Cambridge Academy for Science and Technology

AQA Computer Science

Practical Computing Project

CRYPTOGRAPHY ONLINE

Author
J.P. Jacob Powell

Supervisor
B.C. Barry Cooper

April 24, 2018

Contents

Chapter 1

Testing

1.1 The Web Application

Since my Web Application has many moving parts I wil be testing each of the componenets individually first. Then when I can be sure that the components work individually I will test all of them together.

1.1.1 Web Application Test Table

Test #	Test Description	Test Type	Expected Result	Pass /Fail	Ref No
1	Connecting to the Website	Typical	The user will be able to successfully load the Website	Pass	01
2	Loading the Basic Concepts Page	Typical	The user will be presented with the content for the basic concepts page	Pass	02
3	Loading the Modular Arithmetic Page	Typical	The user will be able to successfully load the content for the Modular Arithmetic Page	Pass	03
4	Loading the Login Page	Typical	The user will be able to successfully load the Login Page	Pass	04
5	Loading the Register Page	Typical	The user will be able to successfully load the Register Page	Pass	05

6	Loading the Profile Page	Typical	The user will be able to successfully load the P rofile Page	Pass	06
7	Check user has to e nter a username w hen registering	Erroneous	The user will not be abl e to register if they don 't enter a username	Pass	07
8	Check the user ha s to enter a passwo rd when registering	Erroneous	The user will not be abl e to register for an acco unt if the don't enter a password	Pass	08
9	Check that the us er has to enter the same password wh en confirming their password to registe r	Erroneous	The user will not be ab le to register if they do n't enter the same pass word	Pass	09
10	Check that the use r doesn't have to e nter a email if they want to register	Typical	The user will be able to register whether or not they enter an email ad dress	Pass	10
11	Check that if the u ser does enter an e mail a confirmation email is sent to the address supplied	Typical	The user will receive a n email providing them with a confirmation lin k to activate their acco unt	Pass	11
12	Check that the pas sword entered mee ts strength require ments	Erroneous	If a user registers with a weak password the u ser will not be able to r egister but if they sign up with a strong passw ord then they will be re gistered	Pass	12
13	When a user regist ers with all valid in formation that user data is added to th e authentication ta bles	Typical	The authentication info rmation is added to the authentication tables	Pass	13
14	When a user regist ers a record is also created for them in the db_user tables	Typical	A record for the user i s created in the db_use r table	Pass	14

15	After the user has registered they are then sent to the homepage	Typical	After the user has registered the website will navigate them to the homepage	Pass	15
16	Once the user has registered and reached the homepage a custom header navigation bar should be loaded	Typical	The user header will be loaded rather than the normal site header navigation bar	Pass	16
17	The admin settings tab should not show for any non-admins	Typical	When a normal user logs in they should not see the admin settings tab in the header	Pass	17
18	The admin settings tab should show for any admin users when they log in	Typical	The admin settings tab should load onto the header when an admin logs in	Pass	18
19	When a user is not logged in and they navigate to the profile page it should say that no user is logged in	Typical	The profile page displays that no user is logged in	Pass	19
20	When a logged in user navigates to the profile page it should show the user their profile page	Typical	The user will be presented with the profile page for their account	Pass	20
21	When a user is not logged in and they navigate to the profile page it should say that no user is logged in	Typical	The profile page displays that no user is logged in	Pass	21
22	When a logged in user goes to their profile page it should show them the number of questions that they have answered	Typical	The user will be able to see the total number of questions they have answered	Pass	22

23	When a logged in user goes to their profile page it should show the total number of questions answered correctly	Typical	The profile page will show the total number of questions that have been answered correctly.	Pass	23
22	When a user tries to log in with valid credentials they are logged in	Typical	The user will be logged in	Pass	22
23	After a few attempts to try to log in the user will have to wait to log in again	Typical	The user will be given a time out and will have to wait a fair interval until they can try to login in again	Pass	23
24	When a user answers a question it should store the question in the user_answered_questions table	Typical	The relevant question information is stored in the user_answered_questions table	Pass	24
25	When the user answers the question correctly then it displays the user got the question correct	Typical	The user is shown that they got the question correct	Pass	25
26	When the user answers the question wrong it displays that they got the question wrong	Typical	The user is shown that they got the question wrong	Pass	26
27	When ever the user answers the question it updates the question in the user_answered_question table	Typical	The users question answer should be updated in the user_answered_question table	Pass	27
28		Typical		Pass	28
28		Typical		Pass	28
28		Typical		Pass	28

28		Typical		Pass	28
28		Typical		Pass	28
28		Typical		Pass	28
28		Typical		Pass	28
29		Typical		Pass	29

1.2 AES Implementation

My AES Implementation has been tested against the Federal Information Processing Standard Publication 197 (FIPS 197) test vectors. All test vectors use hexadecimal notation.

