Exercise Sheet 8

Rainbow Tables

Obligatory homework this week: Exercise 3. Hand-in by November 7, 23:59.

Exercise 1: Success Probability
In general, the success probability of the Rainbow Table method, mt rows and t columns, is given by the formula:

$$P_R = 1 - \left(\frac{2}{2 + \frac{mt^2}{2^l}} \right)^2 . \tag{1}$$

Here, l is the size the key in bits.

Consider a version of AES-128 where 104 bits of the input are fixed to zero, i.e. the effective key-length is 24 bits. Let $m = 2^8$. Plot the success probability as a function of t. What parameter of t seem reasonable to you? How does this relate to the online and memory complexity? How does this compare to Hellman Tables?

Exercise 2: Multiple Rainbow Tables
A possible extension of Rainbow Tables is to use multiple tables with different reduction functions. The success probability of this approach is given by

$$P_R = 1 - \left(\frac{2}{2 + \frac{mt^2}{2^l}} \right)^{2\ell} .$$

What is the optimal number of tables to use? Consider the pre-computation, memory, and online costs.

Exercise 3: Coverage of Rainbow Tables
Consider the 24-bit key version of AES-128 described in Exercise 1. Create a function

$$f(k) : [0, 2^{24} - 1] \rightarrow [0, 2^{24} - 1]$$

which encrypts a fixed plaintext with AES-128 using the 24-bit key k, and then restricts the output to 24 bits (e.g. by throwing away the last 104 bits). Then define $f_i(k) = (f(k)+i) \mod 2^{24}$.

Your task is now to calculate the coverage of a Rainbow Table for this version of AES. The i'th column should use $f_i(k)$ as its reduction function.

Using the results of Exercise 1, choose a reasonable value for m. Keep track of how many points in $[0, 2^{24} - 1]$ the tables cover, for each iteration of $f_i(k)$ (i.e. each step of the $m \cdot t$ chains). Make a graph over how the number of covered points develops over time. Does the graph match the predictions made by Equation 1? (Remember that the coverage is just $P_R \cdot 2^l$) How does this compare to the coverage of your Hellman Tables?.

Your hand-in (via CampusNet) should include:

1. source code of your Rainbow Table implementation,
2. a short report containing your results and discussion of these.

Group work is strongly encouraged, but please make sure to hand in individually.