CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Video Summary

- What are Cryptography Tools
- What is Confidentiality
- How to Achieve Confidentiality
- Encryption For Confidentiality
- Attacks on Encryption Algorithms

Characterizing Cryptographic Systems

- **Operations used for encryption:**
  - Substitution: replace one element in plaintext with another
  - Transposition: re-arrange elements
  - Product systems: multiple stages of substitutions and transpositions

Hello world

FMOOR.....

Hello world

→ H L w l

→ e o o d

→ l r

HLWleoodl r

- **Type of keys used:**
  - Symmetric-key: sender/receiver use same key (single-key, secret-key, shared-key)
  - Public-key: sender/receiver use different keys (asymmetric)

Asymm,

- **Processing of plaintext:**
  - Block Cipher: process one block of elements at a time
  - Stream Cipher: process input elements continuously

byte by-byte

Block & Stream Ciphers

Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common ✓

Stream Cipher

Voice call.

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

Example Substitution Cipher: Caesar Cipher

weak

- **Encrypt:** Shift plaintext letters K positions to right

- **Example:**

26 Key

ComputerEngineering

Fr P s

Key=3 (how many keys we have?)

FrpsxwhuHqjlqhhulqj

1 ×

2 ×

3

https://www.xarg.org/tools/caesar-cipher/

Example Transposition Cipher: Rail-Fence Cipher

- **Encrypt:** Plaintext letters written in diagonals over K rows;
  ciphertext obtained by reading row-by-row

c P e n n r g
o u r g e i
m t E i e n

- **Example:**

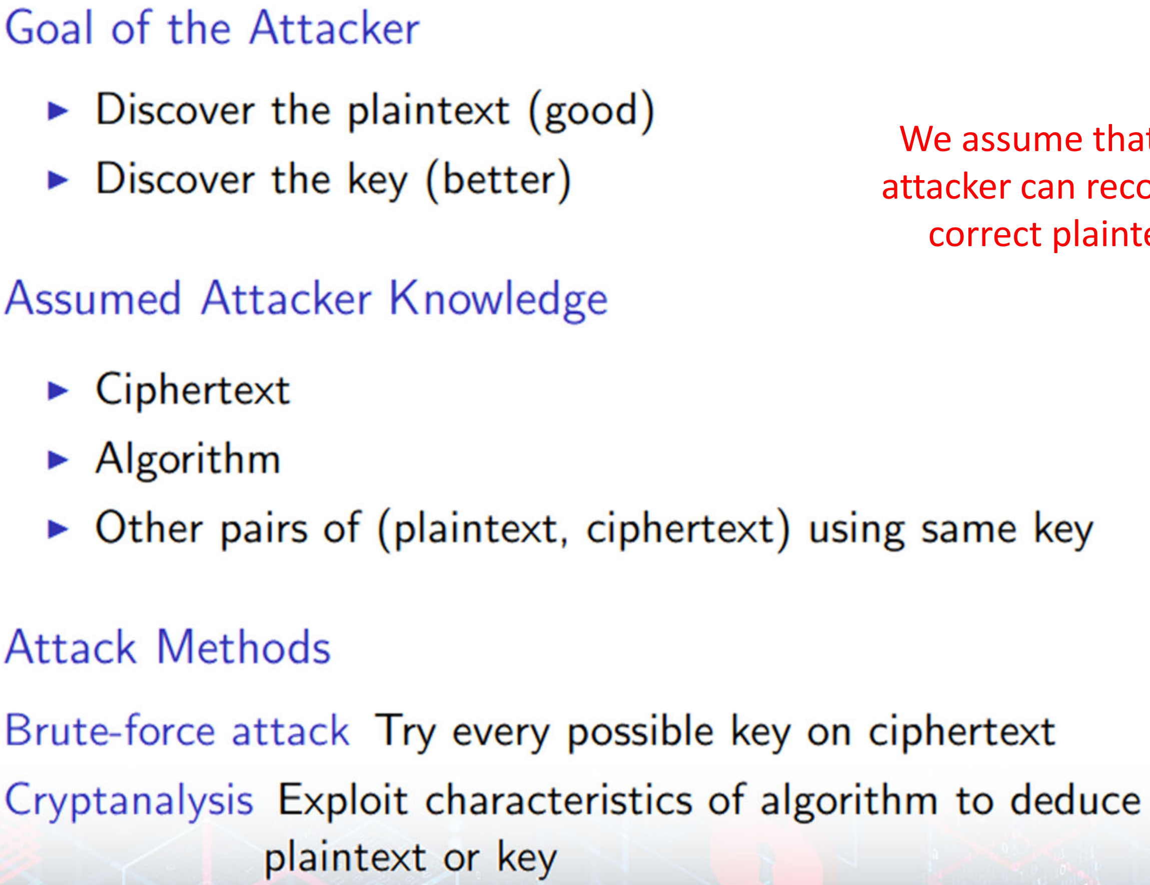
ComputerEngineering

Key=3

?

cPennrgourgeimtEien

Attacks



Goal of the Attacker

- Discover the plaintext (good)
- Discover the key (better)

We assume that the attacker can recognize correct plaintext

Assumed Attacker Knowledge

- Ciphertext
- Algorithm
- Other pairs of (plaintext, ciphertext) using same key

Attack Methods

Brute-force attack Try every possible key on ciphertext

Cryptanalysis Exploit characteristics of algorithm to deduce plaintext or key

Video Summary

- What are Cryptography Tools ✓
- What is Confidentiality ✓
- How to Achieve Confidentiality ✓
- Encryption For Confidentiality ✓
- Attacks ✓