Teaching Public-Key Cryptography in School

Lucia Keller, Dennis Komm, Giovanni Serafini,
Andreas Sprock, and Björn Steffen

ETH Zürich

ISSEP 2010, 14. January 2010

Motivation

Cryptography in school

- Cryptography is an important part of computer science
- It raises interest of students of all ages
- It allows the teacher to create interesting lessons with experiments and games
- It is used in everyday-life

Aim: Easy way to communicate ideas of public-key cryptography to students (age 15 to 18).

Motivation

Problems

- Protocols employ involved mathematics
- Many details are unimportant for main ideas

Challenge of didactics: Explain the concepts behind public-key cryptography as accessible as possible.

Motivation

Problems

- Protocols employ involved mathematics
- Many details are unimportant for main ideas

Challenge of didactics: Explain the concepts behind public-key cryptography as accessible as possible.

Our approach

- use simple graph-based public-key cryptosystem
- requires only minimal mathematical background
- introduced in 2003 by Tim Bell et al. in *Computers and Education, volume 40, number 3*

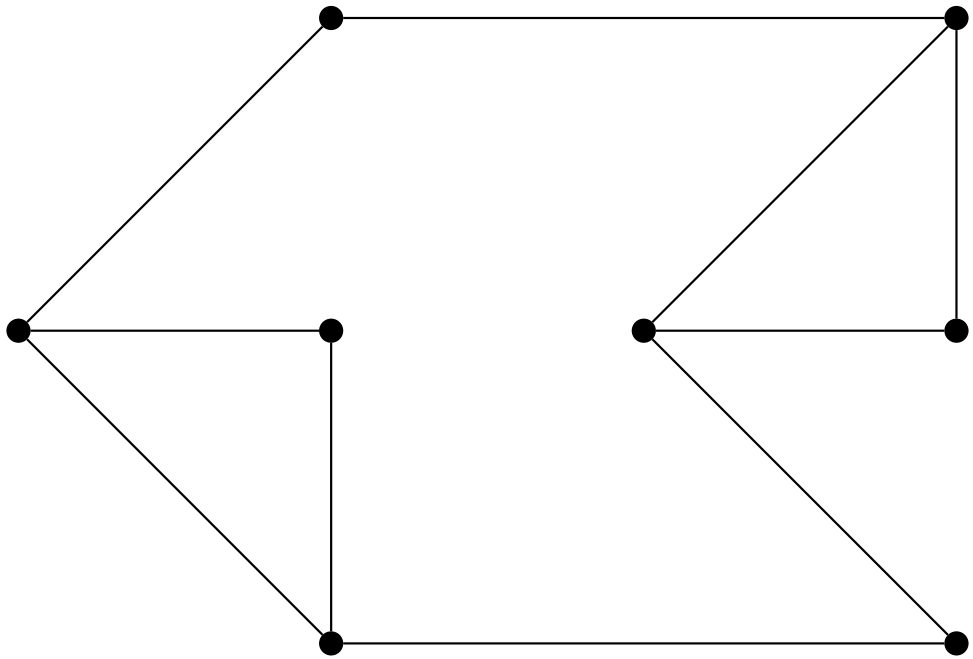
Public-Key Cryptography

The idea of public-key cryptography

- Several persons want to securely communicate with each other
- Each person A owns a key pair $(private, public)$
- *public* is publicly known and is used to encrypt messages
- *private* is used to decrypt messages
- Only A has access to *private*

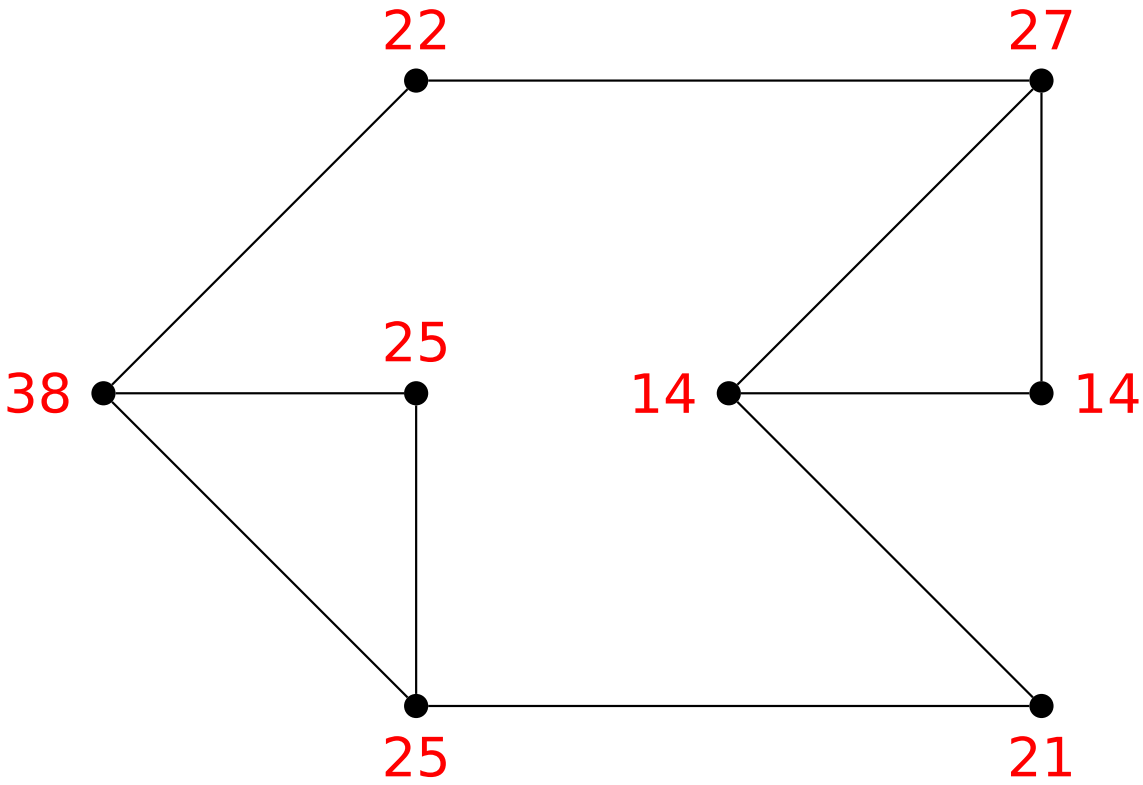
Contest

The graph for the students to encrypt a number.



Contest 2

A cipher text from the teacher.



Conclusion

Upcoming textbook

Karin Freiermuth, Juraj Hromkovič, Lucia Keller, and Björn Steffen: *Einführung in die Kryptologie*. Vieweg+Teubner 2010.