**Advanced Security 1 – DT211-4, DT282-4 and DT228-4**

**Assignment (5 Mark)**

**Part A**

Write a Java program (or any other programming language you are happy to use) which will test if the given number is a prime number or no. In order to achieve this you have to implement the Miller-Rabin Algorithm as shown below

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

**Part A**

Write a Java program (or any other programming language you are happy to use) to perform the Key Expansion of AES algorithm as shown below. You don't need to implement the whole AES algorithm.

```
KeyExpansion (byte key[16], word w[44])
{
    word temp
    for (i = 0; i < 4; i++)   w[i] = (key[4*i], key[4*i+1],
                                      key[4*i+2],
                                      key[4*i+3]);
     for (i = 4; i < 44; i++)
     {
      temp = w[i - 1];
      if (i mod 4 = 0)   temp = SubWord (RotWord (temp))
                               ⊕ Rcon[i/4];
      w[i] = w[i-4] ⊕ temp
     }
}
```

The input will be 16 byte Key: **0f1571c947d9e8590cb7add6af7f6798**

The output will be **keywords** (w0 to w43) as shown in the table below.

| Key Words | Auxiliary Function |
|---|---|
| w0 = 0f 15 71 c9<br>w1 = 47 d9 e8 59<br>w2 = 0c b7 ad d6<br>w3 = af 7f 67 98 | RotWord(w3)= 7f 67 98 af = x1<br>SubWord(x1)= d2 85 46 79 = y1<br>Rcon(1)= 01 00 00 00<br>y1 ⊕ Rcon(1)= d3 85 46 79 = z1 |
| w4 = w0 ⊕ z1 = dc 90 37 b0<br>w5 = w4 ⊕ w1 = 9b 49 df e9<br>w6 = w5 ⊕ w2 = 97 fe 72 3f<br>w7 = w6 ⊕ w3 = 38 81 15 a7 | RotWord(w7)= 81 15 a7 38 = x2<br>SubWord(x4)= 0c 59 5c 07 = y2<br>Rcon(2)= 02 00 00 00<br>y2 ⊕ Rcon(2)= 0e 59 5c 07 = z2 |
| w8 = w4 ⊕ z2 = d2 c9 6b b7<br>w9 = w8 ⊕ w5 = 49 80 b4 5e<br>w10 = w9 ⊕ w6 = de 7e c6 61<br>w11 = w10 ⊕ w7 = e6 ff d3 c6 | RotWord(w11)= ff d3 c6 e6 = x3<br>SubWord(x2)= 16 66 b4 8e = y3<br>Rcon(3)= 04 00 00 00<br>y3 ⊕ Rcon(3)= 12 66 b4 8e = z3 |
| w12 = w8 ⊕ z3 = c0 af df 39<br>w13 = w12 ⊕ w9 = 89 2f 6b 67<br>w14 = w13 ⊕ w10 = 57 51 ad 06<br>w15 = w14 ⊕ w11 = b1 ae 7e c0 | RotWord(w15)= ae 7e c0 b1 = x4<br>SubWord(x3)= e4 f3 ba c8 = y4<br>Rcon(4)= 08 00 00 00<br>y4 ⊕ Rcon(4)= ec f3 ba c8 = 4 |
| w16 = w12 ⊕ z4 = 2c 5c 65 f1<br>w17 = w16 ⊕ w13 = a5 73 0e 96<br>w18 = w17 ⊕ w14 = f2 22 a3 90<br>w19 = w18 ⊕ w15 = 43 8c dd 50 | RotWord(w19)= 8c dd 50 43 = x5<br>SubWord(x4)= 64 c1 53 1a = y5<br>Rcon(5)= 10 00 00 00<br>y5 ⊕ Rcon(5)= 74 c1 53 1a = z5 |
| w20 = w16 ⊕ z5 = 58 9d 36 eb<br>w21 = w20 ⊕ w17 = fd ee 38 7d<br>w22 = w21 ⊕ w18 = 0f cc 9b ed<br>w23 = w22 ⊕ w19 = 4c 40 46 bd | RotWord(w23)= 40 46 bd 4c = x6<br>SubWord(x5)= 09 5a 7a 29 = y6<br>Rcon(6)= 20 00 00 00<br>y6 ⊕ Rcon(6)= 29 5a 7a 29 = z6 |
| w24 = w20 ⊕ z6 = 71 c7 4c c2<br>w25 = w24 ⊕ w21 = 8c 29 74 bf<br>w26 = w25 ⊕ w22 = 83 e5 ef 52<br>w27 = w26 ⊕ w23 = cf a5 a9 ef | RotWord(w27)= a5 a9 ef cf = x7<br>SubWord(x6)= 06 d3 df 8a = y7<br>Rcon(7)= 40 00 00 00<br>y7 ⊕ Rcon(7)= 46 d3 df 8a = z7 |
| w28 = w24 ⊕ z7 = 37 14 93 48<br>w29 = w28 ⊕ w25 = bb 3d e7 f7<br>w30 = w29 ⊕ w26 = 38 d8 08 a5<br>w31 = w30 ⊕ w27 = f7 7d a1 4a | RotWord(w31)= 7d a1 4a f7 = x8<br>SubWord(x7)= ff 32 d6 68 = y8<br>Rcon(8)= 80 00 00 00<br>y8 ⊕ Rcon(8)= 7f 32 d6 68 = z8 |
| w32 = w28 ⊕ z8 = 48 26 45 20<br>w33 = w32 ⊕ w29 = f3 1b a2 d7<br>w34 = w33 ⊕ w30 = cb c3 aa 72<br>w35 = w34 ⊕ w32 = 3c be 0b 38 | RotWord(w35)= be 0b 38 3c = x9<br>SubWord(x8)= ae 2b 07 eb = y9<br>Rcon(9)= 1B 00 00 00<br>y9 ⊕ Rcon(9)= b5 2b 07 eb = z9 |
| w36 = w32 ⊕ z9 = fd 0d 42 cb<br>w37 = w36 ⊕ w33 = 0e 16 e0 1c<br>w38 = w37 ⊕ w34 = c5 d5 4a 6e<br>w39 = w38 ⊕ w35 = f9 6b 41 56 | RotWord(w39)= 6b 41 56 f9 = x10<br>SubWord(x9)= 7f 83 b1 99 = y10<br>Rcon(10)= 36 00 00 00<br>y10 ⊕ Rcon(10)= 49 83 b1 99 = z10 |
| w40 = w36 ⊕ z10 = b4 8e f3 52<br>w41 = w40 ⊕ w37 = ba 98 13 4e<br>w42 = w41 ⊕ w38 = 7f 4d 59 20<br>w43 = w42 ⊕ w39 = 86 26 18 76 | |

**Table 5.3** Key Expansion for AES Example