

Cryptography CS 555



Lecture 1: Security services, attacks and mechanisms

Department of Computer Sciences
Purdue University

Course Information

- Meetings
 - Tu&Th 1:30-2:45 PM
- Professor contact info:
 - Office: REC 217D/CS174
 - Email: crisn@cs
 - **Office hours: TuTh 3 – 4 PM in CS174**
- TA: Jayesh Pandey
 - Office: MATH B3
 - Office hours: W 1:30 - 3:30
 - Email: jpandey@cs
- Class webpage

http://www.cs.purdue.edu/homes/crisn/courses/cs555_2005

Grading Policy

- Written Assignments (~6) 20%
- Final Project 25%
- Midterm Exam 20%
- Final Exam 30%
- Class Participation 5%
- Undergrads are required to attend class

Homework

- Homework must be TYPED.
- Homework is due and will be returned in class at 1:30.
- Every student has 3 extra days for all the written assignments that he can use. Email me and the TA with name and number of extra days used for an assignment. After using your 3 extra days, no late homework will be accepted.
- You **must work alone** on the assignments.
- **NO CHEATING!**



Exams and Project

- Midterm - February 24
- Final – check university web page
- Project:
 - Teams of 2/3 required
 - Proposal due one week before midterm
 - Must have a practical aspect
 - There will be a meeting with the professor to discuss the results of the project
 - **PLEASE COME AND TALK TO ME IF YOU HAVE PROBLEMS WITH YOUR PROJECT, DON'T WAIT TILL THE LAST DAY!!!**



Course Overview (1)

- Concepts and principles of cryptography: security services, attacks and mechanisms.
- Classical cryptographic systems: shift cipher, Vigenere and Vernam ciphers, Jefferson wheel cipher and the Enigma machine.
- Block ciphers: DES, Blowfish, RC5, IDEA, AES.
- Stream ciphers: SEAL, RC4.



Course Overview (2)

- Public-key encryption: RSA, ElGamal, Rabin.
Probabilistic cryptosystems: Goldwasser-Micali.
- Data integrity: hash functions, MD5, SHA1, HMAC.
- Digital signatures: RSA, ElGamal, DSA, Schnorr.
- Authentication protocols, data and entity authentication. One time passwords, Lamport's scheme, challenge-response schemes, Kerberos.



Course Overview (3)

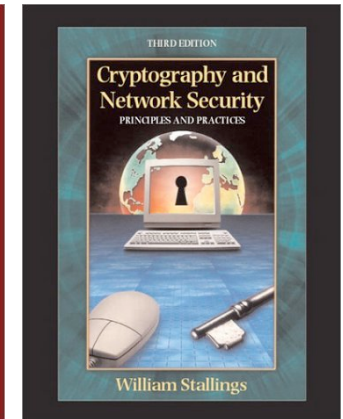
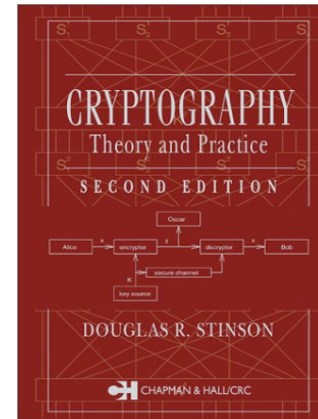
- Key management: two-party key exchange and group key management protocols.
- Verifiable encryption and applications.
- Digital rights.
- Zero-knowledge proofs.
- Identity-based cryptosystems.
- Notions of threshold cryptography.
- Proactive security.



Reference Material

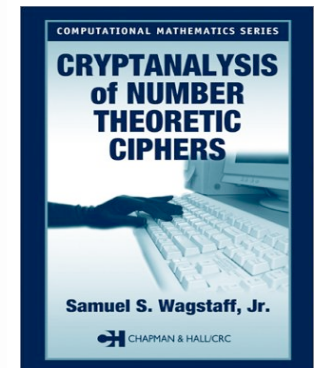
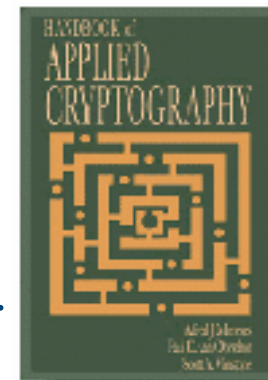
- Textbooks

- D. R. Stinson, *Cryptography (Theory and Practice)*, Second Edition, CRC Press 2002.
- W. Stallings, *Cryptography and Network Security, Principles and Practice*, Third Edition, Prentice Hall, 2002.



