Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-01-06

Overview of Cryptography and Its Applications

CHAPTER 1

What is this class about?

- **Cryptology**: the study of communication over insecure channels an related fields
  - **Cryptography**: Design of systems for communication over insecure channels
  - **Cryptanalysis**: Breaking cryptographic systems

What is this class about?

- **Coding Theory:**
  representing input information symbols by output symbols called *code symbols*
  - compression
  - secrecy
  - error correction
    - communication over noisy channels
    - many cryptographic systems are destroyed by a single bit error

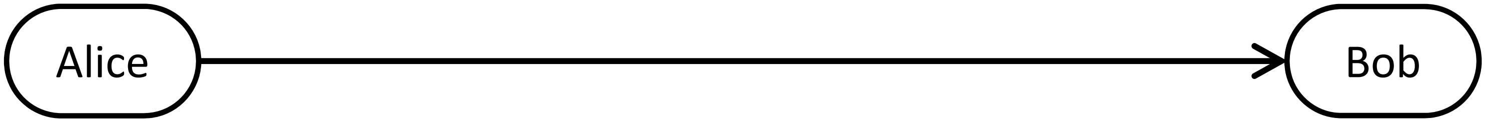
Math is Coming!

- Cryptology relies on:
  - – Number Theory
    - Properties of Primes
  - – Modern Algebra
    - Properties of Groups, Rings, and Fields
  - – Probability Theory
    - Random Number Generation, Quantifying Error, etc.

Section 1.1

SECURE COMMUNICATIONS

Secure Communications



Alice

Bob

Lunch at 1pm?

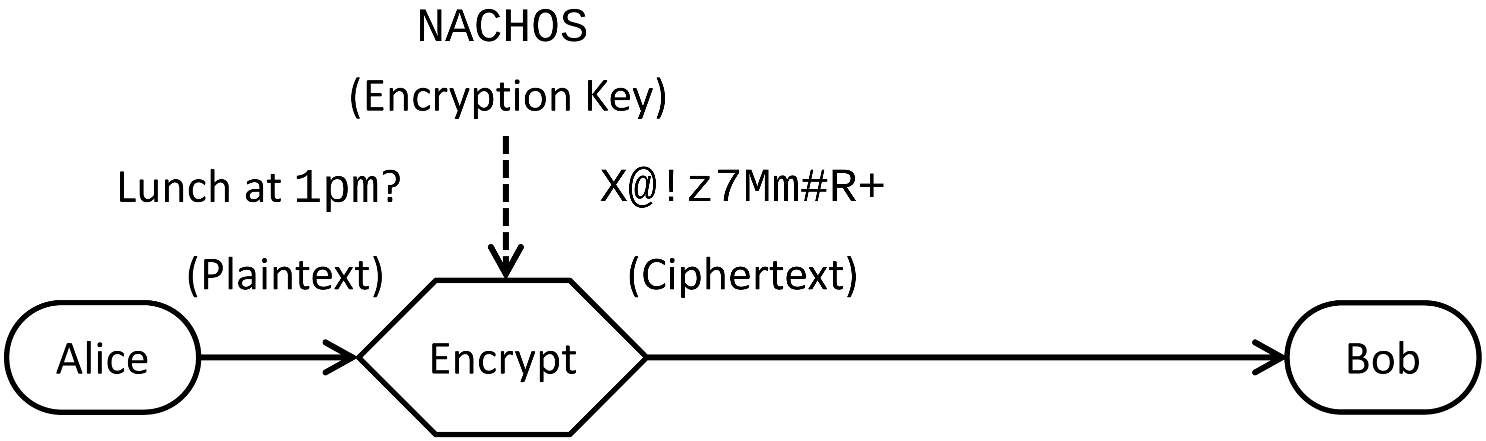
(Plaintext)

Lunch at 1pm?