1.2.1 AES Implementation Testing Code

In order to completely test my solution I have written a short program that uses to test vectors from FIPS 197. I can then compare the results from my program and from the FIPS 197 document. If they match then I know my implementation of the algorithm is correct.

```
1  /**
2   * @file aes_implementation_test.cc
3   * @date 28/02/2018
4   *
5   * @breif This file will contain test methods to verify the functionality of my implementation of the AES Algorithm
6   *        All of the test keys and plaintexts are the same as shown in FIPS 197.
7   *
8   * @version 0.01
9   * @author Jacob Powell
10  *
11  */
12
13 #include "aes_implementation.h"
14
15 #include <iostream>
16 #include <iomanip>
17
18 void test_aes_256(){
19     AESImplementation aes(AES256);
20     byte key_256[] = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f,
21                       0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19, 0x1a, 0x1b, 0x1c, 0x1d, 0x1e, 0x1f};
22     byte plaintext[] = {0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff};
23     byte ciphertext[16];
24     byte plaintext2[16];
25
26     aes.encrypt_block(plaintext, ciphertext, key_256);
27
28     std::cout << "Cipher Text: ";
29     for(byte i = 0; i < 16; i++){
30         std::cout << std::hex << std::setfill('0') << std::setw(2) << unsigned(ciphertext[i]);
31     }
32     std::cout << std::endl;
33
```

```
34      aes.decrypt_block(ciphertext, plaintext2, key_256);
35
36      std::cout << "Plaintext: ";
37      for(byte i = 0; i < 16; i++){
38          std::cout << std::hex << std::setfill('0') << std::setw(2) << ↩
            unsigned(plaintext2[i]);
39      }
40      std::cout << std::endl;
41
42  }
43
44  void test_aes_192(){
45      AESImplementation aes(AES192);
46      byte key_192[] = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0↩
            x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f,
47                        0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17};
48      byte plaintext[] = {0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0↩
            x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff};
49      byte ciphertext[16];
50      byte plaintext2[16];
51
52      aes.encrypt_block(plaintext, ciphertext, key_192);
53
54      std::cout << "Cipher Text: ";
55      for(byte i = 0; i < 16; i++){
56          std::cout << std::hex << std::setfill('0') << std::setw(2) << ↩
            unsigned(ciphertext[i]);
57      }
58      std::cout << std::endl;
59
60      aes.decrypt_block(ciphertext, plaintext2, key_192);
61
62      std::cout << "Plaintext: ";
63      for(byte i = 0; i < 16; i++){
64          std::cout << std::hex << std::setfill('0') << std::setw(2) << ↩
            unsigned(plaintext2[i]);
65      }
66      std::cout << std::endl;
67
68      std::cout << std::endl;
69  }
70
71  void test_aes_128(){
72      AESImplementation aes(AES128);
73
74      byte key_128[] = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0↩
            x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f};
75      byte plaintext[] = {0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77, 0↩
            x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff};
76      byte ciphertext[16];
77      byte plaintext2[16];
78
79      aes.encrypt_block(plaintext, ciphertext, key_128, plaintext);
80
81      std::cout << "Cipher Text: ";
```

```
82      for(byte i = 0; i < 16; i++){
83          std::cout << std::hex << std::setfill('0') << std::setw(2) << ↩
                unsigned(ciphertext[i]);
84      }
85      std::cout << std::endl;
86
87      aes.decrypt_block(ciphertext, plaintext2, key_128);
88
89      std::cout << "Plaintext: ";
90      for(byte i = 0; i < 16; i++){
91          std::cout << std::hex << std::setfill('0') << std::setw(2) << ↩
                unsigned(plaintext2[i]);
92      }
93      std::cout << std::endl;
94
95  }
96
97
98  int main(){
99      test_aes_128();
100     test_aes_192();
101     test_aes_256();
102 }
```

1.2.2 AES-128

$$Nk = 4, Nr = 10$$
$$Plaintext = 00112233445566778899aabbccddeeff$$
$$Key = 000102030405060708090a0b0c0d0e0f$$

