

Intro. to Cryptography

COMS 4261

Prof. Zeph Grunschlag

URL: www1.cs.columbia.edu/~zeph/4261

Cryptography

cryptography - science of designing secure communication methods

- *crypt* - “secret” in Latin
- *graphia* - “writing”

cryptanalysis - science of breaking such methods

cryptology = *cryptography* + *cryptanalysis*

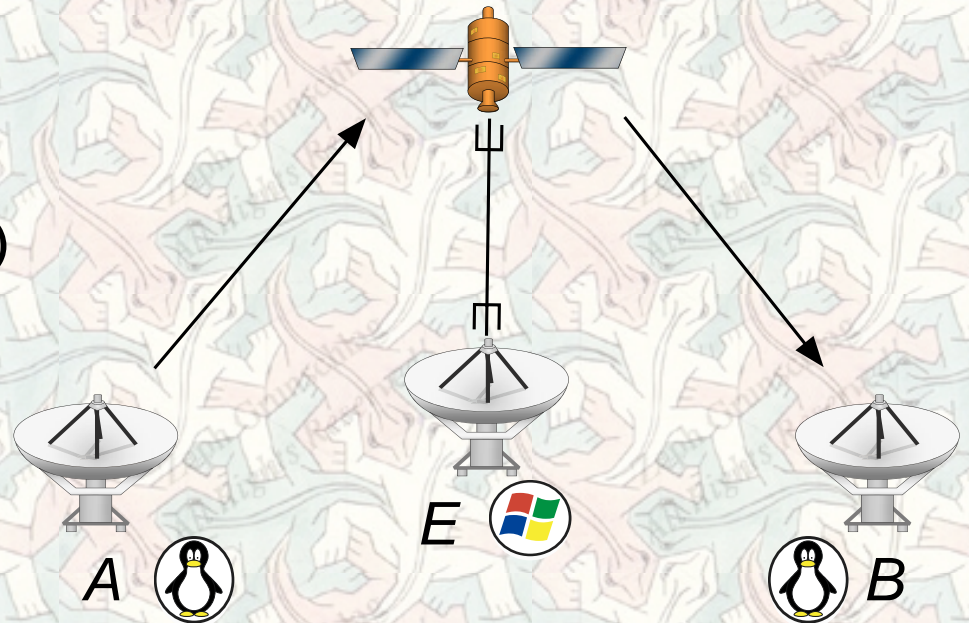
steganography - science of *hiding* communication

Classical Problem

PRIVACY

PROBLEM: Alice (*A*) sends Bob (*B*) a message *M* over insecure channel (e.g. radio) eavesdropped by Eve (*E*)

GOAL: *A* scrambles *M* in a way that *E* cannot decipher but that *B* can



Additional Problems

Authenticity - *B* assured that *M* unchanged

Identity - *B* assured that *A* wrote *M*

Non-repudiation - *A* can't deny writing *M*

Coin flipping - *A* and *B* flip coin over phone

Secret sharing - *A*, *B* can only reveal secret working together

Complex protocols - *electronic elections, digital cash, secret leaking traceability, etc.*

Security Model History

- I. Originally none - invent cipher and assume secure
- II. Classically - cryptanalysis driven
- III. Shannon - defined perfect secrecy
-
- IV. Computational - find some computationally intractable problem which reduces to cracking the given crypto protocol

Primitives

A **primitive** is mathematical object with a basic cryptographic property not admitting further modularization

Primitives : Protocols :: Atoms : Molecules

- One-way functions
- One-way functions with trapdoor
- Pseudorandom number generators
- Pseudorandom functions

What you will learn...

...All of the above

Setting: rigorous mathematical approach

Pre-requisites:

- Must: **discrete math**
- Recommended: **computability theory OR algorithm analysis**
- Helpful: familiarity with *number theory*, *probability*, and *randomized algorithms*

What you will NOT learn...

... won't come close to reflecting all of crypto

... IPSEC, SSL, SSH, or any other protocol that is used in practice

... architecture specific design, or even the most efficient possible algorithms

... hacking, viruses, trojan-horses, DeCSS, firewalls, or any other computer security

Our **Advanced Crypto** deals with first issue, and our **Network Security** course addresses much of the last three

Text

- Cryptography: Theory and Practice, 2nd Ed.
by Douglas R. Stinson
- Additional online sources will be provided

Grades

- 5 or 6 homeworks - 50%
- Midterm - 20%
- Final - 30%

Each portion *curved*

Collaboration Policy

On **homework**

- **GOOD:** study with friends, bounce ideas off each other, solve problems together, then write your own solutions at home **from scratch** and **list all your collaborators** on the top of homework
- **BAD: not listing collaborators OR copying** in any way, shape or form any part of the solution from another source

On **exams - NONE!!!!**