000000000000000000000000000000000000000000000000	833f71258d53036b02952c76c744f5a1
ff800000000000000000000000000000000000000000000000	eba83ff200cff9318a92f8691a06b09f
ffc000000000000000000000000000000000000000000000000	ff620ccbe9f3292abdf2176b09f04eba
ffe000000000000000000000000000000000000000000000000	7ababc4b3f516c9aafb35f4140b548f9
fff000000000000000000000000000000000000000000000000	aa187824d9c4582b0916493ecbde8c57
fff800000000000000000000000000000000000000000000000	1c0ad553177fd5ea1092c9d626a29dc4
fffc000000000000000000000000000000000000000000000000	a5dc46c37261194124ecaebd680408ec
fffe000000000000000000000000000000000000000000000000	e4f2f2ae23e9b10bacfa58601531ba54
ffff000000000000000000000000000000000000000000000000	b7d67cf1a1e91e8ff3a57a172c7bf412
ffff800000000000000000000000000000000000000000000000	26706be06967884e847d137128ce47b3
ffffc000000000000000000000000000000000000000000000000	b2f8b409b0585909aad3a7b5a219072a
ffffe000000000000000000000000000000000000000000000000	5e4b7bff0290c78344c54a23b722cd20
fffff000000000000000000000000000000000000000000000000	07093657552d4414227ce161e9ebf7dd

fffff800000000000000000000000000000000000000000000000000000000	e1af1e7d8bc225ed4dffb771ecbb9e67
fffffc000000000000000000000000000000000000000000000000000000000	ef6555253635d8432156cfd9c11b145a
fffffe000000000000000000000000000000000000000000000000000000000	fb4035074a5d4260c90cbd6da6c3fceb
ffffff000000000000000000000000000000000000000000000000000000000	446ee416f9ad1c103eb0cc96751c88e1
ffffff800000000000000000000000000000000000000000000000000000000	198ae2a4637ac0a7890a8fd1485445c9
ffffffc000000000000000000000000000000000000000000000000000000000	562012ec8faded0825fb2fa70ab30cbd
ffffffe000000000000000000000000000000000000000000000000000000000	cc8a64b46b5d88bf7f247d4dbaf38f05
fffffff000000000000000000000000000000000000000000000000000000000	a168253762e2cc81b42d1e5001762699
fffffff800000000000000000000000000000000000000000000000000000000	1b41f83b38ce5032c6cd7af98cf62061
fffffffc000000000000000000000000000000000000000000000000000000000	61a89990cd1411750d5fb0dc988447d4
fffffffe000000000000000000000000000000000000000000000000000000000	b5accc8ed629edf8c68a539183b1ea82
ffffffff000000000000000000000000000000000000000000000000000000000	b16fa71f846b81a13f361c43a851f290
ffffffff800000000000000000000000000000000000000000000000000000000	4fad6efdff5975aee7692234bcd54488
ffffffffc000000000000000000000000000000000000000000000000000000000	ebfdb05a783d03082dfe5fdd80a00b17
ffffffffe000000000000000000000000000000000000000000000000000000000	eb81b584766997af6ba5529d3bdd8609
fffffffff000000000000000000000000000000000000000000000000000000000	0cf4ff4f49c8a0ca060c443499e29313
fffffffff800000000000000000000000000000000000000000000000000000000	cc4ba8a8e029f8b26d8afff9df133bb6
fffffffffc000000000000000000000000000000000000000000000000000000000	fefebf64360f38e4e63558f0ffc550c3
fffffffffe000000000000000000000000000000000000000000000000000000000	12ad98cbf725137d6a8108c2bed99322
ffffffffff000000000000000000000000000000000000000000000000000000000	6afaa996226198b3e2610413ce1b3f78
ffffffffff800000000000000000000000000000000000000000000000000000000	2a8ce6747a7e39367828e290848502d9
ffffffffffc000000000000000000000000000000000000000000000000000000000	223736e8b8f89ca1e37b6deab40facf1
ffffffffffe000000000000000000000000000000000000000000000000000000000	c0f797e50418b95fa6013333917a9480

fffffffffff000000000000000000000000000000000000	a758de37c2ece2a02c73c01fedc9a132
fffffffffff800000000000000000000000000000000000	3a9b87ae77bae706803966c66c73adbd
ffffffffffc000000000000000000000000000000000000	d365ab8df8ffd782e358121a4a4fc541
ffffffffffe000000000000000000000000000000000000	c8dcd9e6f75e6c36c8daee0466f0ed74
fffffffffff000000000000000000000000000000000000	c79a637beb1c0304f14014c037e736dd
fffffffffff800000000000000000000000000000000000	105f0a25e84ac930d996281a5f954dd9
ffffffffffc000000000000000000000000000000000000	42e4074b2927973e8d17ffa92f7fe615
ffffffffffe000000000000000000000000000000000000	4fe2a9d2c1824449c69e3e0398f12963
fffffffffff000000000000000000000000000000000000	b7f29c1e1f62847a15253b28a1e9d712
fffffffffff800000000000000000000000000000000000	36ed5d29b903f31e8983ef8b0a2bf990
ffffffffffc000000000000000000000000000000000000	27b8070270810f9d023f9dd7ff3b4aa2
ffffffffffe000000000000000000000000000000000000	94d46e155c1228f61d1a0db4815ecc4b
fffffffffff000000000000000000000000000000000000	ca6108d1d98071428eeceef1714b96dd
fffffffffff800000000000000000000000000000000000	dc5b25b71b6296cf73dd2cdcac2f70b1
ffffffffffc000000000000000000000000000000000000	44aba95e8a06a2d9d3530d2677878c80
ffffffffffe000000000000000000000000000000000000	a570d20e89b467e8f5176061b81dd396
fffffffffff000000000000000000000000000000000000	758f4467a5d8f1e7307dc30b34e404f4
fffffffffff800000000000000000000000000000000000	bcea28e9071b5a2302970ff352451bc5
ffffffffffc000000000000000000000000000000000000	7523c00bc177d331ad312e09c9015c1c
ffffffffffe000000000000000000000000000000000000	ccac61e3183747b3f5836da21a1bc4f4
fffffffffff000000000000000000000000000000000000	707b075791878880b44189d3522b8c30
fffffffffff800000000000000000000000000000000000	7132d0c0e4a07593cf12ebb12be7688c
ffffffffffc000000000000000000000000000000000000	effbac1644deb0c784275fe56e19ead3

