Modern Cryptology - TMTO Attack

Anders Lammert Hartmann (s153596)

Amalie Due Jensen (s160503)

April 23, 2021

1 Introduction

In this report we examine the Time-Memory-Trade-Off (TMTO) attack using two different types of tables. First, we use Hellman-tables to see how many possible key-values are covered in the tables using certain parameters. More specifically we will fix the number of rows in each table and the number of tables and see how the point coverage develops as more and more columns are added to each table. The result will be compared with the theoretical probability of success when using Hellman-tables. Furthermore another TMTO attack using rainbow tables will be examined. Here only a single table will be used. We will then fix the number of rows in the table and see how many points are covered as a function of the number of columns used in the table. Again this will be compared to the theoretical success probability when using rainbow tables.

The code used for the exercises can be found at `https://github.com/AmalieDue/TMTO-attack`

2 Hellman tables

In this section we will cover the three exercises about Hellman tables.

2.1 Exercise 1

The success probability using ℓ Hellman tables with m rows, t columns, and effective key size l is given by

$$P_H = 1 - \exp\left(-\sqrt{\frac{2 \cdot m \cdot \ell^2}{2^l}} \cdot \frac{\exp\left(\sqrt{\frac{2 \cdot m \cdot \ell^2}{2^l}} - 1\right)}{\exp\left(\sqrt{\frac{2 \cdot m \cdot \ell^2}{2^l}} + 1\right)}\right) \tag{2.1}$$

We will consider AES with an effective key size of 24. Hence $l = 24$. Now first we will see how the probability changes as a function of m. To do this we let $\ell = 2^8$ and let

$$m \cdot t \cdot \ell = 2^{24} \implies t = \frac{2^{24}}{2^8 \cdot m} \tag{2.2}$$

Plotting the success probability as a function of m yields

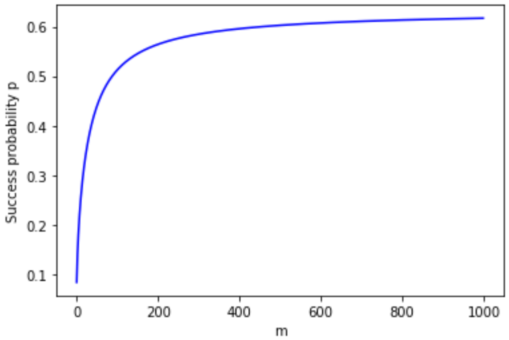


Figure 1: The probability of success using Hellman tables as a function of m (the number of rows)

In this plot it can be seen that the success probability converges to approximately 0.62. This is to be expected since mathematical theory states that the longest cycle will contain 0.62 percent of the possible keys.

2.2 Exercise 2

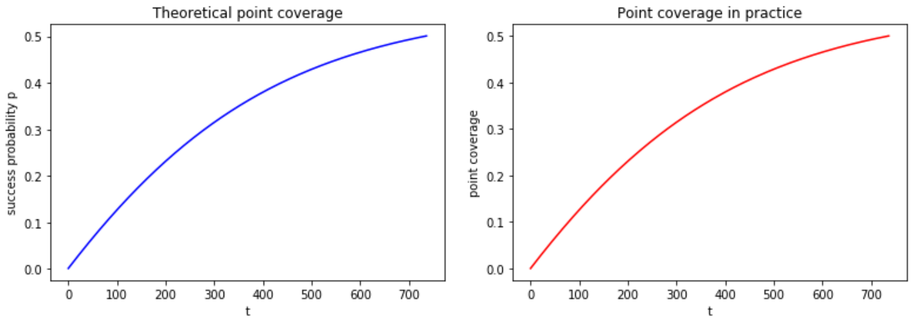
In this exercise we will calculate reasonable values for m and t such that a time-memory trade off occurs and the success probability is good enough. We will consider the case where we want the success probability to be 0.5. Solving $P_H = 0.5$ in equation (2.1) for m gives $m = 89$ and $t = 737$. Now we want $m \cdot t^2 \approx 2^l$ to achieve the best use of Hellman tables. In this case we have

$$89 \cdot 737^2 \approx 3 \cdot 2^{24} \tag{2.3}$$

So we are a factor of 3 away from this. This we consider to be okay. Just to mention it if we had said the success probability to 0.575 then m would increase, t would decrease and $m \cdot t^2 \approx 2^{24}$.

2.3 Exercise 3

In this exercise, we implement a set of Hellman tables and calculate the coverage in the tables. We use the parameters $m = 89$, $t = 737$, $\ell = 2^8$, and $l = 24$ due to the reasons explained above. The implementation has been structured in the following way: First, we compute random starting key-values in each row, in each table. This means that in total we compute $m \cdot \ell$ starting key-values. Then, we keep adding new columns in all the tables. Every time we have added one new column in all the tables, we calculate the total current coverage across all the tables. In this way, it is possible to track how the coverage develops when the number of columns increases. Figures 2(a) and 2(b) shows the theoretical point coverage and our observed point coverage. Note that on both figures, we have fixed $m = 89$, and we then plot the point coverage as a function of t.



(a) Theoretical point coverage

(b) Practical point coverage

Figure 2: Comparison between the theoretical point coverage and the practical point coverage

The figures 2(a) and 2(b) show that the theoretical and the observed values look very much the same. Figure 3 shows the absolute difference between the theoretical and the observed values, and this figure confirms that the observed values are very close to the theoretical values.

