# Q & A session I

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

# 2WF80

- Main places for information
  - Course page.
  - Zulip chat room.
  - Canvas – mostly only for live Q & A sessions;
    Do you want quizzes?
    Update from the lecture: enough people want quizzes to that I will make some. I'll keep the quizzes open for longer.
- We will use `https://www.wonder.me` for the exercise sessions on Thursdays. I will post the link to our room on Zulip.

  The tool is good for interactions so that you can work in small groups and also good for asking for help / us strolling around.

  You still need some shared space for writing, e.g. etherpad, cryptopad.
- Us = me + Stan Korzilius, Jonathan Levin, Mohammad Mahzoun, and Alex Pellegrini as teaching assistants.

# Homeworks

- There will be 4 sheets of homeworks, accounting for 30% of the final grade. No sheet this week, first sheet on Nov 19, due one week later. Sheets are posted *after* exercise session, due *before* the next exercise session.
- Please submit in groups of 2 – 3.
- Submission is by *encrypted* email to the TAs,
  so that you learn how to use crypto in real live.
  Include your own public key and those of your team mates when you submit. We can only reply to you if we get your keys.
- Everybody should submit at least once (with team members in cc).
- Some homeworks require submission of implementations, you're free to choose a programming language.
  - Use Python / Sage if you don't have a preference.
  - Code in Sage or Pari-GP is fine; we can handle Mathematica if necessary.
  - The code should compile and run!! The TAs will not debug for you.
  - The code should be humanly readable and have comments.
    This is not a challenge in code obfuscation.
  - The code should be submitted as code, not as a pdf or such.

# Questions on substitution ciphers

Somebody was asking about how to decrypt the substitution cipher. Further hints are to look for short words that probably are THE or THAT or THIS or THEN, which gives you some information.
Another hint is that the text is about the course subject.

Somebody pointed out that the Caesar cipher is also a substitution cipher. That's correct, but it's a family with a very restricted key space in that they keep the letters in fixed order.

# Questions on Viginère

Somebody was asking about triple encrypting with Viginère.
My first understanding of the question was that it would be doing

```
  THISISABETTERWAYTOENCRYPTTHANCAESAR
+ CRYPTOCRYPTOCRYPTOCRYPTOCRYPTOCRYPT
----------------------------------
  VYGHBGCSCIMSTNYNMCGEAGRDVKFPGQCVQPK
+ CRYPTOCRYPTOCRYPTOCRYPTOCRYPTOCRYPT
----------------------------------
  X.................................
+ CRYPTOCRYPTOCRYPTOCRYPTOCRYPTOCRYPT
----------------------------------
  Z.................................
```

Which would just be a cumbersome way to encrypt with each shifting distance multiplied by 3, i.e. with GZUTFQ
The person then clarified that they meant using different keywords of different lengths, and that seems a lot more secure. This should give frequency patterns similar to a keyword of length the lcm of the keyword lengths, but also at a lot more work.