fffffffffffffffe0000000000000000	a005063f30f4228b374e2459738f26bb
ffffffffffffffff0000000000000000	29975b5f48bb68fcbbc7cea93b452ed7
ffffffffffffffff8000000000000000	cf3f2576e2afedc74bb1ca7eeec1c0e7
fffffffffffffffc0000000000000000	07c403f5f966e0e3d9f296d6226dca28
fffffffffffffffe0000000000000000	c8c20908249ab4a34d6dd0a31327ff1a
ffffffffffffffff0000000000000000	c0541329ecb6159ab23b7fc5e6a21bca
ffffffffffffffff8000000000000000	7aa1acf1a2ed9ba72bc6deb31d88b863
fffffffffffffffc0000000000000000	808bd8eddabb6f3bf0d5a8a27be1fe8a
fffffffffffffffe0000000000000000	273c7d7685e14ec66bbb96b8f05b6ddd
ffffffffffffffff0000000000000000	32752eefc8c2a93f91b6e73eb07cca6e
ffffffffffffffff8000000000000000	d893e7d62f6ce502c64f75e281f9c000
fffffffffffffffc0000000000000000	8dfd999be5d0cfa35732c0ddc88ff5a5
fffffffffffffffe0000000000000000	02647c76a300c3173b841487eb2bae9f
ffffffffffffffff0000000000000000	172df8b02f04b53adab028b4e01acd87
ffffffffffffffff8000000000000000	054b3bf4998aeb05afd87ec536533a36
fffffffffffffffc0000000000000000	3783f7bf44c97f065258a666cae03020
fffffffffffffffe0000000000000000	aad4c8a63f80954104de7b92cede1be1
ffffffffffffffff0000000000000000	cbfe61810fd5467ccdacb75800f3ac07
ffffffffffffffff8000000000000000	830d8a2590f7d8e1b55a737f4af45f34
fffffffffffffffc0000000000000000	fffcd4683f858058e74314671d43fa2c
fffffffffffffffe0000000000000000	523d0babbb82f46ebc9e70b1cd41ddd0
ffffffffffffffff0000000000000000	344aab37080d7486f7d542a309e53eed
ffffffffffffffff8000000000000000	56c5609d0906b23ab9caca816f5dbebd

fffffffffffffffffffffc0000000000000000000000000	7026026eedd91adc6d831cdf9894bdc6
fffffffffffffffffffffe0000000000000000000000000	88330baa4f2b618fc9d9b021bf503d5a
ffffffffffffffffffffff0000000000000000000000000	fc9e0ea22480b0bac935c8a8ebefcdcf
ffffffffffffffffffffff8000000000000000000000000	29ca779f398fb04f867da7e8a44756cb
fffffffffffffffffffffc0000000000000000000000000	51f89c42985786bfc43c6df8ada36832
fffffffffffffffffffffe0000000000000000000000000	6ac1de5fb8f21d874e91c53b560c50e3
ffffffffffffffffffffff0000000000000000000000000	03aa9058490eda306001a8a9f48d0ca7
ffffffffffffffffffffff8000000000000000000000000	e34ec71d6128d4871865d617c30b37e3
fffffffffffffffffffffc0000000000000000000000000	14be1c535b17cabd0c4d93529d69bf47
fffffffffffffffffffffe0000000000000000000000000	c9ef67756507beec9dd3862883478044
ffffffffffffffffffffff0000000000000000000000000	40e231fa5a5948ce2134e92fc0664d4b
ffffffffffffffffffffff8000000000000000000000000	03194b8e5dda5530d0c678c0b48f5d92
fffffffffffffffffffffc0000000000000000000000000	90bd086f237cc4fd99f4d76bde6b4826
fffffffffffffffffffffe0000000000000000000000000	19259761ca17130d6ed86d57cd7951ee
ffffffffffffffffffffff0000000000000000000000000	d7cbb3f34b9b450f24b0e8518e54da6d
ffffffffffffffffffffff8000000000000000000000000	725b9caebe9f7f417f4068d0d2ee20b3
fffffffffffffffffffffc0000000000000000000000000	9d924b934a90ce1fd39b8a9794f82672
fffffffffffffffffffffe0000000000000000000000000	c50562bf094526a91c5bc63c0c224995
ffffffffffffffffffffff0000000000000000000000000	d2f11805046743bd74f57188d9188df7
ffffffffffffffffffffff8000000000000000000000000	8dd274bd0f1b58ae345d9e7233f9b8f3
fffffffffffffffffffffc0000000000000000000000000	9d6bdc8f4ce5feb0f3bed2e4b9a9bb0b
fffffffffffffffffffffe0000000000000000000000000	fd5548bcf3f42565f7efa94562528d46
ffffffffffffffffffffff0000000000000000000000000	d2ccaebd3a4c3e80b063748131ba4a71

ffffffffffffffffffffffffff8000000000000000000	e03cb23d9e11c9d93f117e9c0a91b5760
ffffffffffffffffffffffffffc0000000000000000000	78f933a2081ac1db84f69d10f4523fe0
ffffffffffffffffffffffffffe0000000000000000000	4061f7412ed320de0edc8851c2e2436f
fffffffffffffffffffffffffff0000000000000000000	9064ba1cd04ce6bab98474330814b4d4
ffffffffffffffffffffffffff8000000000000000000	48391bffb9cfff80ac238c886ef0a461
ffffffffffffffffffffffffffc000000000000000000	b8d2a67df5a999fdbf93edd0343296c9
ffffffffffffffffffffffffffe000000000000000000	aaca7367396b69a221bd632bea386eec
fffffffffffffffffffffffffff000000000000000000	a80fd5020dfe65f5f16293ec92c6fd89
fffffffffffffffffffffffffff8000000000000000000	2162995b8217a67f1abc342e146406f8
fffffffffffffffffffffffffffc000000000000000000	c6a6164b7a60bae4e986ffac28dfadd9
fffffffffffffffffffffffffffe000000000000000000	64e0d7f900e3d9c83e4b8f96717b2146
ffffffffffffffffffffffffffff000000000000000000	1ad2561de8c1232f5d8dbab4739b6cbb
ffffffffffffffffffffffffffff800000000000000000	279689e9a557f58b1c3bf40c97a90964
ffffffffffffffffffffffffffffc000000000000000000	c4637e4a5e6377f9cc5a8638045de029
ffffffffffffffffffffffffffffe000000000000000000	492e607e5aea4688594b45f3aee3df90
fffffffffffffffffffffffffffff000000000000000000	e8c4e4381feec74054954c05b777a00a
fffffffffffffffffffffffffffff800000000000000000	91549514605f38246c9b724ad839f01d
fffffffffffffffffffffffffffffc00000000000000000	74b24e3b6fefe40a4f9ef7ac6e44d76a
fffffffffffffffffffffffffffffe00000000000000000	2437a683dc5d4b52abb4a123a8df86c6
fffffffffffffffffffffffffffff000000000000000000	bb2852c891c5947d2ed44032c421b85f
fffffffffffffffffffffffffffff800000000000000000	1b9f5fbd5e8a4264c0a85b80409afa5e
fffffffffffffffffffffffffffffc0000000000000000	30dab809f85a917fe924733f424ac589
fffffffffffffffffffffffffffffe0000000000000000	eaef5c1f8d605192646695ceadc65f32

