CS5800 – ALGORITHMS

MODULE 2. COMPLEXITY (AND COMPUTABILITY & CRYPTOGRAPHY)

Lesson 5: Diffie-Hellman Key Exchange

Ravi Sundaram

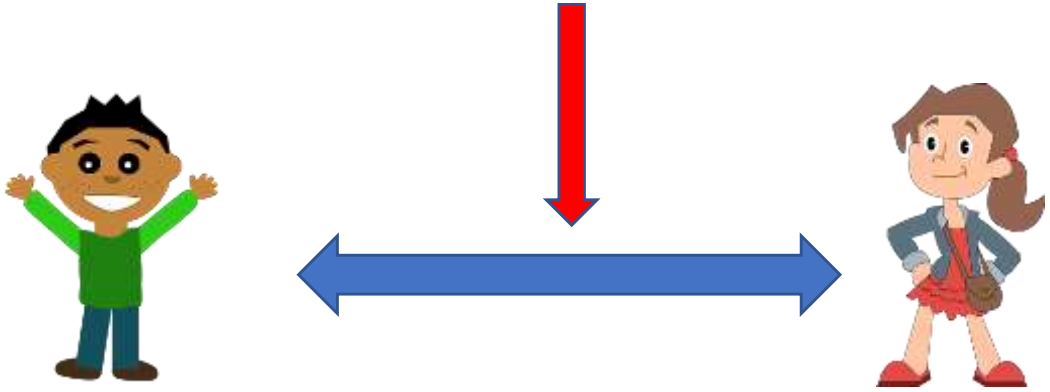
Topics

- Fundamental problem of secure Internet
- Engagement Ring Puzzle
- Diffie-Hellman key exchange protocol
- Summary

Fundamental Problem of Secure Internet

- Alice and Bob wish to communicate

in the presence of Eve (eavesdropper)

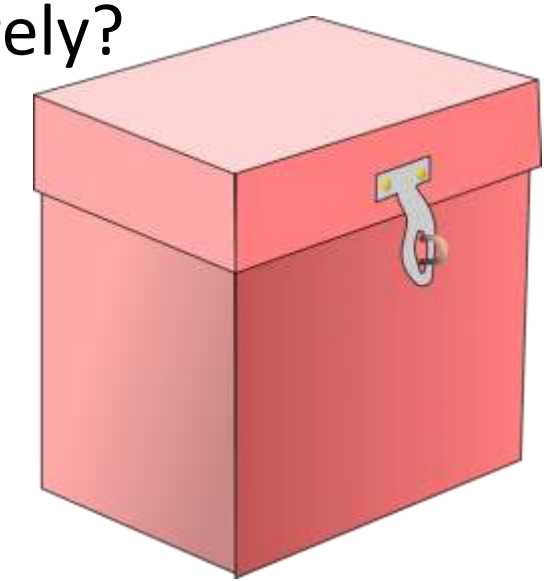


- How can they do it?

- Historically, they would first meet in private and arrange a codebook

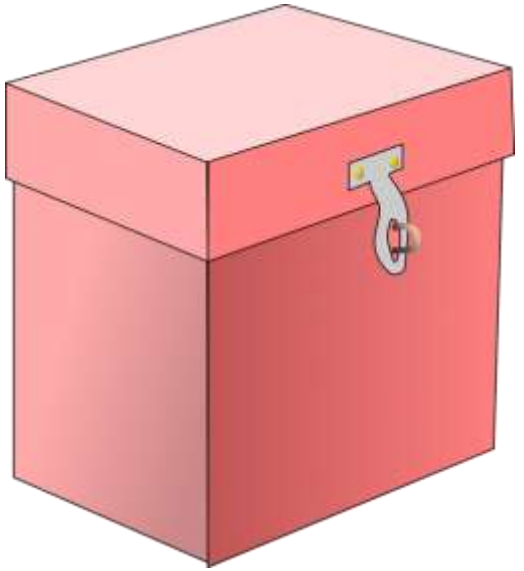
Engagement Ring Puzzle

- Alice and Bob meet over the Internet and fall in love
- Bob wants to mail Alice a ring, but anything sent in an unlocked box risks getting stolen.
- How can Bob send the ring securely?