1.2.2.1 Cipher (ENCRYPT)

round[0].input	00112233445566778899aabbccddeeff
round[0].k_sch	000102030405060708090a0b0c0d0e0f
round[1].start	00102030405060708090a0b0c0d0e0f0
round[1].s_box	63cab7040953d051cd60e0e7ba70e18c
round[1].s_row	6353e08c0960e104cd70b751bacad0e7
round[1].m_col	5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch	d6aa74fdd2af72fadaa678f1d6ab76fe
round[2].start	89d810e8855ace682d1843d8cb128fe4
round[2].s_box	a761ca9b97be8b45d8ad1a611fc97369
round[2].s_row	a7be1a6997ad739bd8c9ca451f618b61
round[2].m_col	ff87968431d86a51645151fa773ad009
round[2].k_sch	b692cf0b643dbdf1be9bc5006830b3fe
round[3].start	4915598f55e5d7a0daca94fa1f0a63f7
round[3].s_box	b59cb73fcd90ee05774222dc067fb68

round[3].s_row	3bd92268fc74fb735767cbe0c0590e2d
round[3].m_col	4c9c1e66f771f0762c3f868e534df256
round[3].k_sch	b6ff744ed2c2c9bf6c590cbf0469bf41
round[4].start	fa636a2825b339c940668a3157244d17
round[4].s_box	2dfb02343f6d12dd09337ec75b36e3f0
round[4].s_row	2d6d7ef03f33e334093602dd5bfb12c7
round[4].m_col	6385b79ffc538df997be478e7547d691
round[4].k_sch	47f7f7bc95353e03f96c32bcfd058dfd
round[5].start	247240236966b3fa6ed2753288425b6c
round[5].s_box	36400926f9336d2d9fb59d23c42c3950
round[5].s_row	36339d50f9b539269f2c092dc4406d23
round[5].m_col	f4bcd45432e554d075f1d6c51dd03b3c
round[5].k_sch	3caaa3e8a99f9deb50f3af57adf622aa
round[6].start	c81677bc9b7ac93b25027992b0261996
round[6].s_box	e847f56514dadde23f77b64fe7f7d490
round[6].s_row	e8dab6901477d4653ff7f5e2e747dd4f
round[6].m_col	9816ee7400f87f556b2c049c8e5ad036
round[6].k_sch	5e390f7df7a69296a7553dc10aa31f6b
round[7].start	c62fe109f75eedc3cc79395d84f9cf5d
round[7].s_box	b415f8016858552e4bb6124c5f998a4c
round[7].s_row	b458124c68b68a014b99f82e5f15554c
round[7].m_col	c57e1c159a9bd286f05f4be098c63439
round[7].k_sch	14f9701ae35fe28c440adf4d4ea9c026
round[8].start	d1876c0f79c4300ab45594add66ff41f
round[8].s_box	3e175076b61c04678dfc2295f6a8bfc0
round[8].s_row	3e1c22c0b6fcbf768da85067f6170495
round[8].m_col	baa03de7a1f9b56ed5512cba5f414d23
round[8].k_sch	47438735a41c65b9e016baf4aebf7ad2
round[9].start	fde3bad205e5d0d73547964ef1fe37f1
round[9].s_box	5411f4b56bd9700e96a0902fa1bb9aa1
round[9].s_row	54d990a16ba09ab596bbf40ea111702f
round[9].m_col	e9f74eec023020f61bf2ccf2353c21c7
round[9].k_sch	549932d1f08557681093ed9cbe2c974e
round[10].start	bd6e7c3df2b5779e0b61216e8b10b689
round[10].s_box	7a9f102789d5f50b2beffd9f3dca4ea7
round[10].s_row	7ad5fda789ef4e272bca100b3d9ff59f
round[10].k_sch	13111d7fe3944a17f307a78b4d2b30c5
round[10].output	69c4e0d86a7b0430d8cdb78070b4c55a

