Cryptography

Introduction to Cryptography

Professor Travis Peters
CSCI 476 - Computer Security
Spring 2020

Some slides and figures adapted from Wenliang (Kevin) Du's
Computer & Internet Security: A Hands-on Approach (2nd Edition).
Thank you Kevin and all of the others that have contributed to the SEED resources!

Introduction & Overview

- **Information Security**
  - *The protection of information and information systems (a.k.a. cybersecurity)*
  - *What security technologies to use? Procedures? Controls?*

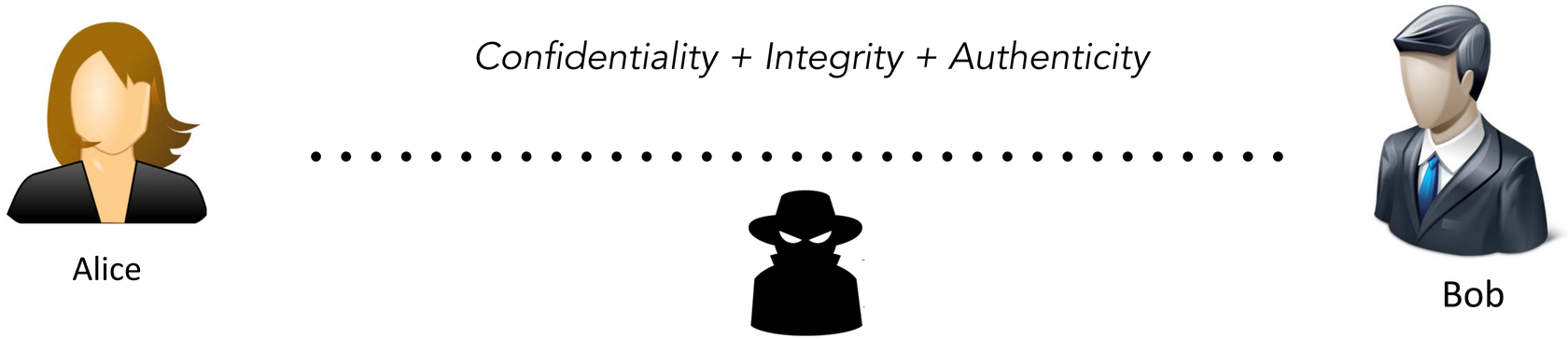
- **Cryptography**
  - Provides the *mathematical techniques* that underpins most information security tech

We study this topic for completeness.
Security education should IMHO include education on crucial topics, including cryptography.
HOWEVER… Beyond these exercises…

Never Roll Your Own Crypto!

What is Cryptography?

Cryptography is the *practice* and *study* of techniques for secure communication in the presence of third parties called adversaries.



"Can only Bob see my message?"

"Is this message really from Alice?"

"How can I make sure my message will reach Bob without being changed?"

"Is this the message Alice intended to send?"

"Is it possible that Alice can deny ever sending me this message in the future?"

CSCI 476 Cryptography Roadmap

- Secret-Key Encryption *(a.k.a., Symmetric Key Encryption)*
- Cryptographic Hash Functions *(e.g., MD5, SHA-*)*
- Public-Key Encryption *(a.k.a., Asymmetric Key Encryption)*

Please review the schedule and start the readings (Chapters 21-23)