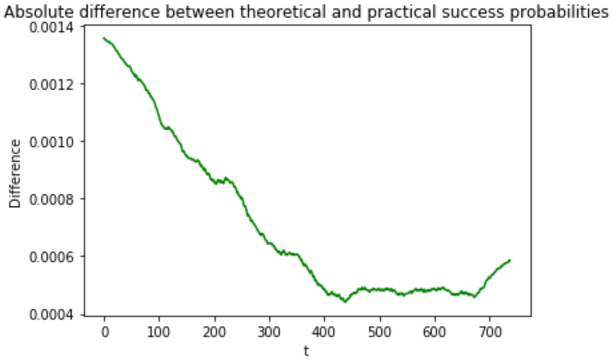


Figure 3: Difference between theoretical and practical values

3 Rainbow tables

In this section we will cover the 3 exercises about rainbow tables. The effective key size is 24 and l=24.

3.1 Exercise 1

The success probability when using rainbow tables with $m \cdot t$ rows and t columns is given by

$$P_{rainbow} = 1 - \left(\frac{2}{2 + \frac{m \cdot t^2}{2^l}} \right)^2 \tag{3.1}$$

Now we let $m = 2^8$ and plot the probability as a function of t. This yields:

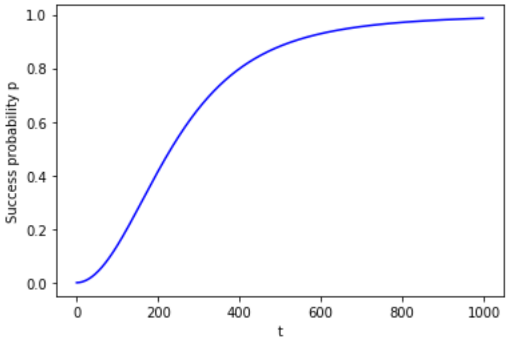


Figure 4: Success probability of using rainbow tables as a function of t

Here we can see as t increases so does the probability of success. Furthermore there is a value of t (around t=600) where the graph flattens out and choosing t higher might not result in a much higher success probability but mostly affect the overall complexity.

3.2 Exercise 2

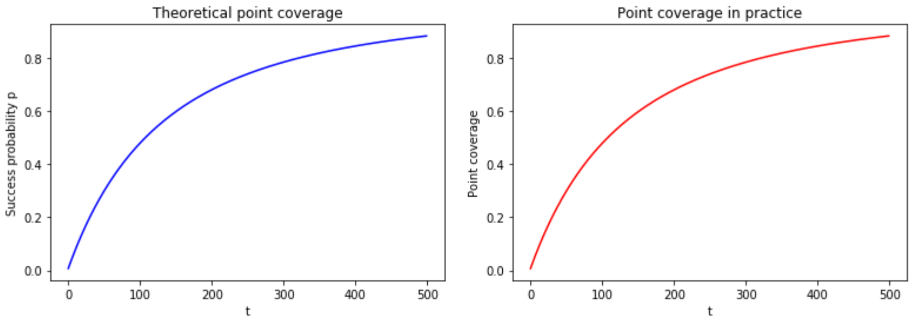
Using multiple rainbow tables have the success probability

$$P_{rainbow} = 1 - \left(\frac{2}{2 + \frac{m \cdot t^2}{2^l}} \right)^{2 \cdot \ell} \tag{3.2}$$

Now how many rainbow tables are optimal is hard to answer in general since it of course depend on t and m. The whole idea, however, is is to only use a single table and make sure to choose m and t appropriately such that when using multiple tables will only increase the overall complexity and not the probability of success. Hence if m and t are chosen appropriately a single rainbow table is to prefer.

3.3 Exercise 3

In this exercise we will compare the point coverage of a rainbow table with $m = 2^8$ and $t = 500$. The way we will do this is calculating the keys column by column and at each step calculate how many points are covered. At the end we expect to end up with 0.88 of all possible points since $P_{rainbow}(500) \approx 0.88$. Doing this yields the following graphs:



(a) Theoretical point coverage

(b) Practical point coverage

Figure 5: Comparison between the theoretical point coverage and the practical point coverage

Notice that these figures look exactly the same which means that the theoretical and practical values are nearly the same. We have also plotted to actual difference between the graphs:

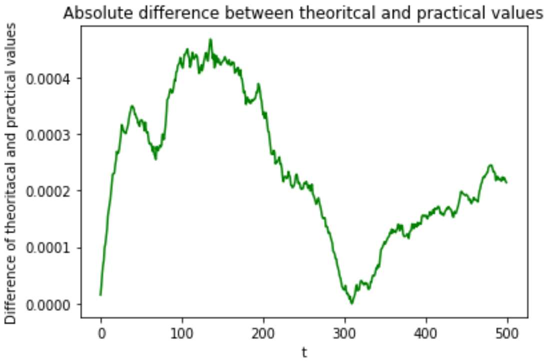


Figure 6: Difference between theoretical and practical values

Here we can see that the difference is very very small and that our experiment is successful. The final coverage in this experiment was 0.8819 which is ecaxtly what we expected.