1) SPA of RSA Using CRT

2) No Covert Channel?

a) Can you still think of a covert channel?

The number/frequency of failing computers, and thus of replacement purchases, could be used to extract information over long times.

E.g. a bit could be transmitted by breaking/buying two/three computers at once for a 0 or 1.

b) What is the capacity of this channel?

$1b/25$ years to not attract attention (due to the average)

3) PINs, Pollen, Probability (Part II)

a) How many trials without prior knowledge?

We know 4 keys, the missing one is 1 out of 6. Therefore, I think the average number of trials is

$$\frac{5! \times 6}{2} = \frac{6!}{2} = 360$$

tries on average.

b) What can be achieved using pollen?

I think I would still wipe all keys except one [TODO calculate other options].

This leaves us with some cases:

- First key is pollenated. This also reveals the unknown key! Still need all others in order, so $4!$ combinations $\frac{1}{5}$ of the time.
- Second or Fourth key is pollenated. We know that all pollenated keys are after, and all clean ones before the one we didn't wipe.
  - If a not worn out key is pollenated, we learned the unknown key. $3!$ combinations $\frac{2}{5 \times 2}$ of the time

    - If all worn out keys are pollenated, we still need the unkown key. $3! \times 6$ combinations $\frac{2}{5\times2}$ of the time.
- Middle key is pollenated.
    - If the unkown key is in the second half, and thus revealed: $2! \times 2!$ combinations left $\frac{1}{5\times2}$ of the time
    - If the unkown key is not revealed: $2! \times 2! \times 6$ combinations left $\frac{1}{5\times2}$ of the time
- Last key is pollenated. Like first case except we didn't learn the unknown key. $4! \times 6$ combinations $\frac{1}{5}$ of the time.

The expected number of combinations is therefore $\frac{1}{5} \times 4! + \frac{2}{10} \times 3! + \frac{2}{10} \times 3! \times 6 + \frac{1}{10} \times 4 + \frac{1}{10} \times 24 + \frac{1}{5} \times 4! \times 6 = 2176$, which we can expect to crack in 1088 attempts.

TODO: this number is so large - one of my calculations is wrong!

c) What to do if only 3 keys are worn off?

In this case it would be better to polinate all warn off keys to maximize the odds of revealing the unknown keys, because trying to find those out of 6×5 combinations is much harder than just 6.

4) Game Theory