ffffffffffffffffffffffffffffff ff00000000000000	b8aa90040b4c15a12316b78e0f9586fc
ffffffffffffffffffffffffffffff ff80000000000000	97fac8297ceaabc87d454350601e0673
ffffffffffffffffffffffffffffff ffc0000000000000	9b47ef567ac28dfe488492f157e2b2e0
ffffffffffffffffffffffffffffff ffe0000000000000	1b8426027ddb962b5c5ba7eb8bc9ab63
ffffffffffffffffffffffffffffff fff0000000000000	e917fc77e71992a12dbe4c18068bec82
ffffffffffffffffffffffffffffff fff8000000000000	dceebbc98840f8ae6daf76573b7e56f4
ffffffffffffffffffffffffffffff fffc000000000000	4e11a9f74205125b61e0aee047eca20d
ffffffffffffffffffffffffffffff fffe000000000000	f60467f55a1f17eab88e800120cbc284
ffffffffffffffffffffffffffffff ffff000000000000	d436649f600b449ee276530f0cd83c11
ffffffffffffffffffffffffffffff ffff800000000000	3bc0e3656a9e3ac7cd378a737f53b637
ffffffffffffffffffffffffffffff ffffc00000000000	6bacae63d33b928aa8380f8d54d88c17
ffffffffffffffffffffffffffffff ffffe00000000000	8935ffbc75ae6251bf8e859f085adcb9
ffffffffffffffffffffffffffffff fffff00000000000	93dc4970fe35f67747cb0562c06d875a
ffffffffffffffffffffffffffffff fffff80000000000	14f9df858975851797ba604fb0d16cc7
ffffffffffffffffffffffffffffff fffffc0000000000	02ea0c98dca10b38c21b3b14e8d1b71f
ffffffffffffffffffffffffffffff fffffe0000000000	8f091b1b5b0749b2adc803e63dda9b72
ffffffffffffffffffffffffffffff ffffff0000000000	05b389e3322c6da08384345a4137fd08
ffffffffffffffffffffffffffffff ffffff8000000000	381308c438f35b399f10ad71b05027d8
ffffffffffffffffffffffffffffff ffffffc000000000	68c230fcfa9279c3409fc423e2acbe04
ffffffffffffffffffffffffffffff ffffffe000000000	1c84a475acb011f3f59f4f46b76274c0
ffffffffffffffffffffffffffffff fffffff000000000	45119b68cb3f8399ee60066b5611a4d7
ffffffffffffffffffffffffffffff fffffff800000000	9423762f527a4060ffca312dcca22a16
ffffffffffffffffffffffffffffff fffffffc00000000	f361a2745a33f056a5ac6ace2f08e344

ffffffffffffffffffffffffffffffff fffffffe00000000	5ef145766eca849f5d011536a6557fdb
ffffffffffffffffffffffffffffffff ffffffff00000000	c9af27b2c89c9b4cf4a0c4106ac80318
ffffffffffffffffffffffffffffffff ffffffff80000000	fb9c4f16c621f4eab7e9ac1d7551dd57
ffffffffffffffffffffffffffffffff ffffffffc0000000	138e06fba466fa70854d8c2e524cffb2
ffffffffffffffffffffffffffffffff ffffffffe0000000	fb4bc78b225070773f04c40466d4e90c
ffffffffffffffffffffffffffffffff fffffffff0000000	8b2cbff1ed0150feda8a4799be94551f
ffffffffffffffffffffffffffffffff fffffffff8000000	08b30d7b3f27962709a36bcadfb974bd
ffffffffffffffffffffffffffffffff ffffffffc000000	fdf6d32e044d77adcf37fb97ac213326
ffffffffffffffffffffffffffffffff ffffffffe000000	93cb284ecdcfd781a8afe32077949e88
ffffffffffffffffffffffffffffffff fffffffff000000	7b017bb02ec87b2b94c96e40a26fc71a
ffffffffffffffffffffffffffffffff fffffffff800000	c5c038b6990664ab08a3aaa5df9f3266
ffffffffffffffffffffffffffffffff ffffffffc00000	4b7020be37fab6259b2a27f4ec551576
ffffffffffffffffffffffffffffffff ffffffffe00000	60136703374f64e860b48ce31f930716
ffffffffffffffffffffffffffffffff fffffffff00000	8d63a269b14d506ccc401ab8a9f1b591
ffffffffffffffffffffffffffffffff fffffffff80000	d317f81dc6aa454aee4bd4a5a5cff4bd
ffffffffffffffffffffffffffffffff ffffffffc0000	dddececd5354f04d530d76ed884246eb
ffffffffffffffffffffffffffffffff ffffffffe0000	41c5205cc8fd8eda9a3cffd2518f365a
ffffffffffffffffffffffffffffffff fffffffff0000	cf42fb474293d96eca9db1b37b1ba676
ffffffffffffffffffffffffffffffff fffffffff8000	a231692607169b4ecdead5cd3b10db3e
ffffffffffffffffffffffffffffffff ffffffffc000	ace4b91c9c669e77e7acacd19859ed49
ffffffffffffffffffffffffffffffff ffffffffe000	75db7cfd4a7b2b62ab78a48f3ddaf4af
ffffffffffffffffffffffffffffffff fffffffff000	c1faba2d46e259cf480d7c38e4572a58
ffffffffffffffffffffffffffffffff fffffffff800	241c45bc6ae16dee6eb7bea128701582

