

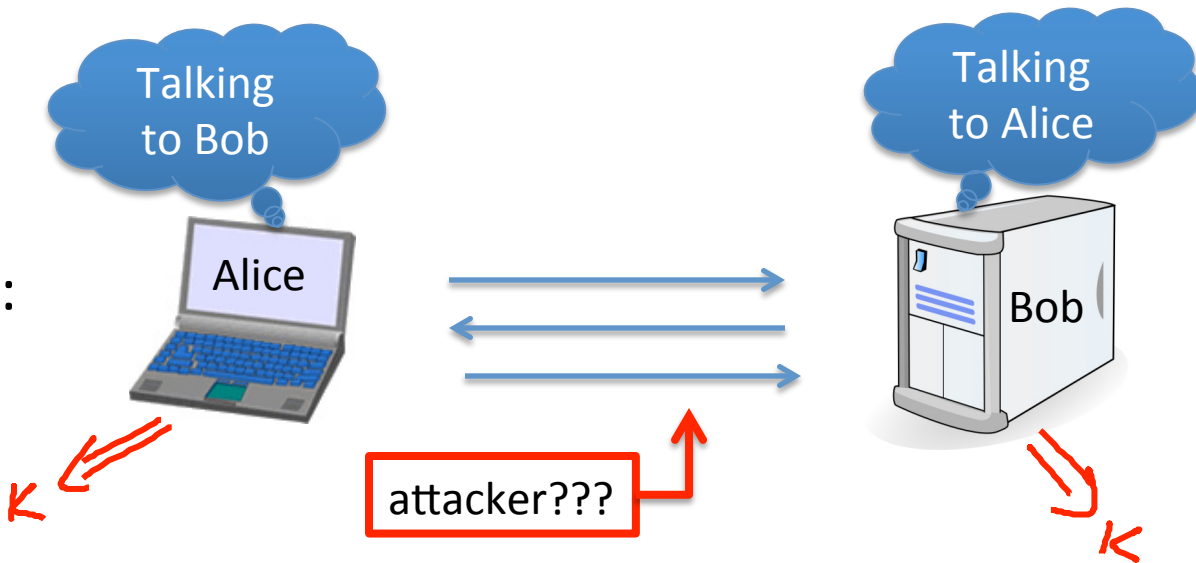


Introduction

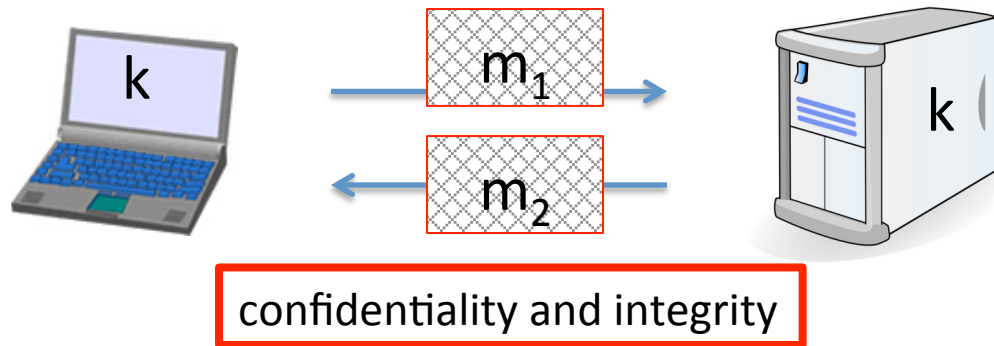
What is cryptography?

Crypto core

Secret key establishment:

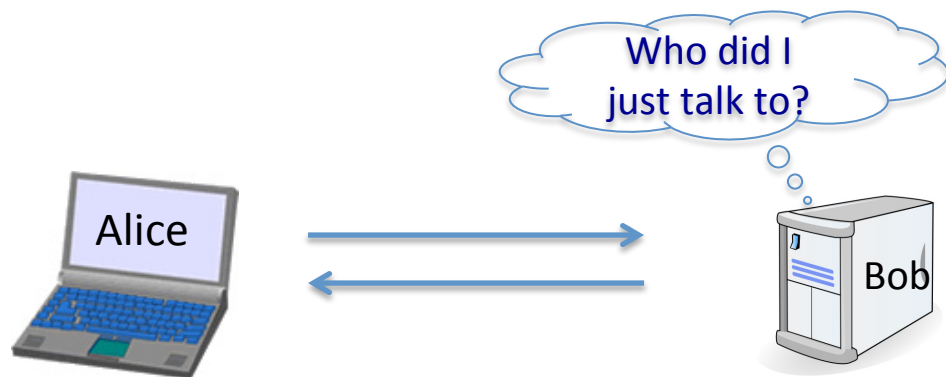


Secure communication:



