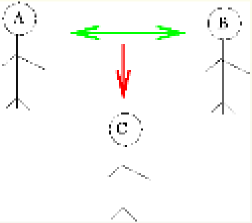
Exchanging Secrets



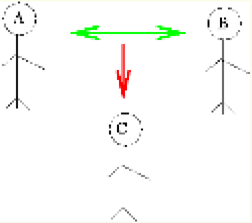
Goal

A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key.*

Exchanging Secrets



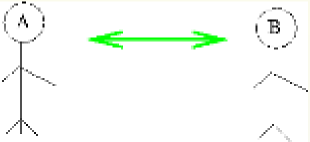
Goal

A and B to agree on a secret number. But, C can listen to all their conversation.

Solution?

A tells B: *I'll send you 3 numbers. Let's use their LCM as the key.*

Mutual Authentication



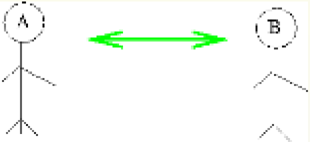
Goal

A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Mutual Authentication



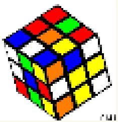
Goal

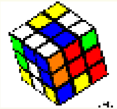
A and B to verify that both know the same secret number. No *third party* (intruder or umpire!)

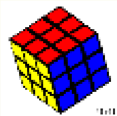
Solution?

A tells B: *I'll tell you first 2 digits, you tell me the last two...*

Zero-Knowledge Proofs







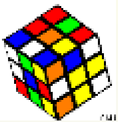
Goal

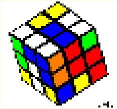
A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

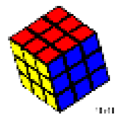
Solution?

A tells B: *Close your eyes, let me solve it…*

Zero-Knowledge Proofs







Goal

A to prove to B that she knows how to solve the cube. Without *actually revealing* the solution!

Solution?

A tells B: *Close your eyes, let me solve it…*

Paper, Scissors, Rock Game

Goal

How to play over Internet? Using **email,** say?

Solution?

You mail me your choice. I'll reply with mine.

Paper, Scissors, Rock Game

Goal

How to play over Internet? Using **email,** say?

Solution?

You mail me your choice. I'll reply with mine.

Sharing a Dosa

Goal

All should get equal share of dosa. No *envy* factor. No *trusted umpire*.

Solution?

2 people case is easy- *you cut, i choose!*

Sharing a Dosa

Goal

All should get equal share of dosa. No *envy* factor. No *trusted umpire*.

Solution?

2 people case is easy- *you cut, i choose!*

Security Concerns

Match the following!

Problems	Attackers
Highly contagious viruses	Unintended blunders
Defacing web pages	Disgruntled employees or customers
Credit card number theft	Organized crime
On-line scams	Foreign espionage agents
Intellectual property theft	Hackers driven by technical challenge
Wiping out data	Petty criminals
Denial of service	Organized terror groups
Spam E-mails	Information warfare
Reading private files	...
Surveillance	...

- Crackers vs. Hackers
- Note how much resources available to attackers.

References

- Books
  - *TCP/IP Illustrated* by Richard Stevens, Vols 1-3, Addison-Wesley.
  - *Applied Cryptography - Protocols, Algorithms, and Source Code in C* by Bruce Schneier, Jon Wiley & Sons, Inc. 1996
  - *Cryptography and Network Security: Principles and Practice* by William Stallings (2nd Edition), Prentice Hall Press; 1998.
  - *Practical Unix and Internet Security,* Simson Garfinkel and Gene Spafford, O'Reilly and Associates, ISBN 1-56592-148-8.
- Web sites
  - *www.cerias.purdue.edu* (Centre for Education and Research in Information Assurance and Security)
  - *www.sans.org* (System Administration, Audit, Network Security)
  - *cve.mitre.org* (Common Vulnerabilities and Exposures)
  - *csrc.nist.gov* (Computer Security Resources Clearinghouse)