ffffffffffffffffffffffffffffffff ffffffffffffc00	8fd03057cf1364420c2b78069a3e2502
ffffffffffffffffffffffffffffffff fffffffffffe00	ddb505e6cc1384cbaec1df90b80beb20
ffffffffffffffffffffffffffffffff ffffffffffff00	5674a3bed27bf4bd3622f9f5fe208306
ffffffffffffffffffffffffffffffff ffffffffffff80	b687f26a89cfbfbb8e5eeac54055315e
ffffffffffffffffffffffffffffffff ffffffffffffc0	0547dd32d3b29ab6a4caeb606c5b6f78
ffffffffffffffffffffffffffffffff ffffffffffffe0	186861f8bc5386d31fb77f720c3226e6
ffffffffffffffffffffffffffffffff fffffffffffff0	eacf1e6c4224efb38900b185ab1dfd42
ffffffffffffffffffffffffffffffff fffffffffffff8	d241aab05a42d319de81d874f5c7b90d
ffffffffffffffffffffffffffffffff fffffffffffffc	5eb9bc759e2ad8d2140a6c762ae9e1ab
ffffffffffffffffffffffffffffffff fffffffffffffe	018596e15e78e2c064159defce5f3085
ffffffffffffffffffffffffffffffff ffffffffffffff	dd8a493514231cbf56eccee4c40889fb

E.3. Keysize = 256

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
80000000000000000000000000000000 00000000000000000000000000000000	e35a6dcb19b201a01ebcfa8aa22b5759
c0000000000000000000000000000000 00000000000000000000000000000000	b29169cdcf2d83e838125a12ee6aa400
e0000000000000000000000000000000 00000000000000000000000000000000	d8f3a72fc3cdf74dfaf6c3e6b97b2fa6
f0000000000000000000000000000000 00000000000000000000000000000000	1c777679d50037c79491a94da76a9a35
f8000000000000000000000000000000 00000000000000000000000000000000	9cf4893ecafa0a0247a898e040691559
fc000000000000000000000000000000 00000000000000000000000000000000	8fbb41370373532631 0a269bd3aa94b2
fe000000000000000000000000000000 00000000000000000000000000000000	60e32246bed2b0e859e55c1cc6b26502
ff000000000000000000000000000000 00000000000000000000000000000000	ec52a212f80a09df6317021bc2a9819e
ff800000000000000000000000000000 00000000000000000000000000000000	f23e5b600eb70dbccf6c0b1d9a68182c

ffc0000000000000000000000000000000000000000000000000000000000000	a3f599d63a82a968c33fe26590745970
ffe0000000000000000000000000000000000000000000000000000000000000	d1ccb9b1337002cbac42c520b5d67722
fff0000000000000000000000000000000000000000000000000000000000000	cc111f6c37cf40a1159d00fb59fb0488
fff8000000000000000000000000000000000000000000000000000000000000	dc43b51ab609052372989a26e9cdd714
fffc0000000000000000000000000000000000000000000000000000000000000	4dcede8da9e2578f39703d4433dc6459
fffe0000000000000000000000000000000000000000000000000000000000000	1a4c1c263bbccfafc11782894685e3a8
ffff0000000000000000000000000000000000000000000000000000000000000	937ad84880db50613423d6d527a2823d
ffff8000000000000000000000000000000000000000000000000000000000000	610b71dfc688e150d8152c5b35ebc14d
fffffc0000000000000000000000000000000000000000000000000000000000000	27ef2495dabf323885aab39c80f18d8b
fffffe0000000000000000000000000000000000000000000000000000000000000	633cafea395bc03adae3a1e2068e4b4e
fffff00000000000000000000000000000000000000000000000000000000000000	6e1b482b53761cf631819b749a6f3724
fffff80000000000000000000000000000000000000000000000000000000000000	976e6f851ab52c771998dbb2d71c75a9
fffffc0000000000000000000000000000000000000000000000000000000000000	85f2ba84f8c307cf525e124c3e22e6cc
fffffe0000000000000000000000000000000000000000000000000000000000000	6bcca98bf6a835fa64955f72de4115fe
ffffff0000000000000000000000000000000000000000000000000000000000000	2c75e2d36eebd65411f14fd0eb1d2a06
ffffff8000000000000000000000000000000000000000000000000000000000000	bd49295006250ffca5100b6007a0eade
ffffffc0000000000000000000000000000000000000000000000000000000000000	a190527d0ef7c70f459cd3940df316ec
ffffffe0000000000000000000000000000000000000000000000000000000000000	bbd1097a62433f79449fa97d4ee80dbf
fffffff0000000000000000000000000000000000000000000000000000000000000	07058e408f5b99b0e0f061a1761b5b3b
fffffff8000000000000000000000000000000000000000000000000000000000000	5fd1f13fa0f31e37fabde328f894eac2
fffffffc0000000000000000000000000000000000000000000000000000000000000	fc4af7c948df26e2ef3e01c1ee5b8f6f
fffffffe0000000000000000000000000000000000000000000000000000000000000	829fd7208fb92d44a074a677ee9861ac
ffffffff0000000000000000000000000000000000000000000000000000000000000	ad9fc613a703251b54c64a0e76431711

ffffffff800000000000000000000000 0000000000000000000000000000000000	33ac9eccc4cc75e2711618f80b1548e8
fffffffc000000000000000000000000 0000000000000000000000000000000000	2025c74b8ad8f4cda17ee2049c4c902d
fffffffe000000000000000000000000 0000000000000000000000000000000000	f85ca05fe528f1ce9b790166e8d551e7
ffffffff000000000000000000000000 0000000000000000000000000000000000	6f6238d8966048d4967154e0dad5a6c9
fffffffff800000000000000000000000 0000000000000000000000000000000000	f2b21b4e7640a9b3346de8b82fb41e49
fffffffffc000000000000000000000000 0000000000000000000000000000000000	f836f251ad1d11d49dc344628b1884e1
fffffffffe000000000000000000000000 0000000000000000000000000000000000	077e9470ae7abea5a9769d49182628c3
fffffffff0000000000000000000000000 0000000000000000000000000000000000	e0dcc2d27fc9865633f85223cf0d611f
fffffffff80000000000000000000000000 0000000000000000000000000000000000	be66cfea2fecd6bf0ec7b4352c99bcaa
fffffffffc000000000000000000000000 0000000000000000000000000000000000	df31144f87a2ef523facdcf21a427804
fffffffffe000000000000000000000000 0000000000000000000000000000000000	b5bb0f5629fb6aae5e1839a3c3625d63
ffffffffff000000000000000000000000 0000000000000000000000000000000000	3c9db3335306fe1ec612bdbfae6b6028
ffffffffff800000000000000000000000 0000000000000000000000000000000000	3dd5c34634a79d3cfcc8339760e6f5f4
ffffffffffc000000000000000000000000 0000000000000000000000000000000000	82bda118a3ed7af314fa2ccc5c07b761
ffffffffffe000000000000000000000000 0000000000000000000000000000000000	2937a64f7d4f46fe6fea3b349ec78e38
fffffffffff000000000000000000000000 0000000000000000000000000000000000	225f068c28476605735ad671bb8f39f3
fffffffffff800000000000000000000000 0000000000000000000000000000000000	ae682c5ecd71898e08942ac9aa89875c
fffffffffffc000000000000000000000000 0000000000000000000000000000000000	5e031cb9d676c3022d7f26227e85c38f
fffffffffffe000000000000000000000000 0000000000000000000000000000000000	a78463fb064db5d52bb64bfef64f2dda
ffffffffffff000000000000000000000000 0000000000000000000000000000000000	8aa9b75e784593876c53a00eae5af52b
ffffffffffff800000000000000000000000 0000000000000000000000000000000000	3f84566df23da48af692722fe980573a
ffffffffffffc000000000000000000000000 0000000000000000000000000000000000	31690b5ed41c7eb42a1e83270a7ff0e6
ffffffffffffe000000000000000000000000 0000000000000000000000000000000000	77dd7702646d55f08365e477d3590eda