(Plaintext)

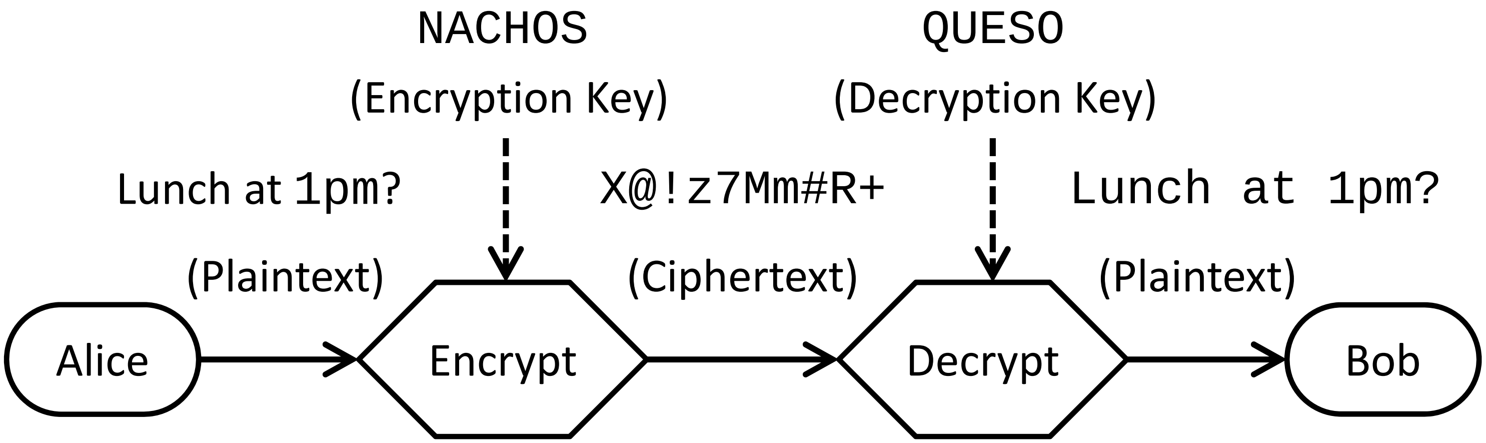
- Alice sends Bob a message
  - Unencrypted text is called the **plaintext**

Cryptography



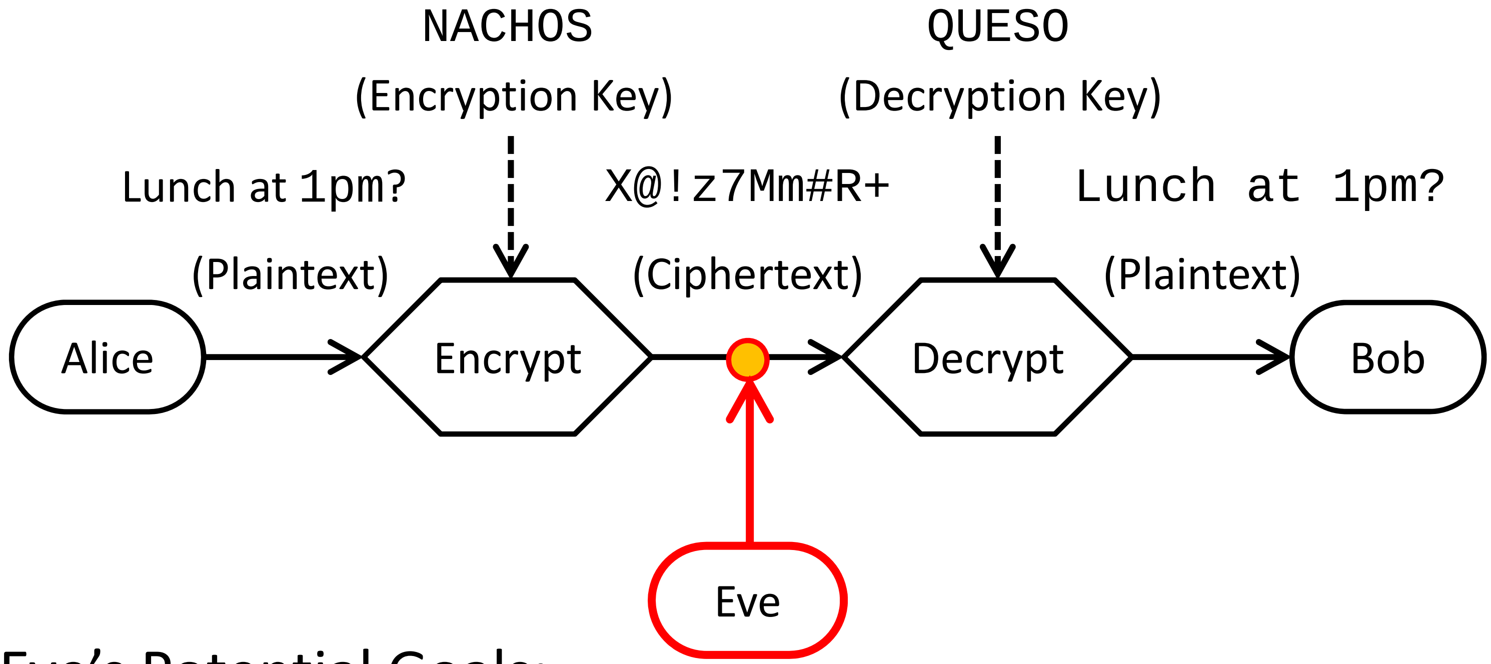
- Alice encrypts the plaintext message with some **encryption method** using an **encryption key** to produce an encrypted message called the **ciphertext**

