Daniel Frey

CS 4920-001

Assignment 4

3/19/18

**Problem 1:**

**a.** Blocks beyond P2 will not be affected if there’s an error in C1. C1 only has dependence for P1 and P2. P3 does not depend on C1, but rather C2 and C3.

P1 = D(K, C1) ⊕ IV

P2 = D(K, C2) ⊕ C1

P3 = D(K, C3)⊕ C2

**b.** If there’s an error in P1, then the error propagates through all the ciphertext blocks, since all cipher blocks will depend on P1. The receiver, however, will end up with the correct plaintext for all blocks except P1 that started off with an error.

C1 = E(K, [P1 ⊕ IV])

C2 = E(K, [C1 ⊕ P2]), then Ci = E(K, [Ci-1 ⊕ Pi])

**Problem 2:**

**a.** The sequence for *a* = 3 is: 1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1

Period = 30

*a* = 32: 1, 9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1, 9, 19, 16, 20, 25, 8, 10, 28, 4, 5, 14, 2, 18, 7, 1

Period = 15

*a* = 33: 1, 27, 16, 29, 8, 30, 4, 15, 2, 23, 1, 27, 16, 29, 8, 30, 4, 15, 2, 23, 1, 27, 16, 29, 8, 30, 4, 15, 2, 23, 1

Period = 10

*a* = 34: 1, 19, 20, 8, 28, 5, 2, 7, 9, 16, 25, 10, 4, 14, 18, 1, 19, 20, 8, 25, 4, 2, 7, 9, 16, 25, 10, 4, 14, 18, 1

Period = 15

**b.** Maximum period for *m* = 24 is 24–2 = 4

**c.** *a* must be 5 or 11 to achieve the maximum period.

**d.** The seed must be odd.

**Problem 3:**

**a.** Simply storing i, j, and S, will require 8 + 8 + (256 × 8) = 2064 bits in a straightforward scheme.

**b.** The number of states is log2(256! × 2562) ≈ 21700. Therefore, 1700 bits are required to represent the state.

**Problem 4**

**a.** Credit: Lawrie Brown. Java in applet.

**b.** for (col = 0; col < NUM\_COLS; col++) {

i = col \* COL\_SIZE; // start index for this col

ta[i] = (byte)(mul(2,a[i]) ^ mul(3,a[i+1]) ^ a[i+2] ^ a[i+3]);

ta[i+1] = (byte)(a[i] ^ mul(2,a[i+1]) ^ mul(3,a[i+2]) ^ a[i+3]);

ta[i+2] = (byte)(a[i] ^ a[i+1] ^ mul(2,a[i+2]) ^ mul(3,a[i+3]));

ta[i+3] = (byte)(mul(3,a[i]) ^ a[i+1] ^ a[i+2] ^ mul(2,a[i+3]));

}

For each column, there is a multiplication and bitwise XOR performed on the elements.

**c.**

|  |  |
| --- | --- |
| **Key Words** | **Key** |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w0 = | 0f | 15 | 71 | c9 | | w1 = | 47 | d9 | e8 | 59 | | w2 = | 1c | b7 | ad | d6 | | w3 = | af | 7f | 67 | 98 | | 0f1571c947d9e8591cb7add6af7f6798 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w4 = | dc | 90 | 37 | b0 | | w5 = | 9b | 49 | df | e9 | | w6 = | 87 | fe | 72 | 3f | | w7 = | 28 | 81 | 15 | a7 | | dc9037b09b49dfe987fe723f288115a7 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w8 = | d2 | c9 | 6b | 84 | | w9 = | 49 | 80 | b4 | 6d | | w10= | ce | 7e | c6 | 52 | | w11= | e6 | ff | d3 | f5 | | d2c96b844980b46dce7ec652e6ffd3f5 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w12= | c0 | af | 8d | 0a | | w13= | 89 | 2f | 39 | 67 | | w14= | 47 | 51 | ff | 35 | | w15= | a1 | ae | 2c | c0 | | c0af8d0a892f39674751ff35a1ae2cc0 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w16= | 2c | de | 37 | 38 | | w17= | a5 | f1 | 0e | 5f | | w18= | e2 | a0 | f1 | 6a | | w19= | 43 | 0e | dd | aa | | 2cde3738a5f10e5fe2a0f16a430eddaa |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w20= | 97 | 1f | 9b | 22 | | w21= | 32 | ee | 95 | 7d | | w22= | d0 | 4e | 64 | 17 | | w23= | 93 | 40 | b9 | bd | | 971f9b2232ee957dd04e64179340b9bd |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w24= | be | 49 | e1 | f3 | | w25= | 8c | a7 | 74 | 83 | | w26= | 5c | e9 | 10 | 94 | | w27= | cf | a9 | a9 | 29 | | be49e1fe8ca774835ce91094cfa9a929 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w28= | 2d | 9a | 44 | 74 | | w29= | a1 | 3d | 30 | f7 | | w30= | fd | d4 | 20 | 63 | | w31= | 32 | 7d | 89 | 4a | | 2d9a4474a13d30f7fdd42063327d894a |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w32= | 52 | 3d | 92 | 57 | | w33= | f3 | 00 | a2 | a0 | | w34= | 0e | d4 | 82 | c3 | | w35= | 3c | a9 | 0b | 89 | | 523d9257f300a2a00ed482c33ca90b89 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w36= | 9a | 16 | 35 | bc | | w37= | 69 | 16 | 97 | 1c | | w38= | 67 | c2 | 15 | df | | w39= | 5b | 6b | 1e | 56 | | 9a1635bc6916971c67c215df5b6b1e56 |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | w40= | d3 | 64 | 84 | 85 | | w41= | ba | 72 | 13 | 99 | | w42= | dd | b0 | 06 | 46 | | w43= | 86 | db | 18 | 10 | | d3648485ba721399ddb0064686db1810 |