ffffffffffffff0000000000000000000000000000000000000000000000000000	4c022ac62b3cb78d739cc67b3e20bb7e
ffffffffffffff8000000000000000000000000000000000000000000000000000	092fa137ce18b5dfe7906f550bb13370
fffffffffffffc0000000000000000000000000000000000000000000000000000	3e0cdadf2e68353c0027672c97144dd3
fffffffffffffe0000000000000000000000000000000000000000000000000000	d8c4b200b383fc1f2b2ea677618a1d27
ffffffffffffff0000000000000000000000000000000000000000000000000000	11825f99b0e9bb3477c1c0713b015aac
ffffffffffffff8000000000000000000000000000000000000000000000000000	f8b9fffb5c187f7ddc7ab10f4fb77576
ffffffffffffffc000000000000000000000000000000000000000000000000000	ffb4e87a32b37d6f2c8328d3b5377802
ffffffffffffffe000000000000000000000000000000000000000000000000000	d276c13a5d220f4da9224e74896391ce
ffffffffffffffff000000000000000000000000000000000000000000000000000	94efe7a0e2e031e2536da01df799c927
ffffffffffffffff800000000000000000000000000000000000000000000000000	8f8fd822680a85974e53a5a8eb9d38de
ffffffffffffffffc00000000000000000000000000000000000000000000000000	e0f0a91b2e45f8cc37b7805a3042588d
ffffffffffffffffe00000000000000000000000000000000000000000000000000	597a6252255e46d6364dbeeda31e279c
ffffffffffffffffff00000000000000000000000000000000000000000000000000	f51a0f694442b8f05571797fec7ee8bf
ffffffffffffffffff80000000000000000000000000000000000000000000000000	9ff071b165b5198a93dddeebc54d09b5
ffffffffffffffffffc0000000000000000000000000000000000000000000000000	c20a19fd5758b0c4bc1a5df89cf73877
ffffffffffffffffffe0000000000000000000000000000000000000000000000000	97120166307119ca2280e9315668e96f
ffffffffffffffffff0000000000000000000000000000000000000000000000000000	4b3b9f1e099c2a09dc091e90e4f18f0a
ffffffffffffffffff8000000000000000000000000000000000000000000000000000	eb040b891d4b37f6851f7ec219cd3f6d
ffffffffffffffffffc000000000000000000000000000000000000000000000000000	9f0fdec08b7fd79aa39535bea42db92a
ffffffffffffffffffe000000000000000000000000000000000000000000000000000	2e70f168fc74bf911df240bcd2cef236
ffffffffffffffffff0000000000000000000000000000000000000000000000000000	462ccd7f5fd1108dbc152f3cacad328b
ffffffffffffffffff8000000000000000000000000000000000000000000000000000	a4af534a7d0b643a01868785d86dfb95
ffffffffffffffffffc000000000000000000000000000000000000000000000000000	ab980296197e1a5022326c31da4bf6f3

fffffffffffffffffe000000000000000000000000000000000000000000000000	f97d57b3333b6281b07d486db2d4e20c
ffffffffffffffffff000000000000000000000000000000000000000000000000	f33fa36720231afe4c759ade6bd62eb6
ffffffffffffffffff800000000000000000000000000000000000000000000000	fdcfac0c02ca538343c68117e0a15938
fffffffffffffffffc000000000000000000000000000000000000000000000000	ad4916f5ee5772be764fc027b8a6e539
fffffffffffffffffe000000000000000000000000000000000000000000000000	2e16873e1678610d7e14c02d002ea845
ffffffffffffffffff000000000000000000000000000000000000000000000000	4e6e627c1acc51340053a8236d579576
ffffffffffffffffff800000000000000000000000000000000000000000000000	ab0c8410aeeead92feec1eb430d652cb
fffffffffffffffffc000000000000000000000000000000000000000000000000	e86f7e23e835e114977f60e1a592202e
fffffffffffffffffe000000000000000000000000000000000000000000000000	e68ad5055a367041fade09d9a70a794b
ffffffffffffffffff000000000000000000000000000000000000000000000000	0791823a3c666bb6162825e78606a7fe
ffffffffffffffffff800000000000000000000000000000000000000000000000	dcca366a9bf47b7b868b77e25c18a364
fffffffffffffffffc000000000000000000000000000000000000000000000000	684c9efc237e4a442965f84bce20247a
fffffffffffffffffe000000000000000000000000000000000000000000000000	a858411ffbe63fdb9c8aa1bfaed67b52
ffffffffffffffffff000000000000000000000000000000000000000000000000	04bc3da2179c3015498b0e03910db5b8
ffffffffffffffffff800000000000000000000000000000000000000000000000	40071eeab3f935dbc25d00841460260f
fffffffffffffffffc000000000000000000000000000000000000000000000000	0ebd7c30ed2016e08ba806ddb008bcc8
fffffffffffffffffe000000000000000000000000000000000000000000000000	15c6becf0f4cec7129cbd22d1a79b1b8
ffffffffffffffffff000000000000000000000000000000000000000000000000	0aeede5b91f721700e9e62edbf60b781
ffffffffffffffffff800000000000000000000000000000000000000000000000	266581af0dcfbed1585e0a242c64b8df
fffffffffffffffffc000000000000000000000000000000000000000000000000	6693dc911662ae473216ba22189a511a
fffffffffffffffffe000000000000000000000000000000000000000000000000	7606fa36d86473e6fb3a1bb0e2c0adf5
ffffffffffffffffff000000000000000000000000000000000000000000000000	112078e9e11fbb78e26ffb8899e96b9a
ffffffffffffffffff800000000000000000000000000000000000000000000000	40b264e921e9e4a82694589ef3798262

