Announcements

- Midterm Oct.3rd (Tuesday)
  - 9:30-11:30 am
  - Late submission: 50% penalty
  - Download and submit at Canvas, like the assignments
  - Answering questions:
    - Bullets of key points are much clearer
    - Try to stick with the key points. You don’t need more than a couple of sentences if you really know the answers

Security Principles

- What are the security principles?
- Identify security examples being used
- Give real life examples of security principles

Cryptography Roadmap

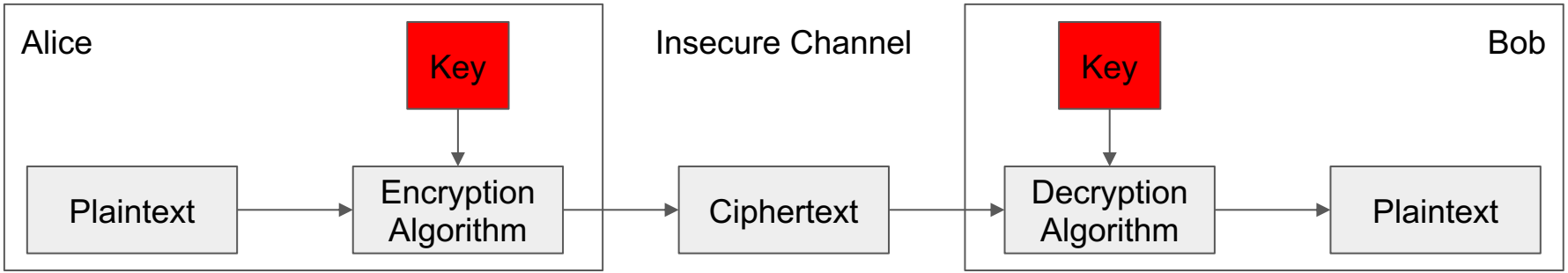
ITIS 6200 / 8200

	Symmetric-key	Asymmetric-key
Confidentiality	• One-time pads • Block ciphers with chaining modes (e.g. AES-CBC) • Stream ciphers	• RSA encryption
Integrity, Authentication	• MACs (e.g. HMAC)	• Digital signatures (e.g. RSA signatures)

- Hash functions
- Pseudorandom number generators
- Public key exchange (e.g. Diffie-Hellman)
- Key management (certificates)
- Password management

Symmetric-Key Encryption: Definition

- A symmetric-key encryption scheme has three algorithms:
  - KeyGen() → *K*: Generate a key *K*
  - Enc(*K*, *M*) → *C*: Encrypt a **plaintext** *M* using the key *K* to produce **ciphertext** *C*
  - Dec(*K*, *C*) → *M*: Decrypt a ciphertext *C* using the key *K*



One-Time Pad

- How does it work?
  - How does encryption work? Formula?
  - How does decryption work? Formula?

- Why is it called One-Time Pad?

- Security
  - What is IND-CPA secure? What is the IND-CPA game?
  - Does One-Time Pad have IND-CPA?
  - What if we reuse the same key for different messages? Do we still have IND-CPA?

Block Cipher

ITIS 6200 / 8200

- How does block ciphers work?
  - Why it is called block ciphers?
  - Why do we need operating modes?
  - Where do we use the key?
- Analyzing Modes
  - Giving a new operating mode, analyzing the formulas used for encryption and description
  - Analyze the performance implication
  - Analyze if the mode is IND-CPA secure: why some modes are secure and others are not
- Security
  - What are IV and nonce?
  - Where do we use them?
  - Why do we need them?
  - Does block cipher provide integrity?

Hash

ITIS 6200 / 8200

- What are the basic properties of hash functions?
  - What is one way function?
  - What is collision resistant?
- What can length extension attacks do?
- Security
  - Do hash provide integrity?
  - How can we use hash for integrity?

MAC

- Why do we want MAC?
  - Why is it different from hash?
- How does HMAC work?
  - What are the inputs?
- Security
  - Do MACs provide integrity?
  - Do MACs provide confidentiality?
  - How do we get both confidentiality and integrity?
    - What is Encrypt-then-MAC?
    - What is MAC-then-encrypt?

PRNG

- Where do we need random numbers?

- PRNG
  - Why is it called Pseudorandom?
  - What is rollback resistance?
  - What can the attacker do if the PRNG is not rollback resistant?

Diffie-Hellman Key Exchange

- Why do we want it?
- How does it work?
  - What variables are public? What variables are private?
  - What is the information being sent between Alice and Bob? Formula?
  - What is the secret being shared? Formula?
- Security
  - What’s the security issue with it?

Public-Key Encryption

- Why do we want Asymmetric-key encryption?
  - What are the major benefits?
  - What is the major issue?

- How does RSA encryption work?
  - What variables are the public key?
  - What variables are the private key?
  - How do we do encryption? Formula?
  - How do we do decryption? Formula?

- Security
  - Can it defend against MITM attack?

Digital Signature

- Why do we need signature?
  - What key is used for digital signature?
  - Why do we sign the hash instead of the plaintext?
- How does RSA signature work?
  - How do we sign a message? Formula?
  - How do we verify a signature? Formula?
- Security
  - How can we combine public-key encryption and digital signature?
  - Can we provide confidentiality and integrity together?

Certificate

ITIS 6200 / 8200

- Why do we need certificate?
- What does a certificate contain?
- What are Certificate Authorities?
  - Why do we need them?