1.2.2.2 Inverse Cipher (DECRYPT)

round[0].iinput	69c4e0d86a7b0430d8cdb78070b4c55a

round[0].ik_sch	13111d7fe3944a17f307a78b4d2b30c5
round[1].istart	7ad5fda789ef4e272bca100b3d9ff59f
round[1].is_box	bdb52189f261b63d0b107c9e8b6e776e
round[1].is_row	bd6e7c3df2b5779e0b61216e8b10b689
round[1].im_col	4773b91ff72f354361cb018ea1e6cf2c
round[1].ik_sch	13aa29be9c8faff6f770f58000f7bf03
round[2].istart	54d990a16ba09ab596bbf40ea111702f
round[2].is_box	fde596f1054737d235febad7f1e3d04e
round[2].is_row	fde3bad205e5d0d73547964ef1fe37f1
round[2].im_col	2d7e86a339d9393ee6570a1101904e16
round[2].ik_sch	1362a4638f2586486bff5a76f7874a83
round[3].istart	3e1c22c0b6fcbf768da85067f6170495
round[3].is_box	d1c4941f7955f40fb46f6c0ad68730ad
round[3].is_row	d1876c0f79c4300ab45594add66ff41f
round[3].im_col	39daee38f4f1a82aaf432410c36d45b9
round[3].ik_sch	8d82fc749c47222be4dadc3e9c7810f5
round[4].istart	b458124c68b68a014b99f82e5f15554c
round[4].is_box	c65e395df779cf09ccf9e1c3842fed5d
round[4].is_row	c62fe109f75eedc3cc79395d84f9cf5d
round[4].im_col	9a39bf1d05b20a3a476a0bf79fe51184
round[4].ik_sch	72e3098d11c5de5f789dfe1578a2cccb
round[5].istart	e8dab6901477d4653ff7f5e2e747dd4f
round[5].is_box	c87a79969b0219bc2526773bb016c992
round[5].is_row	c81677bc9b7ac93b25027992b0261996
round[5].im_col	18f78d779a93eef4f6742967c47f5ffd
round[5].ik_sch	2ec410276326d7d26958204a003f32de
round[6].istart	36339d50f9b539269f2c092dc4406d23
round[6].is_box	2466756c69d25b236e4240fa8872b332
round[6].is_row	247240236966b3fa6ed2753288425b6c
round[6].im_col	85cf8bf472d124c10348f545329c0053
round[6].ik_sch	a8a2f5044de2c7f50a7ef79869671294
round[7].istart	2d6d7ef03f33e334093602dd5bfb12c7
round[7].is_box	fab38a1725664d2840246ac957633931
round[7].is_row	fa636a2825b339c940668a3157244d17
round[7].im_col	fc1fc1f91934c98210fbfb8da340eb21
round[7].ik_sch	c7c6e391e54032f1479c306d6319e50c
round[8].istart	3bd92268fc74fb735767cbe0c0590e2d
round[8].is_box	49e594f755ca638fda0a59a01f15d7fa
round[8].is_row	4915598f55e5d7a0daca94fa1f0a63f7
round[8].im_col	076518f0b52ba2fb7a15c8d93be45e00
round[8].ik_sch	a0db02992286d160a2dc029c2485d561
round[9].istart	a7be1a6997ad739bd8c9ca451f618b61
round[9].is_box	895a43e485188fe82d121068cbd8ced8
round[9].is_row	89d810e8855ace682d1843d8cb128fe4

round[9].im_col	ef053f7c8b3d32fd4d2a64ad3c93071a
round[9].ik_sch	8c56dff0825dd3f9805ad3fc8659d7fd
round[10].istart	6353e08c0960e104cd70b751bacad0e7
round[10].is_box	0050a0f04090e03080d02070c01060b0
round[10].is_row	00102030405060708090a0b0c0d0e0f0
round[10].ik_sch	000102030405060708090a0b0c0d0e0f
round[10].ioutput	00112233445566778899aabbccddeeff

1.2.3 AES-192

$$
\begin{aligned}
Nk = 6, Nr &= 12 \\
Plaintext =& 00112233445566778899aabbccddeeff \\
Key =& 000102030405060708090a0b0c0d0e0f \\
& 1011121314151617
\end{aligned}
$$

1.2.3.1 Cipher (ENCRYPT)

round[0].input	00112233445566778899aabbccddeeff
round[0].k_sch	000102030405060708090a0b0c0d0e0f
round[1].start	00102030405060708090a0b0c0d0e0f0
round[1].s_box	63cab7040953d051cd60e0e7ba70e18c
round[1].s_row	6353e08c0960e104cd70b751bacad0e7
round[1].m_col	5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch	101112131415161758462f95c43f4fe
round[2].start	4f63760643e0aa85aff8c9d041fa0de4
round[2].s_box	84fb386f1ae1ac977941dd70832dd769
round[2].s_row	84e1dd691a41d76f792d389783fbac70
round[2].m_col	9f487f794f955f662afc86abd7f1ab29
round[2].k_sch	544afef55847f0fa4856e2e95c43f4fe
round[3].start	cb02818c17d2af9c62aa64428bb25fd7
round[3].s_box	1f770c64f0b579deaaac432c3d37cf0e
round[3].s_row	1fb5430ef0accf64aa370cde3d77792c
round[3].m_col	b7a53ecbbf9d75a0c40efc79b674cc11
round[3].k_sch	40f949b31cbabd4d48f043b810b7b342
round[4].start	f75c7778a327c8ed8cfebfc1a6c37f53
round[4].s_box	684af5bc0acce85564bb0878242ed2ed
round[4].s_row	68cc08ed0abbd2bc642ef555244ae878
round[4].m_col	7a1e98bdacb6d1141a6944dd06eb2d3e
round[4].k_sch	58e151ab04a2a5557effb5416245080c
round[5].start	22ffc916a81474416496f19c64ae2532
round[5].s_box	9316dd47c2fa92834390a1de43e43f23
round[5].s_row	93faa123c2903f4743e4dd83431692de
round[5].m_col	aaa755b34cffe57cef6f98e1f01c13e6
round[5].k_sch	2ab54bb43a02f8f662e3a95d66410c08
round[6].start	80121e0776fd1d8a8d8c31bc965d1fee
round[6].s_box	cdc972c53854a47e5d64c765904cc028
round[6].s_row	cd54c7283864c0c55d4c727e90c9a465
round[6].m_col	921f748fd96e937d622d7725ba8ba50c
round[6].k_sch	f501857297448d7ebdf1c6ca87f33e3c
round[7].start	671ef1fd4e2a1e03dfdcb1ef3d789b30
round[7].s_box	8572a1542fe5727b9e86c8df27bc1404