**d.**

|  |  |
| --- | --- |
| **Start of Round** | **Round Key** |
| 01 23 45 67  89 ab cd ef  fe dc ba 98  76 54 32 10 | |  |  |  |  | | --- | --- | --- | --- | | 0f | 15 | 71 | c9 | | 47 | d9 | e8 | 59 | | 1c | b7 | ad | d6 | | af | 7f | 67 | 98 | |
| 0e 36 34 ae  ce 72 25 b6  e2 6b 17 4e  d9 2b 55 88 | |  |  |  |  | | --- | --- | --- | --- | | dc | 90 | 37 | b0 | | 9b | 49 | df | e9 | | 87 | fe | 72 | 3f | | 28 | 81 | 15 | a7 | |
| 65 74 70 75  0f c7 ff 3f  f2 f9 f9 f9  5d d0 2a 9c | |  |  |  |  | | --- | --- | --- | --- | | d2 | c9 | 6b | 84 | | 49 | 80 | b4 | 6d | | ce | 7e | c6 | 52 | | e6 | ff | d3 | f5 | |
| 5e 7d b0 ab  6d 76 36 aa  73 91 02 19  5c 2f 91 8c | |  |  |  |  | | --- | --- | --- | --- | | c0 | af | 8d | 0a | | 89 | 2f | 39 | 67 | | 47 | 51 | ff | 35 | | a1 | ae | 2c | c0 | |
| 2b 7a af 65  8a f0 3b e7  36 6a 5f 0e  fe da f4 57 | |  |  |  |  | | --- | --- | --- | --- | | 2c | de | 37 | 38 | | a5 | f1 | 0e | 5f | | e2 | a0 | f1 | 6a | | 43 | 0e | dd | aa | |
| ce 3d 22 c5  ad 1c c0 fa  fc 14 f6 78  12 8c 85 09 | |  |  |  |  | | --- | --- | --- | --- | | 97 | 1f | 9b | 22 | | 32 | ee | 95 | 7d | | d0 | 4e | 64 | 17 | | 93 | 40 | b9 | bd | |
| 66 70 0b 78  27 90 3e e3  b9 b5 fa 71  75 ae e7 03 | |  |  |  |  | | --- | --- | --- | --- | | be | 49 | e1 | f3 | | 8c | a7 | 74 | 83 | | 5c | e9 | 10 | 94 | | cf | a9 | a9 | 29 | |
| 2e b6 65 10  43 c1 81 ee  fd 00 c7 83  0c f8 e4 2b | |  |  |  |  | | --- | --- | --- | --- | | 2d | 9a | 44 | 74 | | a1 | 3d | 30 | f7 | | fd | d4 | 20 | 63 | | 32 | 7d | 89 | 4a | |
| f0 fb 92 60  93 90 de 5c  f3 fd d7 c3  e7 e7 0e d2 | |  |  |  |  | | --- | --- | --- | --- | | 52 | 3d | 92 | 57 | | f3 | 00 | a2 | a0 | | 0e | d4 | 82 | c3 | | 3c | a9 | 0b | 89 | |
| 4a d6 a6 c7  d7 42 0c 9b  b6 71 5b 9b  2d 2a d8 60 | |  |  |  |  | | --- | --- | --- | --- | | 9a | 16 | 35 | bc | | 69 | 16 | 97 | 1c | | 67 | c2 | 15 | df | | 5b | 6b | 1e | 56 | |
| b0 03 d6 73  2c 20 a9 5b  ff 25 ca e4  1b 49 eb 05 | |  |  |  |  | | --- | --- | --- | --- | | d3 | 64 | 84 | 85 | | ba | 72 | 13 | 99 | | dd | b0 | 06 | 46 | | 86 | db | 18 | 10 | |
| 34 d3 f0 ee  cb 4d fa 16  cb 8b f0 7f  29 a0 cb 79 |  |

**Problem 5:**

**a**. The avalanche effect is a property such that a small change in either the plaintext or the key produces a drastic change in the ciphertext. Ideally, you want approximately half of the bits to differ.