- Recommended reading

- Handbook of Applied Cryptography (HAC) Menezes, Oorschot, Vanstone, CRC Press (<http://www.cacr.math.uwaterloo.ca/hac/>)
- Cryptanalysis of Number Theoretic Ciphers. S. S., Wafstaff, Jr, CRC Press



Academic Integrity

- Purdue University Academic Integrity:

<http://www.purdue.edu/ODOS/administration/integrity.htm>

- Class policy

<http://www.cerias.purdue.edu/homes/spaf/cpolicy.html>

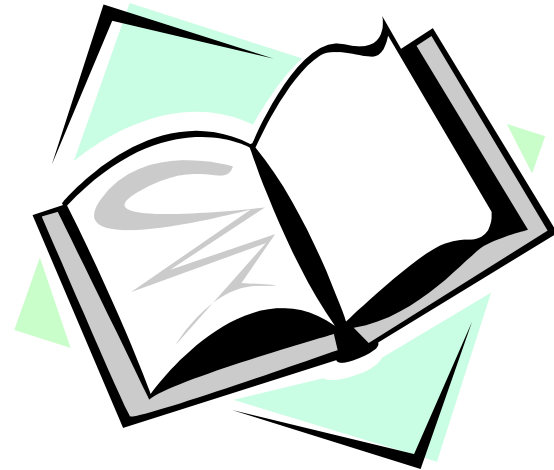
Lecture Outline

- Security services.
- Security attacks.
- Security mechanisms.
- Terminology.
- Attacks of ciphers and cryptographic protocols.



