

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

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

Table 5.3 Key Expansion for AES Example