round[7].s_row	85e5c8042f8614549ebca17b277272df
round[7].m_col	e913e7b18f507d4b227ef652758acbcc
round[7].k_sch	e510976183519b6934157c9ea351f1e0
round[8].start	0c0370d00c01e622166b8accd6db3a2c
round[8].s_box	fe7b5170fe7c8e93477f7e4bf6b98071
round[8].s_row	fe7c7e71fe7f807047b95193f67b8e4b
round[8].m_col	6cf5edf996eb0a069c4ef21cbfc25762
round[8].k_sch	1ea0372a995309167c439e77ff12051e
round[9].start	7255dad30fb80310e00d6c6b40d0527c
round[9].s_box	40fc5766766c7bcae1d7507f09700010
round[9].s_row	406c501076d70066e17057ca09fc7b7f
round[9].m_col	7478bcdce8a50b81d4327a9009188262
round[9].k_sch	dd7e0e887e2fff68608fc842f9dcc154
round[10].start	a906b254968af4e9b4bdb2d2f0c44336
round[10].s_box	d36f3720907ebf1e8d7a37b58c1c1a05
round[10].s_row	d37e3705907a1a208d1c371e8c6fbfb5
round[10].m_col	0d73cc2d8f6abe8b0cf2dd9bb83d422e
round[10].k_sch	859f5f237a8d5a3dc0c02952beefd63a
round[11].start	88ec930ef5e7e4b6cc32f4c906d29414
round[11].s_box	c4cedcabe694694e4b23bfdd6fb522fa
round[11].s_row	c494bffae62322ab4bb5dc4e6fce69dd
round[11].m_col	71d720933b6d677dc00b8f28238e0fb7
round[11].k_sch	de601e7827bcdf2ca223800fd8aeda32
round[12].start	afb73eeb1cd1b85162280f27fb20d585
round[12].s_box	79a9b2e99c3e6cd1aa3476cc0fb70397
round[12].s_row	793e76979c3403e9aab7b2d10fa96ccc

1.2.3.2 Inverse Cipher (DECRYPTION)

round[0].iinput	dda97ca4864cdfe06eaf70a0ec0d7191
round[0].ik_sch	a4970a331a78dc09c418c271e3a41d5d
round[1].istart	793e76979c3403e9aab7b2d10fa96ccc
round[1].is_box	afd10f851c28d5eb62203e51fbb7b827
round[1].is_row	afb73eeb1cd1b85162280f27fb20d585
round[1].im_col	122a02f7242ac8e20605afce51cc7264
round[1].ik_sch	d6bebd0dc209ea494db073803e021bb9
round[2].istart	c494bffae62322ab4bb5dc4e6fce69dd
round[2].is_box	88e7f414f532940eccd293b606ece4c9
round[2].is_row	88ec930ef5e7e4b6cc32f4c906d29414
round[2].im_col	5cc7aecce3c872194ae5ef8309a933c7
round[2].ik_sch	8fb999c973b26839c7f9d89d85c68c72
round[3].istart	d37e3705907a1a208d1c371e8c6fbfb5