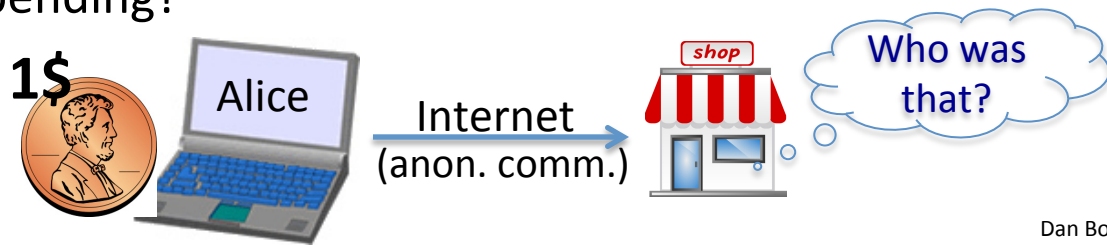
But crypto can do much more

- Digital signatures
- Anonymous communication



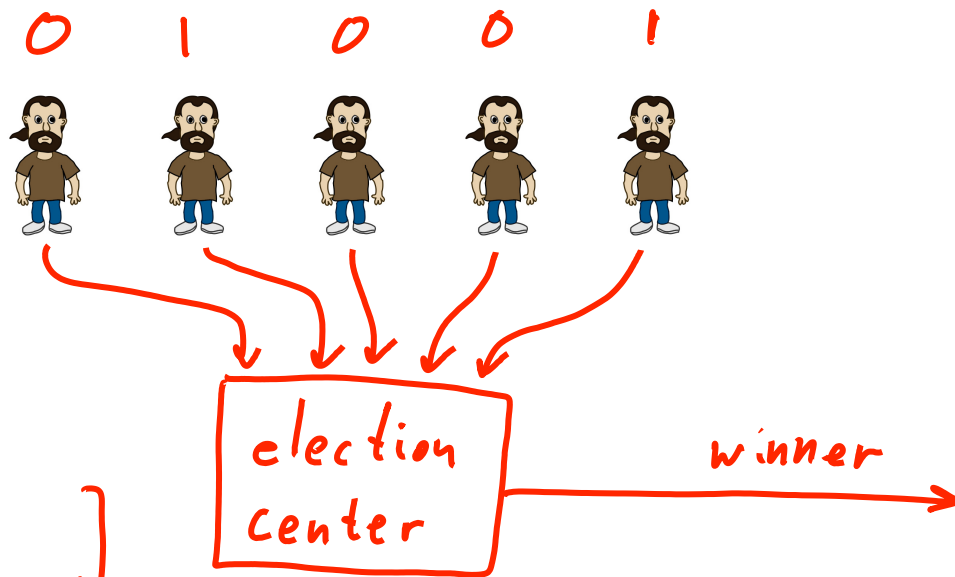
But crypto can do much more

- Digital signatures
- Anonymous communication
- Anonymous **digital** cash
 - Can I spend a “digital coin” without anyone knowing who I am?
 - How to prevent double spending?



Protocols

- Elections
- Private auctions

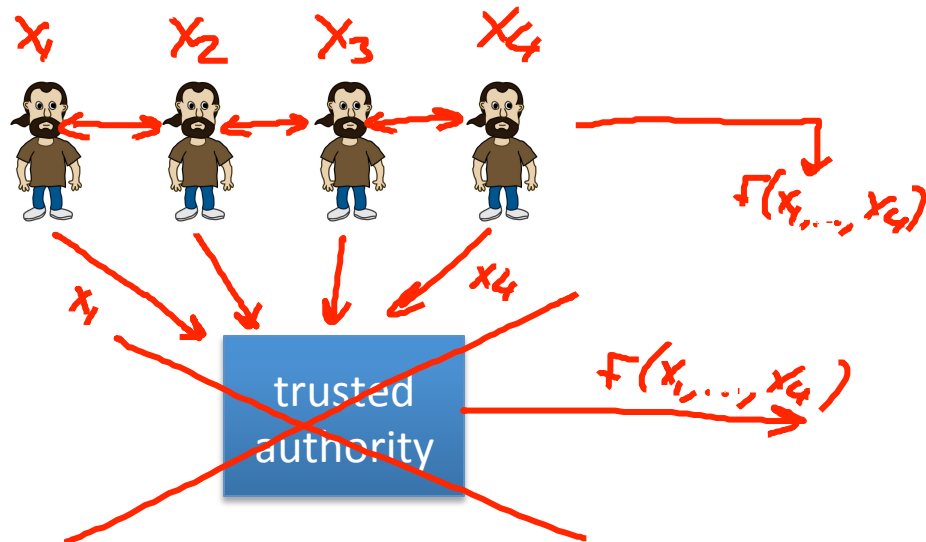


winner = MAJ [votes]

auction winner = [highest bidder, pays 2nd highest bid]