fffffffffffffffffffffffc000000 0000000000000000000000000000000	8d4595cb4fa7026715f55bd68e2882f9
fffffffffffffffffffffffe000000 0000000000000000000000000000000	b588a302bdbc09197df1edae68926ed9
ffffffffffffffffffffffff000000 0000000000000000000000000000000	33f7502390b8a4a221cfecd0666624ba
ffffffffffffffffffffffff800000 0000000000000000000000000000000	3d20253adbce3be2373767c4d822c566
fffffffffffffffffffffffffc00000 0000000000000000000000000000000	a42734a3929bf84cf0116c9856a3c18c
fffffffffffffffffffffffffe00000 0000000000000000000000000000000	e3abc4939457422bb957da3c56938c6d
ffffffffffffffffffffffffff00000 0000000000000000000000000000000	972bdd2e7c525130fadc8f76fc6f4b3f
ffffffffffffffffffffffffff80000 0000000000000000000000000000000	84a83d7b94c699cbcb8a7d9b61f64093
fffffffffffffffffffffffffffc0000 0000000000000000000000000000000	ce61d63514aded03d43e6ebfc3a9001f
fffffffffffffffffffffffffffe0000 0000000000000000000000000000000	6c839dd58eeae6b8a36af48ed63d2dc9
ffffffffffffffffffffffffffff0000 0000000000000000000000000000000	cd5ece55b8da3bf622c4100df5de46f9
ffffffffffffffffffffffffffff8000 0000000000000000000000000000000	3b6f46f40e0ac5fc0a9c1105f800f48d
ffffffffffffffffffffffffffffc000 0000000000000000000000000000000	ba26d47da3aeb028de4fb5b3a854a24b
ffffffffffffffffffffffffffffe000 0000000000000000000000000000000	87f53bf620d3677268445212904389d5
fffffffffffffffffffffffffffff000 0000000000000000000000000000000	10617d28b5e0f4605492b182a5d7f9f6
fffffffffffffffffffffffffffff800 0000000000000000000000000000000	9aaec4fabbf6fae2a71feff02e372b39
fffffffffffffffffffffffffffffc00 0000000000000000000000000000000	3a90c62d88b5c42809abf782488ed130
fffffffffffffffffffffffffffffe00 0000000000000000000000000000000	f1f1c5a40899e15772857ccb65c7a09a
ffffffffffffffffffffffffffffff00 0000000000000000000000000000000	190843d29b25a3897c692ce1dd81ee52
ffffffffffffffffffffffffffffff80 0000000000000000000000000000000	a866bc65b6941d86e8420a7ffb0964db
ffffffffffffffffffffffffffffffc0 0000000000000000000000000000000	8193c6ff85225ced4255e92f6e078a14
ffffffffffffffffffffffffffffffe0 0000000000000000000000000000000	9661cb2424d7d4a380d547f9e7ec1cb9
fffffffffffffffffffffffffffffff0 0000000000000000000000000000000	86f93d9ec08453a071e2e2877877a9c8

ffffffffffffffffffffffffffffff8 0000000000000000000000000000000	27eefa80ce6a4a9d598e3fec365434d2
ffffffffffffffffffffffffffffffc 0000000000000000000000000000000	d62068444578e3ab39ce7ec95dd045dc
ffffffffffffffffffffffffffffffe 0000000000000000000000000000000	b5f71d4dd9a71fe5d8bc8ba7e6ea3048
fffffffffffffffffffffffffffffff 0000000000000000000000000000000	6825a347ac479d4f9d95c5cb8d3fd7e9
fffffffffffffffffffffffffffffff 8000000000000000000000000000000	e3714e94a5778955cc0346358e94783a
fffffffffffffffffffffffffffffff c000000000000000000000000000000	d836b44bb29e0c7d89fa4b2d4b677d2a
fffffffffffffffffffffffffffffff e000000000000000000000000000000	5d454b75021d76d4b84f873a8f877b92
fffffffffffffffffffffffffffffff f000000000000000000000000000000	c3498f7eced2095314fc28115885b33f
fffffffffffffffffffffffffffffff f800000000000000000000000000000	6e668856539ad8e405bd123fe6c88530
fffffffffffffffffffffffffffffff fc00000000000000000000000000000	8680db7f3a87b8605543cfdbe6754076
fffffffffffffffffffffffffffffff fe00000000000000000000000000000	6c5d03b13069c3658b3179be91b0800c
fffffffffffffffffffffffffffffff ff00000000000000000000000000000	ef1b384ac4d93eda00c92add0995ea5f
fffffffffffffffffffffffffffffff ff80000000000000000000000000000	bf8115805471741bd5ad20a03944790f
fffffffffffffffffffffffffffffff ffc0000000000000000000000000000	c64c24b6894b038b3c0d09b1df068b0b
fffffffffffffffffffffffffffffff ffe0000000000000000000000000000	3967a10cffe27d0178545fbf6a40544b
fffffffffffffffffffffffffffffff fff0000000000000000000000000000	7c85e9c95de1a9ec5a5363a8a053472d
fffffffffffffffffffffffffffffff fff8000000000000000000000000000	a9eec03c8abec7ba68315c2c8c2316e0
fffffffffffffffffffffffffffffff fffc000000000000000000000000000	cac8e414c2f388227ae14986fc983524
fffffffffffffffffffffffffffffff fffe000000000000000000000000000	5d942b7f4622ce056c3ce3ce5f1dd9d6
fffffffffffffffffffffffffffffff ffff000000000000000000000000000	d240d648ce21a3020282c3f1b528a0b6
fffffffffffffffffffffffffffffff ffff800000000000000000000000000	45d089c36d5c5a4efc689e3b0de10dd5
fffffffffffffffffffffffffffffff ffffc00000000000000000000000000	b4da5df4becb5462e03a0ed00d295629
fffffffffffffffffffffffffffffff ffffe00000000000000000000000000	dcf4e129136c1a4b7a0f38935cc34b2b

