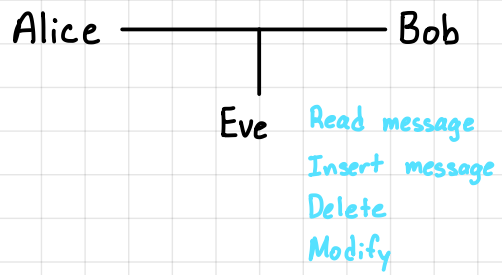
Cryptography – "Communication in the presence of adversaries". - Rivest



Fundamental Services:

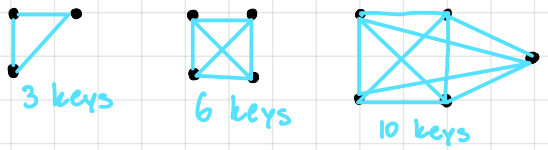
Encryption: Secrecy. No one can extract any info from message.

Authentication: Integrity. Receiver can verify message unchanged.

Types of Cryptography:

Symmetric: sender/receiver know the same secret key.

- Faster, doesn't scale well

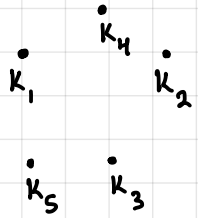


$1 + 2 + 3 + 4 + \ldots + n$

$= \frac{n(n+1)}{2} = O(n^2)$

Asymmetric: sender/receiver know different secret keys.

- slower, scales well



n parties = O(n) keys

Hybrid: Start w/ asymmetric, then switch to symmetric

Building Blocks:

- Public Fixed Invertible Random Function
- Block cyphers
- Stream cyphers
- Cryptographic hash
- Universal hash

} Symmetric

- RSA
- Mathematical "groups"

} asymmetric

Other Topics

- C for low-level programming
- OpenSSL library
- Topics in secure programming

Course Organization

Rhythm:

- 1/2 Material prerecorded
- 1 or 2 live lectures each week @ 12 pm
- 2 quizzes per module (5 modules)
  - 1 mid-module 20% of grade } drops the lowest
  - 1 end-of-module 30% of grade } of each
  - No midterms
  - Final Exam 12/16 5:15 pm Non Standard 30%

Open 9am-10pm
45 min

  * Canvas Quizzes or Mimir (Coding Website)
- Homework
  - Ungraded: don't turn in. prep for quizzes 0%
  - Graded: prep for quiz + programming 20%

Tools:

- Canvas (quizzes, grades, links)
- Piazza (communication, announcments)
- Mimir (programming)