Exercise Sheet 10 for

FAULT ATTACKS AND COUNTERMEASURES

Homework Problems Due: Wednesday, November 18, 23:59

Exercises

Exercise 1: Reversing Key Schedule in AES
Write an algorithm that does inverse Key Schedule in AES, i.e. given the 10^{th} round key, it will generate the 9^{th}, 8^{th}, 7^{th} ... round keys in reverse order.

Exercise 2: Fault attack on CRT-RSA
Study the example on CRT-RSA given in the Lecture Slides. Work out the same example with some other sets of values. For example you may try:
• $p = 17, q = 31, e = 7$. Calculate the values of d, d_p, d_q, s_p, s_q, s. In the next phase corrupt s_q tp some random value s_q^* and try to find the factors of n.

Compulsory Homework Problem

Fault attack on AES with fault in 8th round
Consider the situation in which the first byte of the AES-128 state is faulted at the beginning of the 8th round. The task will be to identify a strategy to guess one of the round keys in this case.

- Prove that the difference between the correct and faulty state at the end of round 8 is of the form:

$$\begin{pmatrix} \Delta_1 & 0 & 0 & 0 \\ \Delta_2 & 0 & 0 & 0 \\ \Delta_3 & 0 & 0 & 0 \\ \Delta_4 & 0 & 0 & 0 \end{pmatrix}$$

- Prove that the difference between the correct and faulty state at the end of round 9 is of the form:

$$\begin{pmatrix} 2\Delta_1 & \Delta_4 & \Delta_3 & 3\Delta_2 \\ \Delta_1 & \Delta_4 & 3\Delta_3 & 2\Delta_2 \\ \Delta_1 & 3\Delta_4 & 2\Delta_3 & \Delta_2 \\ 3\Delta_1 & 2\Delta_4 & \Delta_3 & \Delta_2 \end{pmatrix}$$

- Hence or otherwise devise a strategy to find the 10^{th} round key.