ffffffffffffffffffffffffffffffff fffff00000000000000000000000000	d9a4c7618b0ce48a3d5aee1a1c0114c4
ffffffffffffffffffffffffffffffff fffff80000000000000000000000000	ca352df025c65c7b0bf306fbee0f36ba
ffffffffffffffffffffffffffffffff fffffc00000000000000000000000000	238aca23fd3409f38af63378ed2f5473
ffffffffffffffffffffffffffffffff fffffe00000000000000000000000000	59836a0e06a79691b36667d5380d8188
ffffffffffffffffffffffffffffffff ffffff00000000000000000000000000	33905080f7acf1cdae0a91fc3e85aee4
ffffffffffffffffffffffffffffffff ffffff80000000000000000000000000	72c9e4646dbc3d6320fc6689d93e8833
ffffffffffffffffffffffffffffffff ffffffc0000000000000000000000000	ba77413dea5925b7f5417ea47ff19f59
ffffffffffffffffffffffffffffffff ffffffe0000000000000000000000000	6cae8129f843d86dc786a0fb1a184970
ffffffffffffffffffffffffffffffff fffffff0000000000000000000000000	fcfefb534100796eebbd990206754e19
ffffffffffffffffffffffffffffffff fffffff8000000000000000000000000	8c791d5fdddf470da04f3e6dc4a5b5b5
ffffffffffffffffffffffffffffffff fffffffc000000000000000000000000	c93bbdc07a4611ae4bb266ea5034a387
ffffffffffffffffffffffffffffffff fffffffe000000000000000000000000	c102e38e489aa74762f3efc5bb23205a
ffffffffffffffffffffffffffffffff ffffffff000000000000000000000000	93201481665cbafc1fcc220bc545fb3d
ffffffffffffffffffffffffffffffff ffffffff800000000000000000000000	4960757ec6ce68cf195e454cfd0f32ca
ffffffffffffffffffffffffffffffff ffffffffc00000000000000000000000	feec7ce6a6cbd07c043416737f1bbb33
ffffffffffffffffffffffffffffffff ffffffffe00000000000000000000000	11c5413904487a805d70a8edd9c35527
ffffffffffffffffffffffffffffffff fffffffff00000000000000000000000	347846b2b2e36f1f0324c86f7f1b98e2
ffffffffffffffffffffffffffffffff fffffffff80000000000000000000000	332eee1a0cbd19ca2d69b426894044f0
ffffffffffffffffffffffffffffffff ffffffffc0000000000000000000000	866b5b3977ba6efa5128efbda9ff03cd
ffffffffffffffffffffffffffffffff ffffffffe0000000000000000000000	cc1445ee94c0f08cdee5c344ecd1e233
ffffffffffffffffffffffffffffffff fffffffff0000000000000000000000	be288319029363c2622feba4b05dfdfe
ffffffffffffffffffffffffffffffff fffffffff8000000000000000000000	cfd1875523f3cd21c395651e6ee15e56
ffffffffffffffffffffffffffffffff ffffffffc0000000000000000000000	cb5a408657837c53bf16f9d8465dce19

ffffffffffffffffffffffffffffffff fffffffffe0000000000000000000000	ca0bf42cb107f55ccff2fc09ee08ca15
ffffffffffffffffffffffffffffffff fffffffffff0000000000000000000000	fdd9bbb4a7dc2e4a23536a5880a2db67
ffffffffffffffffffffffffffffffff fffffffffff8000000000000000000000	ede447b362c484993dec9442a3b46aef
ffffffffffffffffffffffffffffffff ffffffffffc0000000000000000000000	10dffb05904bff7c4781df780ad26837
ffffffffffffffffffffffffffffffff fffffffffffe0000000000000000000000	c33bc13e8de88ac25232aa7496398783
ffffffffffffffffffffffffffffffff ffffffffffff0000000000000000000000	ca359c70803a3b2a3d542e8781dea975
ffffffffffffffffffffffffffffffff ffffffffffff8000000000000000000000	bcc65b526f88d05b89ce8a52021fdb06
ffffffffffffffffffffffffffffffff ffffffffffffc000000000000000000000	db91a38855c8c4643851fbfb358b0109
ffffffffffffffffffffffffffffffff ffffffffffffe000000000000000000000	ca6e8893a114ae8e27d5ab03a5499610
ffffffffffffffffffffffffffffffff ffffffffffffff0000000000000000000000	6629d2b8df97da728cdd8b1e7f945077
ffffffffffffffffffffffffffffffff ffffffffffffff8000000000000000000000	4570a5a18cfc0dd582f1d88d5c9a1720
ffffffffffffffffffffffffffffffff ffffffffffffffc000000000000000000000	72bc65aa8e89562e3f274d45af1cd10b
ffffffffffffffffffffffffffffffff ffffffffffffffe000000000000000000000	98551da1a6503276ae1c77625f9ea615
ffffffffffffffffffffffffffffffff fffffffffffffff0000000000000000000000	0ddfe51ced7e3f4ae927daa3fe452cee
ffffffffffffffffffffffffffffffff fffffffffffffff8000000000000000000000	db826251e4ce384b80218b0e1da1dd4c
ffffffffffffffffffffffffffffffff fffffffffffffffc000000000000000000000	2cacf728b88abbad7011ed0e64a1680c
ffffffffffffffffffffffffffffffff fffffffffffffffe000000000000000000000	330d8ee7c5677e099ac74c9994ee4cfb
ffffffffffffffffffffffffffffffff ffffffffffffffff000000000000000000000	edf61ae362e882ddc0167474a7a77f3a
ffffffffffffffffffffffffffffffff ffffffffffffffff800000000000000000000	6168b00ba7859e0970ecfd757efecf7c
ffffffffffffffffffffffffffffffff ffffffffffffffffc00000000000000000000	d1415447866230d28bb1ea18a4cdfd02
ffffffffffffffffffffffffffffffff ffffffffffffffffe00000000000000000000	516183392f7a8763afec68a060264141
ffffffffffffffffffffffffffffffff fffffffffffffffff00000000000000000000	77565c8d73cfd4130b4aa14d8911710f
ffffffffffffffffffffffffffffffff fffffffffffffffff80000000000000000000	37232a4ed21ccc27c19c9610078cabac

ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	804f32ea71828c7d329077e712231666
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	d64424f23cb97215e9c2c6f28d29eab7
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	023e82b533f68c75c238cebdb2ee89a2
ffffffffffffffffffffffffffffffff ffffffffffffffff8000000000000000	193a3d24157a51f1ee0893f6777417e7
ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	84ecacfcd400084d078612b1945f2ef5
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	1dcd8bb173259eb33a5242b0de31a455
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	35e9eddbc375e792c19992c19165012b
ffffffffffffffffffffffffffffffff ffffffffffffffff8000000000000000	8a772231c01dfdd7c98e4cfddcc0807a
ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	6eda7ff6b8319180ff0d6e65629d01c3
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	c267ef0e2d01a993944dd397101413cb
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	e9f80e9d845bcc0f62926af72eabca39
ffffffffffffffffffffffffffffffff ffffffffffffffff8000000000000000	6702990727aa0878637b45dcd3a3b074
ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	2e2e647d5360e09230a5d738ca33471e
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	1f56413c7add6f43d1d56e4f02190330
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	69cd0606e15af729d6bca143016d9842
ffffffffffffffffffffffffffffffff ffffffffffffffff8000000000000000	a085d7c1a500873a20099c4caa3c3f5b
ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	4fc0d230f8891415b87b83f95f2e09d1
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	4327d08c523d8eba697a4336507d1f42
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	7a15aab82701efa5ae36ab1d6b76290f
ffffffffffffffffffffffffffffffff ffffffffffffffff8000000000000000	5bf0051893a18bb30e139a58fed0fa54
ffffffffffffffffffffffffffffffff fffffffffffffffc0000000000000000	97e8adf65638fd9cdf3bc22c17fe4dbd
ffffffffffffffffffffffffffffffff fffffffffffffffe0000000000000000	1ee6ee326583a0586491c96418d1a35d
ffffffffffffffffffffffffffffffff ffffffffffffffff0000000000000000	26b549c2ec756f82ecc48008e529956b

ffffffffffffffffffffffffffffffff ffffffffffffffffffff8000000000	70377b6da669b072129e057cc28e9ca5
ffffffffffffffffffffffffffffffff ffffffffffffffffffffc000000000	9c94b8b0cb8bcc919072262b3fa05ad9
ffffffffffffffffffffffffffffffff ffffffffffffffffffffe000000000	2fbb83dfd0d7abcb05cd28cad2dfb523
ffffffffffffffffffffffffffffffff fffffffffffffffffffff000000000	96877803de77744bb970d0a91f4debae
ffffffffffffffffffffffffffffffff fffffffffffffffffffff800000000	7379f3370cf6e5ce12ae5969c8eea312
ffffffffffffffffffffffffffffffff fffffffffffffffffffffc00000000	02dc99fa3d4f98ce80985e7233889313
ffffffffffffffffffffffffffffffff fffffffffffffffffffffe00000000	1e38e759075ba5cab6457da51844295a
ffffffffffffffffffffffffffffffff fffffffffffffffffffff00000000	70bed8dbf615868a1f9d9b05d3e7a267
ffffffffffffffffffffffffffffffff fffffffffffffffffffff80000000	234b148b8cb1d8c32b287e896903d150
ffffffffffffffffffffffffffffffff fffffffffffffffffffffc0000000	294b033df4da853f4be3e243f7e513f4
ffffffffffffffffffffffffffffffff fffffffffffffffffffffe0000000	3f58c950f0367160adec45f2441e7411
ffffffffffffffffffffffffffffffff fffffffffffffffffffff0000000	37f655536a704e5ace182d742a820cf4
ffffffffffffffffffffffffffffffff fffffffffffffffffffff8000000	ea7bd6bb63418731aeac790fe42d61e8
ffffffffffffffffffffffffffffffff fffffffffffffffffffffc000000	e74a4c999b4c064e48bb1e413f51e5ea
ffffffffffffffffffffffffffffffff fffffffffffffffffffffe000000	ba9ebefdb4ccf30f296cecb3bc1943e8
ffffffffffffffffffffffffffffffff fffffffffffffffffffff000000	3194367a4898c502c13bb7478640a72d
ffffffffffffffffffffffffffffffff fffffffffffffffffffff800000	da797713263d6f33a5478a65ef60d412
ffffffffffffffffffffffffffffffff fffffffffffffffffffffc00000	d1ac39bb1ef86b9c1344f214679aa376
ffffffffffffffffffffffffffffffff fffffffffffffffffffffe00000	2fdea9e650532be5bc0e7325337fd363
ffffffffffffffffffffffffffffffff fffffffffffffffffffff00000	d3a204dbd9c2af158b6ca67a5156ce4a
ffffffffffffffffffffffffffffffff fffffffffffffffffffff80000	3a0a0e75a8da36735aee6684d965a778
ffffffffffffffffffffffffffffffff fffffffffffffffffffffc0000	52fc3e620492ea99641ea168da5b6d52
ffffffffffffffffffffffffffffffff fffffffffffffffffffffe0000	d2e0c7f15b4772467d2cfc873000b2ca

ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffff0000	563531135e0c4d70a38f8bdb190ba04e
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffff8000	a8a39a0f5663f4c0fe5f2d3cafff421a
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffc000	d94b5e90db354c1e42f61fabe167b2c0
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffe000	50e6d3c9b6698a7cd276f96b1473f35a
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffff000	9338f08e0ebee96905d8f2e825208f43
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffff800	8b378c86672aa54a3a266ba19d2580ca
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffc00	cca7c3086f5f9511b31233da7cab9160
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffe00	5b40ff4ec9be536ba23035fa4f06064c
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffff00	60eb5af8416b257149372194e8b88749
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffff80	2f005a8aed8a361c92e440c15520cbd1
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffc0	7b03627611678a997717578807a800e2
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffe0	cf78618f74f6f3696e0a4779b90b5a77
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffff0	03720371a04962eaea0a852e69972858
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffff8	1f8a8133aa8ccf70e2bd3285831ca6b7
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffffc	27936bd27fb1468fc8b48bc483321725
ffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffffe	b07d4f3e2cd2ef2eb545980754dfea0f
ffffffffffffffffffffffffffffffff ffffffffffffffffffffffffffffffff	4bf85f1b5d54adbc307b0a048389adcb

Appendix F. Bibliography

[1] *Advanced Encryption Standard (AES)*, FIPS Publication 197, National Institute of Standards and Technology, November 2001.

[2] *Security Requirements for Cryptographic Modules*, FIPS Publication 140-2, National Institute of Standards and Technology, May 2001.