# Homework

**Information Security II**

Julia Wanker

23 May 2018

## 1 SPA of RSA Using CRT

### 1.1 Learn Secret

We can do a chosen chiphertext attack and observe the corresponding result of $x \bmod p > x \bmod q$.
Initially, we choose $x$ to be equal to 0 (where $x \bmod p > x \bmod q$ will be false) and then repeatedly set the least significant bits to 1, so we repeatedly increase $x$ and check the result of $x \bmod p > x \bmod q$ in order to be able to determine the value of $q$ and further calculate $p$ and $d$ out of $n$ and $q$.

- If $p > q$
  In this case, the RHS of the equation will be around 0 earlier, making the equation result in true. This result is reached exactly when $q = x$. Hence we now know $q$ and can calculate $p$ out of it and further calculate $d$.
- If $p < q$
  In this case, the LHS of the equation will be around 0 earlier, but the equation will still be false at this point. Thus we keep increasing $x$. Then, at some point the RHS of the equation will turn around 0 and sice the LHS was about 0 at an earlier stage, the LHS will then be greater than 0 and hence the equation will be true. This result is again reached when $q = x$ and hence we now know $q$ and can again calculate $p$ and further $d$.

### 1.2 Protection through Padding

Padding verification after a RSA decrption may help to detect active attacks, since the padding process may be invalid when an attacker disrupts the RSA private key, i.e. fault injection.

## 2 No Covert Channel?

### 2.1 Possible Covert Channel

Assuming the attacker is running malware on all computers within the datacenter, then the attacker could monitor the **frequency of failing computers**. The attacker can further interpret the replacement pattern as a string of bits, forming a covert channel.

### 2.2 Capacity of Covert Channel

If we assume the average case of replacing computers every 10 years, the channel has a capacity of

$$\frac{\frac{1}{10}bit}{year} * amountPCs$$

.

## 3 PINs, Pollen, Probability (Part II)

### 3.1 Trials without prior Knowledge

Assuming we have a key of 5 digits where only 4 digits are worn off on the keypad, which tells us that those are the numbers forming the key. Then, within the key there is one of those numbers two times. So we have 240 trials in total:

$$\binom{5 \times 4}{2,1,1,1} = \frac{5! * 4}{2!} = \frac{5 * 4 * 3 * 2 * 4}{2} = \frac{120 * 4}{2} = \frac{480}{2} = 240$$

Which will lead to **120 trials on average**.

### 3.2 Trials when selectively cleaning Keys

When we can selectively clean keys I would suggest to **wipe all keys except one** (where we know that it is contained in the overall key, one of the worn offs), since we know from the discussion of the optional exercise sheet that the number of trials gets less the more keys we clean (down to one leaving dirty).

$$4! * 4 + 3! * 4 + (2! * 2) * 4 + 3! * 4 + 4! * 4 = 96 + 24 + 16 + 24 + 96 = \frac{256}{5} = 51.2$$

which leads to **25.6 trials on average**.

The components for the formula were constructed as follows:

- dirty key is **first number** of the overall key: 4! different permutations
- dirty key is **second number** of the overall key: 3! different permutations
- dirty key is **middle number** of the overall key: 2! different permutations for each side, which gives us 2*2! permutations in total
- dirty key is **second to the last number** of the overall key: 3! different permutations
- dirty key is **last number** of the overall key: 4! different permutations

But since one key is reused, we might learn less information than stated above (n***4** in formula).

### 3.3 Progress of three worn off Keys

Assuming we have now only 3 digits worn off on the keypad, then the overall key might contain exactly two digits for two times each or one digit is included three times. Then the total number of trials only reuces compared to 4 worn off keys, but does not yield an improvement compared to one dusty key:

$$\binom{5 \times 3 \times 3}{2, 2, 1} = \frac{5! * 9}{2! * 2!} = \frac{5 * 4 * 3 * 2 * 9}{2 * 2} = \frac{120 * 9}{4} = \frac{1080}{4} = 270$$

So we have **135 trials on average** for the first case.

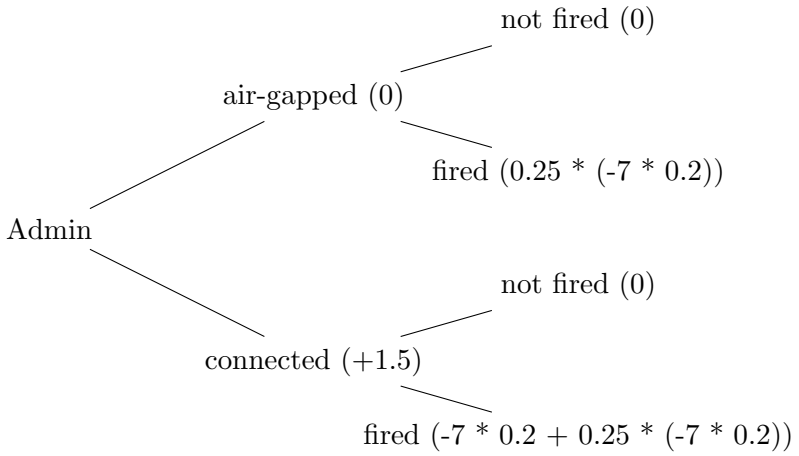
$$\binom{5 \times 3}{3,1,1} = \frac{5! * 3}{3!} = \frac{5 * 4 * 3 * 2 * 3}{3 * 2} = \frac{120 * 3}{6} = \frac{360}{6} = 60$$

So we have **30 trials on average** for the second case.

Thus we have an **average amount of 82.5 trials** in total ($\frac{30+135}{2}$)

# 4 Game Theory

| |
|---|
| N := {1, 2}<br>S1 := {connected (c), disconnected (d)}<br>S2 := {connected (c), disconnected (d)} |




## 4.1 Utility Functions

u1(d, d) = 0
u1(d, c) = 0 + 0.2 * (0.25 * (-7))
u1(c, d) = 1.5 + 0.2 * (-7)
u1(c, c) = 1.5 + 0.2 * (-7) + 0.2 * (0.25 * (-7))

u2(d, d) = 0
u2(d, c) = 0 + 0.2 * (0.25 * (-7))
u2(c, d) = 1.5 + 0.2 * (-7)
u2(c, c) = 1.5 + 0.2 * (-7) + 0.2 * (0.25 * (-7))

### 4.2 Game Matrix

| | Admin2:c | Admin2:d |
|---|---|---|
| Admin1:c | (-0.25, -0.25) | (0.1, -0.35) |
| Admin1:d | (-0.35, 0.1) | (0, 0) |

### 4.3 Nash Equilibrium and Social Optimum

Since every game with a finite number of players and a finite set of actions has at least one Nash equilibrium, we also have to have one here, which is when both are connected to the Internet. (c is the best response to c)

The social optimum is when both administrators have an air-gapped system.

### 4.4 Appropriate Canonical Game

The corresponding canonical game is the *Prisoners' Dilemma*.

### 4.5 Apply for Job?

NO, I would not apply for the job, since I would always have a 25% chance of getting fired although I kept my system air-gapped. Further, in case I do not know my colleague's decision, I would need to connect to the Internet such that he cannot improve by changing his strategy and thus my system would possibly be vulnerable, too.