round[3].is_box	a98ab23696bd4354b4c4b2e9f006f4d2
round[3].is_row	a906b254968af4e9b4bdb2d2f0c44336
round[3].im_col	b7113ed134e85489b20866b51d4b2c3b
round[3].ik_sch	f77d6ec1423f54ef5378317f14b75744
round[4].istart	406c501076d70066e17057ca09fc7b7f
round[4].is_box	72b86c7c0f0d52d3e0d0da104055036b
round[4].is_row	7255dad30fb80310e00d6c6b40d0527c
round[4].im_col	ef3b1be1b9b0e64bdcb79f1e0a707fbb
round[4].ik_sch	1147659047cf663b9b0ece8dfc0bf1f0
round[5].istart	fe7c7e71fe7f807047b95193f67b8e4b
round[5].is_box	0c018a2c0c6b3ad016db7022d603e6cc
round[5].is_row	0c0370d00c01e622166b8accd6db3a2c
round[5].im_col	592460b248832b2952e0b831923048f1
round[5].ik_sch	dcc1a8b667053f7dcc5c194ab5423a2e
round[6].istart	85e5c8042f8614549ebca17b277272df
round[6].is_box	672ab1304edc9bfddf78f1033d1e1eef
round[6].is_row	671ef1fd4e2a1e03dfdcb1ef3d789b30
round[6].im_col	0b8a7783417ae3a1f9492dc0c641a7ce
round[6].ik_sch	c6deb0ab791e2364a4055fbe568803ab
round[7].istart	cd54c7283864c0c55d4c727e90c9a465
round[7].is_box	80fd31ee768c1f078d5d1e8a96121dbc
round[7].is_row	80121e0776fd1d8a8d8c31bc965d1fee
round[7].im_col	4ee1ddf9301d6352c9ad769ef8d20515
round[7].ik_sch	dd1b7cdaf28d5c158a49ab1dbbc497cb
round[8].istart	93faa123c2903f4743e4dd83431692de
round[8].is_box	2214f132a896251664aec94164ff749c
round[8].is_row	22ffc916a81474416496f19c64ae2532
round[8].im_col	1008ffe53b36ee6af27b42549b8a7bb7
round[8].ik_sch	78c4f708318d3cd69655b701bfc093cf
round[9].istart	68cc08ed0abbd2bc642ef555244ae878
round[9].is_box	f727bf53a3fe7f788cc377eda65cc8c1
round[9].is_row	f75c7778a327c8ed8cfebfc1a6c37f53
round[9].im_col	7f69ac1ed939ebaac8ece3cb12e159e3
round[9].ik_sch	60dcef10299524ce62dbef152f9620cf
round[10].istart	1fb5430ef0accf64aa370cde3d77792c
round[10].is_box	cbd264d717aa5f8c62b2819c8b02af42
round[10].is_row	cb02818c17d2af9c62aa64428bb25fd7
round[10].im_col	cfaf16b2570c18b52e7fef50cab267ae
round[10].ik_sch	4b4ecbdb4d4dcfda5752d7c74949cbde
round[11].istart	84e1dd691a41d76f792d389783fbac70
round[11].is_box	4fe0c9e443f80d06affa76854163aad0
round[11].is_row	4f63760643e0aa85aff8c9d041fa0de4
round[11].im_col	794cf891177bfd1d8a327086f3831b39
round[11].ik_sch	1a1f181d1e1b1c194742c7d74949cbde

round[12].istart	6353e08c0960e104cd70b751bacad0e7
round[12].is_box	0050a0f04090e03080d02070c01060b0
round[12].is_row	00102030405060708090a0b0c0d0e0f0
round[12].ik_sch	000102030405060708090a0b0c0d0e0f
round[12].ioutput	00112233445566778899aabbccddeeff

1.2.4 AES-256

$$Nk = 8, Nr = 14$$
$$Plaintext = 00112233445566778899aabbccddeeff$$
$$Key = 000102030405060708090a0b0c0d0e0f$$
$$101112131415161718191a1b1c1d1e1f$$

1.2.4.1 Cipher (ENCRYPT)

round[0].input	00112233445566778899aabbccddeeff
round[0].k_sch	000102030405060708090a0b0c0d0e0f
round[1].start	00102030405060708090a0b0c0d0e0f0
round[1].s_box	63cab7040953d051cd60e0e7ba70e18c
round[1].s_row	6353e08c0960e104cd70b751bacad0e7
round[1].m_col	5f72641557f5bc92f7be3b291db9f91a
round[1].k_sch	101112131415161718191a1b1c1d1e1f
round[2].start	4f63760643e0aa85efa7213201a4e705
round[2].s_box	84fb386f1ae1ac97df5cfd237c49946b
round[2].s_row	84e1fd6b1a5c946fdf4938977cfbac23
round[2].m_col	bd2a395d2b6ac438d192443e615da195
round[2].k_sch	a573c29fa176c498a97fce93a572c09c
round[3].start	1859fbc28a1c00a078ed8aadc42f6109
round[3].s_box	adcb0f257e9c63e0bc557e951c15ef01
round[3].s_row	ad9c7e017e55ef25bc150fe01ccb6395
round[3].m_col	810dce0cc9db8172b3678c1e88a1b5bd
round[3].k_sch	1651a8cd0244beda1a5da4c10640bade
round[4].start	975c66c1cb9f3fa8a93a28df8ee10f63
round[4].s_box	884a33781fdb75c2d380349e19f876fb
round[4].s_row	88db34fb1f807678d3f833c2194a759e
round[4].m_col	b2822d81abe6fb275faf103a078c0033
round[4].k_sch	ae87dff00ff11b68a68ed5fb03fc1567
round[5].start	1c05f271a417e04ff921c5c104701554
round[5].s_box	9c6b89a349f0e18499fda678f2515920
round[5].s_row	9cf0a62049fd59a399518984f26be178
round[5].m_col	aeb65ba974e0f822d73f567bdb64c877
round[5].k_sch	6de1f1486fa54f9275f8eb5373b8518d
round[6].start	c357aae11b45b7b0a2c7bd28a8dc99fa
round[6].s_box	2e5bacf8af6ea9e73ac67a34c286ee2d
round[6].s_row	2e6e7a2dafc6eef83a86ace7c25ba934
round[6].m_col	b951c33c02e9bd29ae25cdb1efa08cc7
round[6].k_sch	c656827fc9a799176f294cec6cd5598b
round[7].start	7f074143cb4e243ec10c815d8375d54c
round[7].s_box	d2c5831a1f2f36b278fe0c4cec9d0329