Cryptography



- Bob decrypts the plaintext message with a corresponding **decryption method** using an **decryption key** to reproduce the original plaintext message

Cryptanalysis



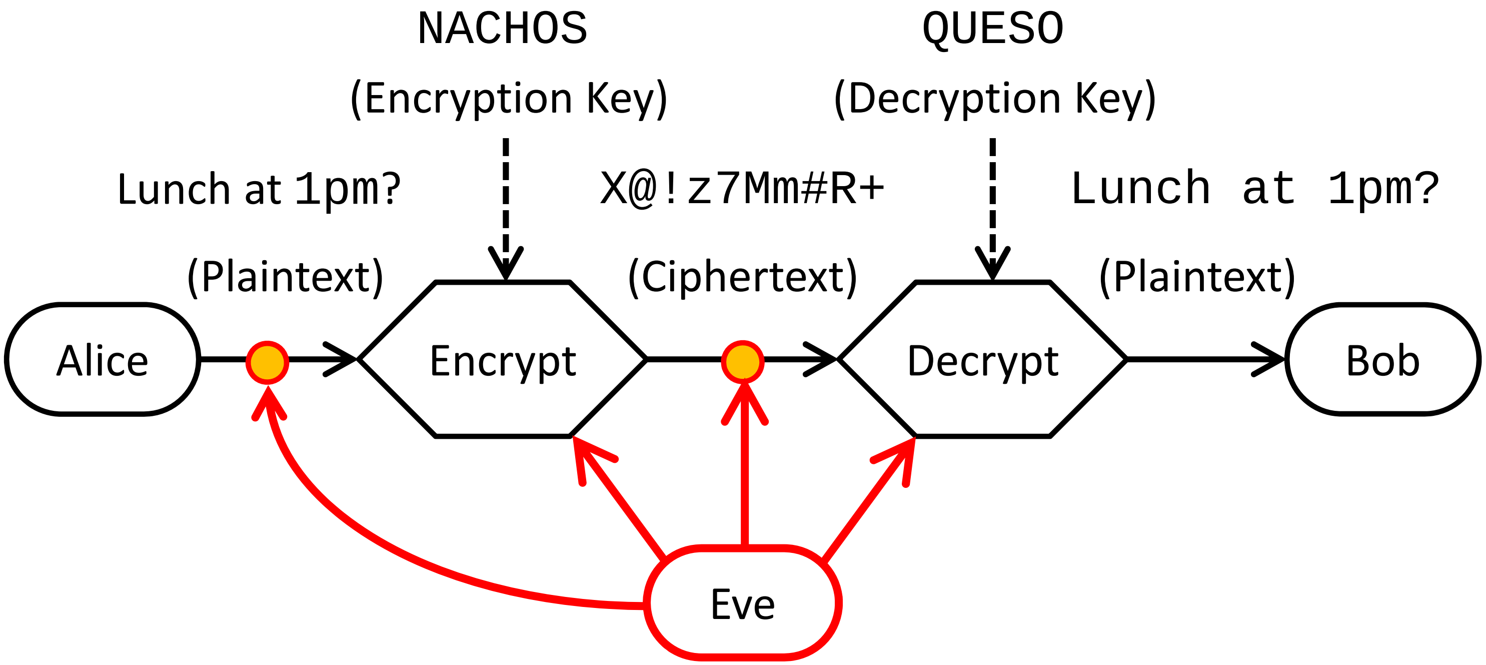
Eve's Potential Goals:

