Cryptology and Security

- An example problem: Homebanking Security

Ivan Damgård, Århus Universitet

www.daimi.au.dk -> Research -> Cryptology and Security
- or:

Why are large sums of money stolen from netbanking account?

- og which solutions can our research suggest?
The problem, technically..

- **Private key**: Gives access to payment order, with digital signature.
- **Password**: Access to private key.
- **Hacking, phising, etc.**

www.daimi.au.dk -> Research -> Cryptology and Security
Why does it go wrong?

Bad security on standard PC’er, both the system and users can be cheated
- hard to solve on short term

Enough to break in, in one place
- this can be solved! - stay tuned

Wasn’t is always a problem?
Yes, but these days, people hack for money and not for fun..
Splitting a key..

Normal digital signature:

+ "500 kr. to Kurt"

Digital signature with shared key:

+ "500 kr. to Kurt"
+ "500 kr. to Kurt"

www.daimi.au.dk -> Research -> Cryptology and Security
A more secure scenario...

The point: only problems if break-in in two places simultaneously..
- Distributed security

www.daimi.au.dk -> Research -> Cryptology and Security
A Research Project

ITSCI (IT Security for Citizens) (the NABIIT program)
Partners: Århus Universitet, PBS, TDC, Giritech, Cryptomathic, Danske bank
Goal: more secure and usable solutions for the IT security of citizens
Collaboration between Security and Human-Computer Interaction groups at Daimi. Important for security in practice.

www.daimi.au.dk -> Research -> Cryptology and Security