round[7].s_row	d22f0c291ffe031a789d83b2ecc5364c
round[7].m_col	ebb19e1c3ee7c9e87d7535e9ed6b9144
round[7].k_sch	3de23a75524775e727bf9eb45407cf39
round[8].start	d653a4696ca0bc0f5acaab5db96c5e7d
round[8].s_box	f6ed49f950e06576be74624c565058ff
round[8].s_row	f6e062ff507458f9be50497656ed654c
round[8].m_col	5174c8669da98435a8b3e62ca974a5ea
round[8].k_sch	0bdc905fc27b0948ad5245a4c1871c2f
round[9].start	5aa858395fd28d7d05e1a38868f3b9c5
round[9].s_box	bec26a12cfb55dff6bf80ac4450d56a6
round[9].s_row	beb50aa6cff856126b0d6aff45c25dc4
round[9].m_col	0f77ee31d2ccadc05430a83f4ef96ac3
round[9].k_sch	45f5a66017b2d387300d4d33640a820a
round[10].start	4a824851c57e7e47643de50c2af3e8c9
round[10].s_box	d61352d1a6f3f3a04327d9fee50d9bdd
round[10].s_row	d6f3d9dda6279bd1430d52a0e513f3fe
round[10].m_col	bd86f0ea748fc4f4630f11c1e9331233
round[10].k_sch	7ccff71cbeb4fe5413e6bbf0d261a7df
round[11].start	c14907f6ca3b3aa070e9aa313b52b5ec
round[11].s_box	783bc54274e280e0511eacc7e200d5ce
round[11].s_row	78e2acce741ed5425100c5e0e23b80c7
round[11].m_col	af8690415d6e1dd387e5fbedd5c89013
round[11].k_sch	f01afafee7a82979d7a5644ab3afe640
round[12].start	5f9c6abfbac634aa50409fa766677653
round[12].s_box	cfde0208f4b418ac5309db5c338538ed
round[12].s_row	cfb4dbedf4093808538502ac33de185c
round[12].m_col	7427fae4d8a695269ce83d315be0392b
round[12].k_sch	2541fe719bf500258813bbd55a721c0a
round[13].start	516604954353950314fb86e401922521
round[13].s_box	d133f22a1aed2a7bfa0f44697c4f3ffd
round[13].s_row	d1ed44fd1a0f3f2afa4ff27b7c332a69
round[13].m_col	2c21a820306f154ab712c75eee0da04f
round[13].k_sch	4e5a6699a9f24fe07e572baacdf8cdea
round[14].start	627bceb9999d5aaac945ecf423f56da5
round[14].s_box	aa218b56ee5ebeacdd6ecebf26e63c06
round[14].s_row	aa5ece06ee6e3c56dde68bac2621bebf
round[14].k_sch	24fc79ccbf0979e9371ac23c6d68de36
round[14].output	8ea2b7ca516745bfeafc49904b496089