1. Read the message
2. Find the en(de)cryption key
3. Corrupt the message (violates integrity)
4. Pretend to be Alice (violates authentication)

Subsection 1.1.1

POSSIBLE ATTACKS

Cryptanalysis



Types of attack based on the amount of available information

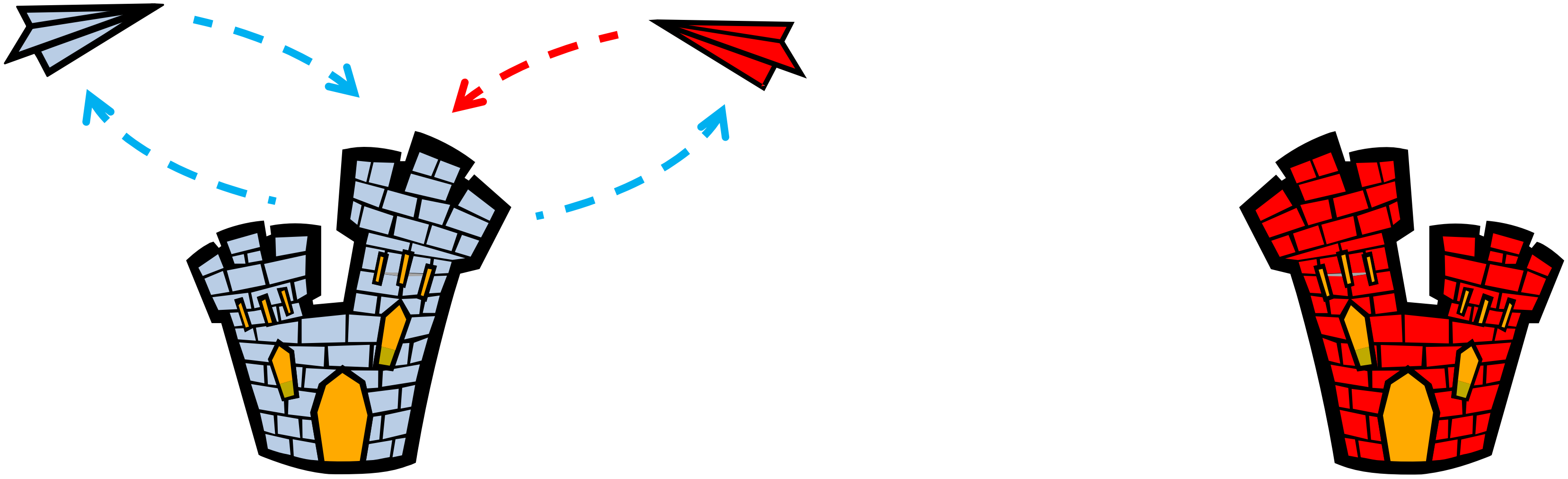
1. Ciphertext only
2. Known plaintext
3. Chosen plaintext
4. Chosen ciphertext

Examples

- **Known Plaintext**:
  - During the Sahara Campaign of WWII, General Montgomery was ordered to avoid an isolated German outpost which sent out the same message everyday,
    "*Keine besonderen Ereignisse*"
    that translates in English to
    "*nothing new to report.*"
  - Other stereotypical messages:
    - "*An die Gruppe*" (to the group)
    - "*weub null seqs null null*" (weather survey 0600)

