

# Basic Cryptography

- CEG 6430/4430 Cyber Network Security
- Junjie Zhang
- [junjie.zhang@wright.edu](mailto:junjie.zhang@wright.edu)
- Wright State University

# Cryptography Offers Mechanisms

- Confidentiality
- Integrity
- Authenticity

# Roadmap

- Hash Function
- Confidentiality
  - Symmetric & Modes of Operation, Asymmetric Encryption
- Key Exchange
  - DH
- Integrity
  - Symmetric (HMAC) and Asymmetric (RSA)
- Authenticity
  - PKI