1.2.4.2 Inverse Cipher (DECRYPT)

round[0].iinput	8ea2b7ca516745bfeafc49904b496089

round[0].ik_sch	24fc79ccbf0979e9371ac23c6d68de36
round[1].istart	aa5ece06ee6e3c56dde68bac2621bebf
round[1].is_box	629deca599456db9c9f5ceaa237b5af4
round[1].is_row	627bceb9999d5aaac945ecf423f56da5
round[1].im_col	e51c9502a5c1950506a61024596b2b07
round[1].ik_sch	34f1d1ffbfceaa2ffce9e25f2558016e
round[2].istart	d1ed44fd1a0f3f2afa4ff27b7c332a69
round[2].is_box	5153862143fb2595149204030166 95e4
round[2].is_row	516604954353950314fb86e401922521
round[2].im_col	91a29306cc450d0226f4b5eaef5efed8
round[2].ik_sch	5e1648eb384c350a7571b746dc80e684
round[3].istart	cfb4dbedf4093808538502ac33de185c
round[3].is_box	5fc69f53ba4076bf50676aaa669c34a7
round[3].is_row	5f9c6abfbac634aa50409fa766677653
round[3].im_col	b041a94eff21ae9212278d903b8a63f6
round[3].ik_sch	c8a305808b3f7bd043274870d9b1e331
round[4].istart	78e2acce741ed5425100c5e0e23b80c7
round[4].is_box	c13baaeccae9b5f6705207a03b493a31
round[4].is_row	c14907f6ca3b3aa070e9aa313b52b5ec
round[4].im_col	638357cec07de6300e30d0ec4ce2a23c
round[4].ik_sch	b5708e13665a7de14d3d824ca9f151c2
round[5].istart	d6f3d9dda6279bd1430d52a0e513f3fe
round[5].is_box	4a7ee5c9c53de85164f348472a827e0c
round[5].is_row	4a824851c57e7e47643de50c2af3e8c9
round[5].im_col	ca6f71058c642842a315595fdf54f685
round[5].ik_sch	74da7ba3439c7e50c81833a09a96ab41
round[6].istart	beb50aa6cff856126b0d6aff45c25dc4
round[6].is_box	5ad2a3c55fe1b93905f3587d68a88d88
round[6].is_row	5aa858395fd28d7d05e1a38868f3b9c5
round[6].im_col	ca46f5ea835eab0b9537b6dbb221b6c2
round[6].ik_sch	3ca69715d32af3f22b67ffade4ccd38e
round[7].istart	f6e062ff507458f9be50497656ed654c
round[7].is_box	d6a0ab7d6cca5e695a6ca40fb953bc5d
round[7].is_row	d653a4696ca0bc0f5acaab5db96c5e7d
round[7].im_col	2a70c8da28b806e9f319ce42be4baead
round[7].ik_sch	f85fc4f3374605f38b844df0528e98e1
round[8].istart	d22f0c291ffe031a789d83b2ecc5364c
round[8].is_box	7f4e814ccb0cd543c175413e8307245d
round[8].is_row	7f074143cb4e243ec10c815d8375d54c
round[8].im_col	f0073ab7404a8a1fc2cba0b80df08517
round[8].ik_sch	de69409aef8c64e7f84d0c5fcfab2c23
round[9].istart	2e6e7a2dafc6eef83a86ace7c25ba934
round[9].is_box	c345bdfa1bc799e1a2dcaab0a857b728
round[9].is_row	c357aae11b45b7b0a2c7bd28a8dc99fa

round[9].im_col	3225fe3686e498a32593c1872b613469
round[9].ik_sch	aed55816cf19c100bcc24803d90ad511
round[10].istart	9cf0a62049fd59a399518984f26be178
round[10].is_box	1c17c554a4211571f970f24f0405e0c1
round[10].is_row	1c05f271a417e04ff921c5c104701554
round[10].im_col	9d1d5c462e655205c4395b7a2eac55e2
round[10].ik_sch	15c668bd31e5247d17c168b837e6207c
round[11].istart	88db34fb1f807678d3f833c2194a759e
round[11].is_box	979f2863cb3a0fc1a9e166a88e5c3fdf
round[11].is_row	975c66c1cb9f3fa8a93a28df8ee10f63
round[11].im_col	d24bfb0e1f997633cfce86e37903fe87
round[11].ik_sch	7fd7850f61cc991673db890365c89d12
round[12].istart	ad9c7e017e55ef25bc150fe01ccb6395
round[12].is_box	181c8a098aed61c2782ffba0c45900ad
round[12].is_row	1859fbc28a1c00a078ed8aadc42f6109
round[12].im_col	aec9bda23e7fd8aff96d74525cdce4e7
round[12].ik_sch	2a2840c924234cc026244cc5202748c4
round[13].istart	84e1fd6b1a5c946fdf4938977cfbac23
round[13].is_box	4fe0210543a7e706efa476850163aa32
round[13].is_row	4f63760643e0aa85efa7213201a4e705
round[13].im_col	794cf891177bfd1ddf67a744acd9c4f6
round[13].ik_sch	1a1f181d1e1b1c191217101516131411
round[14].istart	6353e08c0960e104cd70b751bacad0e7
round[14].is_box	0050a0f04090e03080d02070c01060b0
round[14].is_row	00102030405060708090a0b0c0d0e0f0
round[14].ik_sch	000102030405060708090a0b0c0d0e0f
round[14].ioutput	00112233445566778899aabbccddeeff

Chapter 2

Evaluation

2.1 Looking Back

2.2 The Web Application

2.3 The AES Algorithm

2.4 What I would do differently

2.5 Final Evaluation

List of Figures

List of Tables