Protocols

- Elections
- Private auctions



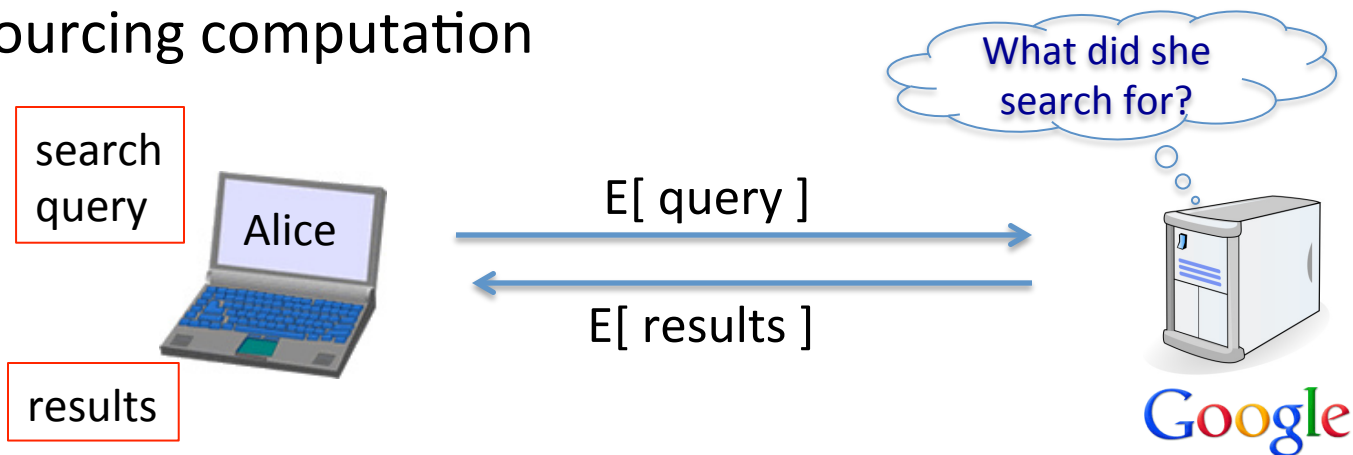
Goal: compute $f(x_1, x_2, x_3, x_4)$

“Thm:” anything that can be done with trusted auth. can also be done without

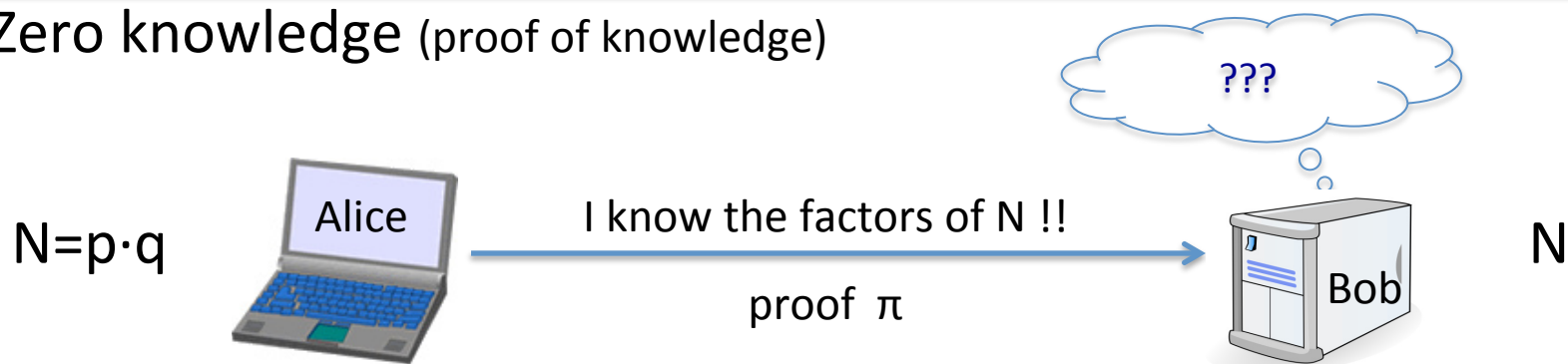
- Secure multi-party computation

Crypto magic

- Privately outsourcing computation




- Zero knowledge (proof of knowledge)



A rigorous science

The three steps in cryptography:

- 
- Precisely specify threat model
 - Propose a construction
 - Prove that breaking construction under threat mode will solve an underlying hard problem

End of Segment