

Security Principles

ITIS 3200

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

Cryptography Roadmap

ITIS 3200

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

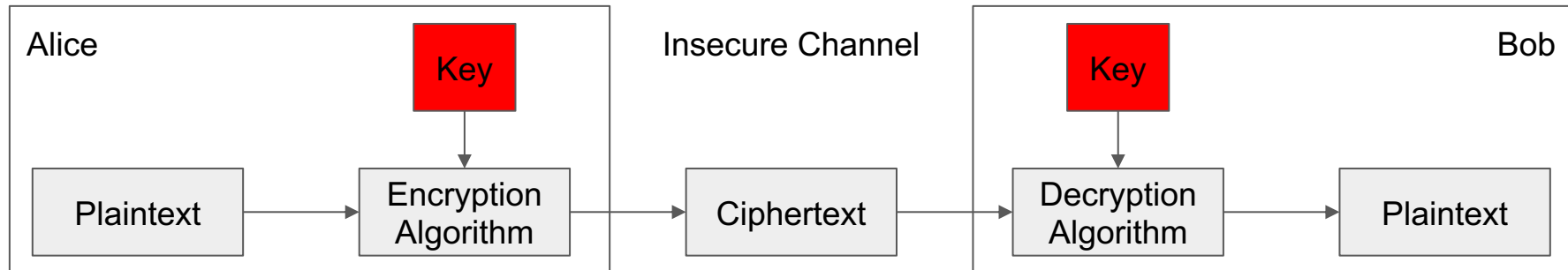
- Hash functions
- Pseudorandom number generators
- Public key exchange (e.g. Diffie-Hellman)

- Key management (certificates)
- Password management

Symmetric-Key Encryption: Definition

ITIS 3200

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



One-Time Pad

ITIS 3200

- 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 3200

- 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 3200

- 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

ITIS 3200

- 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?

Classify: Confidentiality & Integrity

ITIS 3200

- For a given scheme: confidentiality, integrity, both, or neither?
 - A MAC over the plaintext gives integrity but can leak information about M
 - An unkeyed hash $H(M)$ gives no integrity (attacker recomputes it)
 - ECB leaks repeated blocks, so no confidentiality
 - Encrypt-then-MAC over the ciphertext gives both
- Practice: (AES-CTR(M), MAC(C)); AES-CBC(M || MAC(M)); (AES-ECB(M), Hash(M))

PRNG

ITIS 3200

- 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

ITIS 3200

- 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

ITIS 3200

- 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

ITIS 3200

- 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 3200

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

Password Management

ITIS 3200

- Why do we use hash for password management?
- How do we use hash for password management?
- How do we use salted hash? Why are they better for password management?