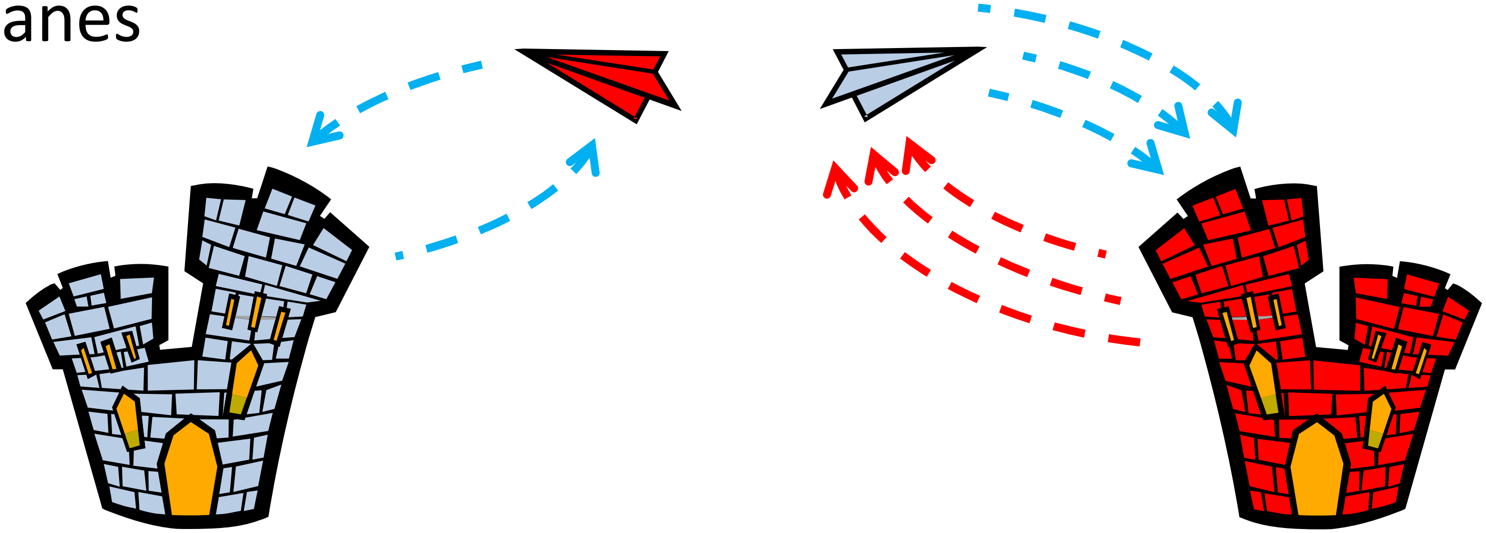
Examples

- **Chosen Plaintext:**
  - Base sends random message to the airplane
  - Airplane encrypts the message and replies to Base



Examples

- **Known Ciphertext**:
  - Enemy Sends a Bunch of Messages to Plane
  - Plane Encrypts and Replies to Enemy Base
  - Enemy Cracks Key and Masquerades their own Planes



Important Assumptions

- **Kerckhoff’s Principle** (1883):
  - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

- **Shannon’s Maxim** (1949):
  - The enemy knows the system

Subsection 1.1.2

SYMMETRIC AND PUBLIC KEY ALGORITHMS

Types of Encryption Keys

- **Symmetric Key**:
  both the encryption and decryption keys are known to Bob and Alice
  - All classical (pre-1970) cryptosystems
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

- **Public Key**:
  encryption key is made public decryption key is kept private
  - RSA (Integer Factoring)
  - ElGamal (Discrete Logs)
  - NTRU (Lattice Based)
  - McEliece (Error-Correcting)

Public Key Encryption

- **Example:**
  - Bob puts out an unlocked pad lock and a box.
  - *Anyone* can put something in and lock it.
  - *Only Bob* can unlock it.

Public

Private

Subsection 1.1.3

KEY LENGTH

Brute Force Attack

- Trying all possible keys and see which ones yield a meaningful decryption

Example: 56-bit key

- $2^{56} \approx 7.2 \times 10^{16}$ possible keys
- Computer tests 10^9 keys/second
- Takes 834 days to test all keys

“It’s not the size that counts”

- A longer key does not guarantee increased security
  - Substitution ciphers have $26! \approx 4.0 \times 10^{26}$ possible keys
    - Can be easily broken by frequency analysis
  - DES ciphers have $2^{56} \approx 7.2 \times 10^{16}$ possible keys
    - Brute force currently the only practical attack

Unbreakable?

- YES!
  - One-time Pad:

Plaintext:	000111000111000
Key:	+ 010010001000010
Ciphertext:	010101001111010

- Problems:
  - Key is as long as the message
  - Key can only be used once

Section 1.2

CRYPTOGRAPHIC APPLICATIONS

Cryptographic Applications

- Four Main Objectives

1. **Confidentiality** - keep messages secret
2. **Data Integrity** - preserve the content
3. **Authentication** - verify who sent/received
   - **Entity authentication**: prove identity of parties
   - **Data-origin**: tie metadata (who, when) to the message
4. **Non-repudiation** - confirms that a message was sent and by who

Cryptographic Applications

- Digital Signatures
- Identification
- Key Establishment
- Secret Sharing
- Security Protocols
- Electronic Cash
- Games