Engagement Ring Puzzle - Solution

- Bob puts the ring in a box, locks it and sends the locked box to Alice
- Alice adds her own lock and sends it back
- Bob removes his lock and sends it back
- Alice removes her lock and puts on the ring

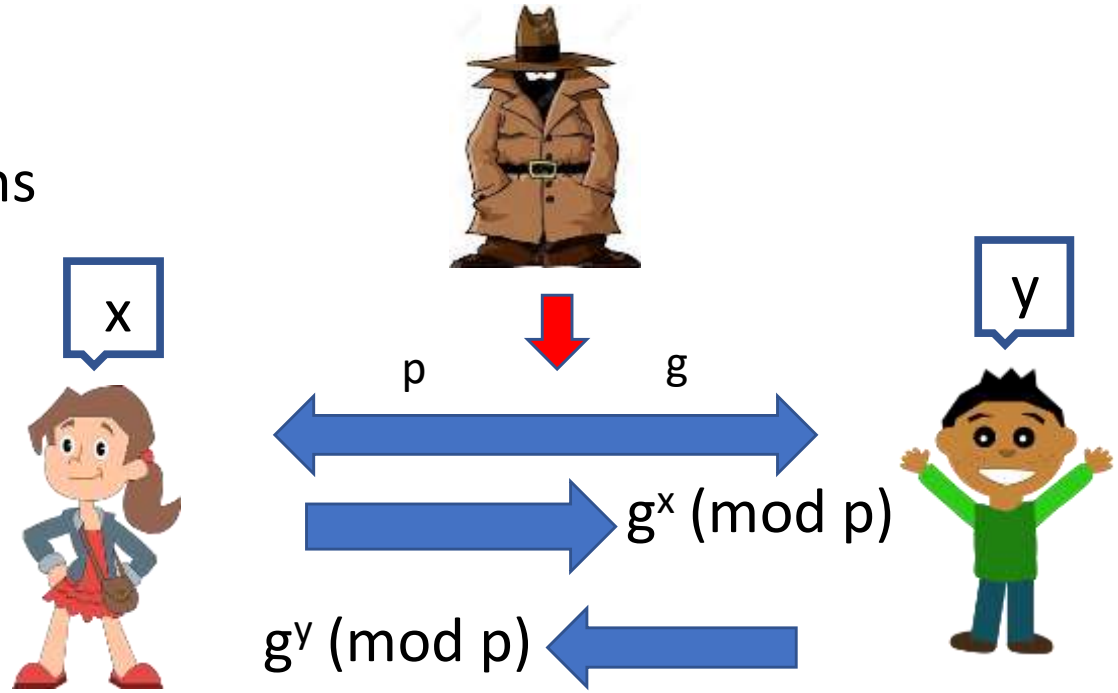


Background

- Martin Hellman (Stanford prof) and Whitfield Diffie (PhD Student) made a revolutionary breakthrough, 1976
- Key to the usefulness of the Internet – your browser can communicate securely over public channels with your bank's web server
- Crux of the idea: Modular exponentiation is easy but discrete log is hard i.e., modular exponentiation is one-way
- Later, declassified records show it was invented at GCHQ by Cocks, Ellis and Willamson in 1970.

Diffie-Hellman Key Exchange Protocol

- Alice and Bob agree on prime p and generator g in public (generator means g mod p, g^2 mod p, g^3 mod p etc., are all different)



- Alice thinks of a random x and sends g^x (mod p) to Bob,
- Bob thinks of a random y and responds with g^y (mod p)
- Note that Alice and Bob can each compute $g^{xy} = (g^x)^y = (g^y)^x$ (mod p) but Eve can't. Voila!

Summary

- Well-defined problems can be divided into two categories
  - Those that can be solved quickly, and
  - Those that can’t
- Cryptography uses this dichotomy to achieve remarkable results
  - Alice and Bob can communicate securely over a public channel
- Thus cryptography can be seen as an application of algorithmic ideas (fast modular exponentiation enables Diffie-Hellman key exchange)
- Main takeaway: algorithmic techniques (over a range of domains including numbers, graphs, strings, etc.,) are the engine of the modern world