**b.**

|  |  |  |
| --- | --- | --- |
| **Round** | **State** | **Num. Bits that Differ** |
|  | 1. 0123456789abcdeffedcba9876543210 2. **1**123456789abcdeffedcba9876543210 | 1 |
| 0 | 0e3634aece7225b6e26b174ed92b5588  1e3634aece7225b6e26b174ed92b5588 | 1 |
| 1 | 657470750fc7ff3ff2f9f9f95dd02a9c  ccada9050fc7ff3ff2f9f9f95dd02a9c | 17 |
| 2 | 5e7db0ab6d7636aa739102195c2f918c  527bb6a19b80375df10c1d9b5521968b | 53 |
| 3 | 2b7aaf658af03be7366a5f0efedaf457  15e454191a45be51008febe6afb1e24c | 69 |
| 4 | ce3d22c5ad1cc0fafc14f678128c8509  ec52b20623d293fa96f9729e2ac203e1 | 58 |
| 5 | 66700b7827903ee3b9b5fa7175aee703  6c987375da036d2b9ee0c8f495d1e243 | 58 |
| 6 | 2eb6651043c181eefd00c7830cf8e42b  61d62fa91f07552276e528c1d2f46748 | 64 |
| 7 | f0fb92609390de5cf3fdd7c3e7e70ed2  daeaf00b1c13564dd12523bcc658a174 | 62 |
| 8 | 4ad6a6c7d7420c9bb6715b9b2d2ad860  cf6859ca889f1844a352ebba09a5eeb2 | 67 |
| 9 | b003d6732c20a95bff25cae41b49eb05  3d26f465a6de9f8ba999b93acff81c4e | 68 |
| 10 | 34d3f0eecb4dfa16cb8bf07f29a0cb79  f479d2aa9e9c8fd40ef1b97b0c2cc390 | 51 |

|  |  |  |
| --- | --- | --- |
| **Round** | **State** | **Num. Bits that Differ** |
|  | 1. 0123456789abcdeffedcba9876543210 2. 0123456789abcdeffedcba987654321**1** | 1 |
| 0 | 0e3634aece7225b6e26b174ed92b5588  0e3634aece7225b6e26b174ed92b5589 | 1 |
| 1 | 657470750fc7ff3ff2f9f9f95dd02a9c  0617d5b30fc7ff3ff2f9f9f95dd02a9c | 16 |
| 2 | 5e7db0ab6d7636aa739102195c2f918c  1a5f92cd9d863d512167a64bfaebf3ee | 56 |
| 3 | 2b7aaf658af03be7366a5f0efedaf457  5fc15bc711ca246c18651d3625dc4e22 | 67 |
| 4 | ce3d22c5ad1cc0fafc14f678128c8509  029d719f845ece375b015899869ef9af | 58 |
| 5 | 66700b7827903ee3b9b5fa7175aee703  821feb7b4a22e9d48605bedb9cd08763 | 65 |
| 6 | 2eb6651043c181eefd00c7830cf8e42b  6375301bb0bf84dce525355194775be7 | 65 |
| 7 | f0fb92609390de5cf3fdd7c3e7e70ed2  da4427cfa3407086d27695f5444ee057 | 65 |
| 8 | 4ad6a6c7d7420c9bb6715b9b2d2ad860  965d753bc4c8cc688634576c90919839 | 65 |
| 9 | b003d6732c20a95bff25cae41b49eb05  cbb2cd80dd1222b9af663e85541e5451 | 69 |
| 10 | 34d3f0eecb4dfa16cb8bf07f29a0cb79  ccad36547b413354a4c2bb10a6ec8b87 | 66 |

|  |  |  |
| --- | --- | --- |
| **Round** | **State** | **Num. Bits that Differ** |
|  | 1. 0123456789abcdeffedcba9876543210 2. 0123456789**b**bcdeffedcba9876543210 | 1 |
| 0 | 0e3634aece7225b6e26b174ed92b5588  0e3634aece6225b6e26b174ed92b5588 | 1 |
| 1 | 657470750fc7ff3ff2f9f9f95dd02a9c  40bb9a9f0fc7ff3ff2f9f9f95dd02a9c | 19 |
| 2 | 5e7db0ab6d7636aa739102195c2f918c  d639f4672b30fc269ab1cbf0d4dfe9f4 | 52 |
| 3 | 2b7aaf658af03be7366a5f0efedaf457  9bcf9b75a8f2a8a8dde3be323b8582b9 | 62 |
| 4 | ce3d22c5ad1cc0fafc14f678128c8509  7c7c178f87b947210faad22ef89d4f99 | 61 |
| 5 | 66700b7827903ee3b9b5fa7175aee703  16898536045ea88ad372abc2b0ebe0ac | 66 |
| 6 | 2eb6651043c181eefd00c7830cf8e42b  2b89923457e81025599a28bc0f631934 | 69 |
| 7 | f0fb92609390de5cf3fdd7c3e7e70ed2  4e026ee308724846161ccfef837e7877 | 67 |
| 8 | 4ad6a6c7d7420c9bb6715b9b2d2ad860  b3e2f61d81dd5ef24b8efdd2eb824e26 | 69 |
| 9 | b003d6732c20a95bff25cae41b49eb05  bbe9336bd1fd2b6de418b149ccf41bc7 | 73 |
| 10 | 34d3f0eecb4dfa16cb8bf07f29a0cb79  39304c4384dfbce6b40fc57acdc5e92b | 61 |