Recommended Reading

- Stallings: Chapter 1
- HAC: Chapter 1
- Wagstaff: Chapter 1

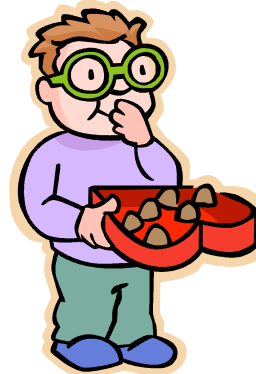


Let's Make the Introductions

- Alice



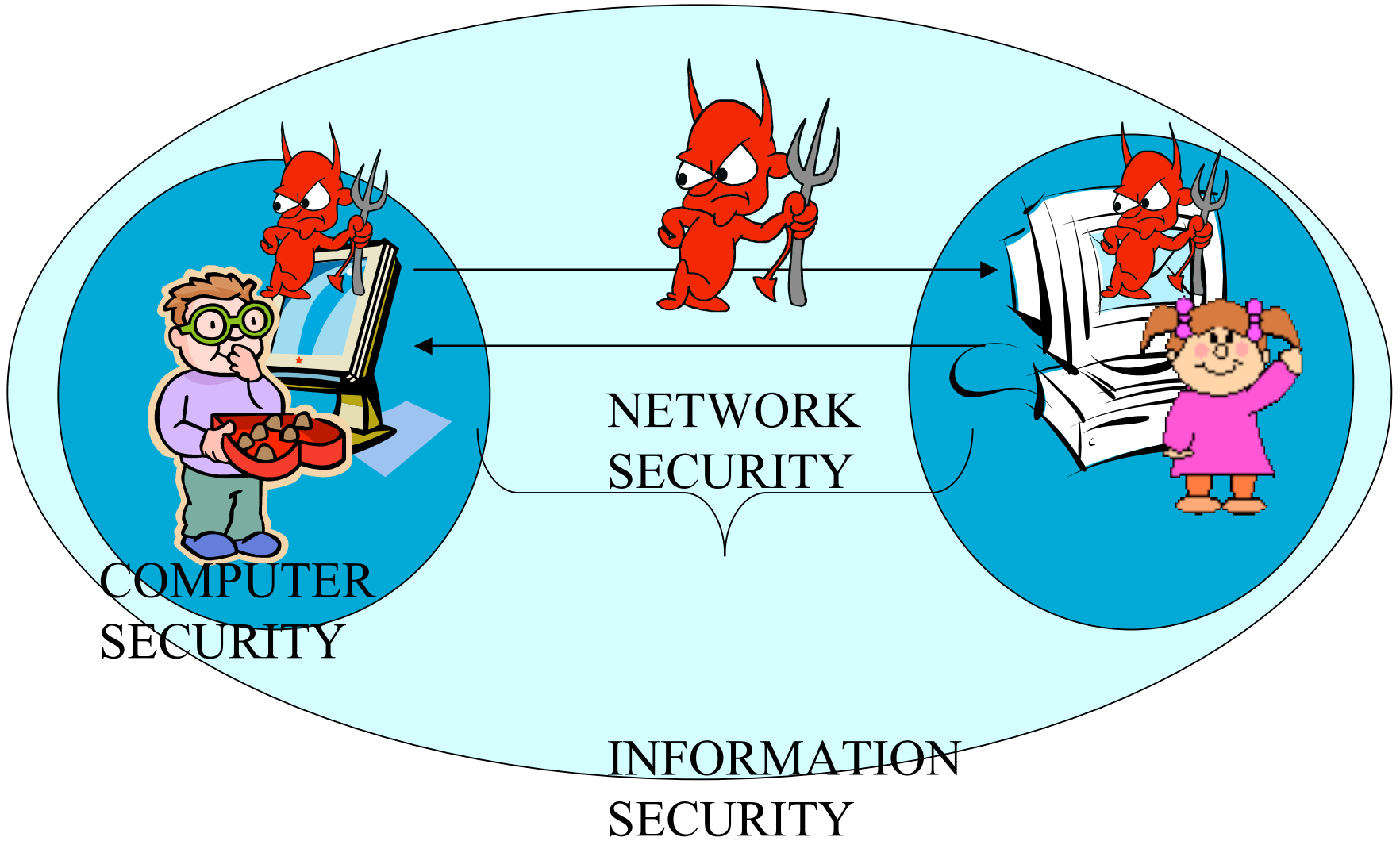
- Bob



- Carl(or Eve)



Information Security



Information Security

- **Security attacks:** Any action that compromises the security of information.
- **Security mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Services (or Goals)

- **1) Confidentiality:** information is available for reading only to authorized parties.

Example: Alice sends a message to Bob, only Alice and Bob can understand the content of the message.

- **2) Authentication:**

- Data source authentication: the data is coming from an authorized party.

Example: Alice receives a message from Bob. This service ensures that the message is from Bob and not from Carl.

- Entity authentication: the entity is who it says it is.

Example: When Alice tries to obtain access to her bank account, an authentication operation is performed to ensure that Alice asks for the information.

Security Services (2)

- **3) Integrity:** detect if data was modified, from the source to the destination.

Example: Alice sends an email to Bob. Carl intercepts the message and modifies it. Data integrity allows for Bob to detect that the message was modified on the way from Alice to him.

- **4) Non-repudiation:** neither the sender, nor the receiver of a message are able to deny the transmission.

Example: Alice sends Bob a contract, signed. The non-repudiation service ensures that Alice can not claim that the signature was produced by somebody else.

Security Services (3)

- **5) Access control:** only authorized parties can use specific resources.

Example: Alice wants to print a document, she must be authorized to get that document and to use the printer.

- **6) Availability:** resources available to authorized parties.

Example: A web site might become unavailable if the server crashes, or is bombarded with requests.

Security Attacks

- **Passive:** the attacker does not modify the data, only monitors the communication. It **threatens confidentiality**.

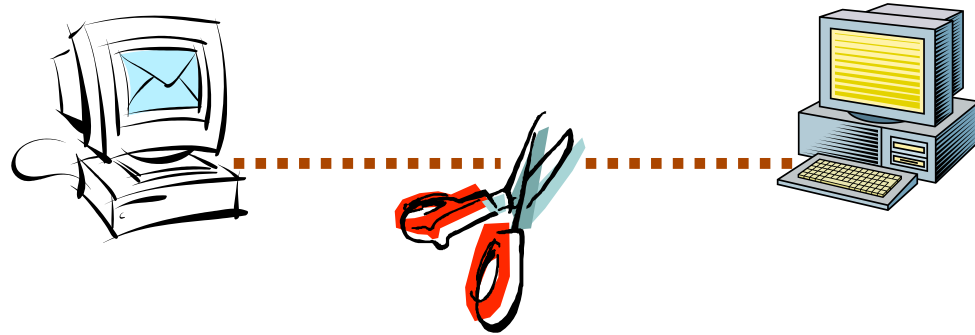
Example: listen to the communication between Alice and Bob, and if it's encrypted try to decrypt it.

- **Active:** the attacker is actively involved in deleting, adding or modifying data. It **threatens all security services**.

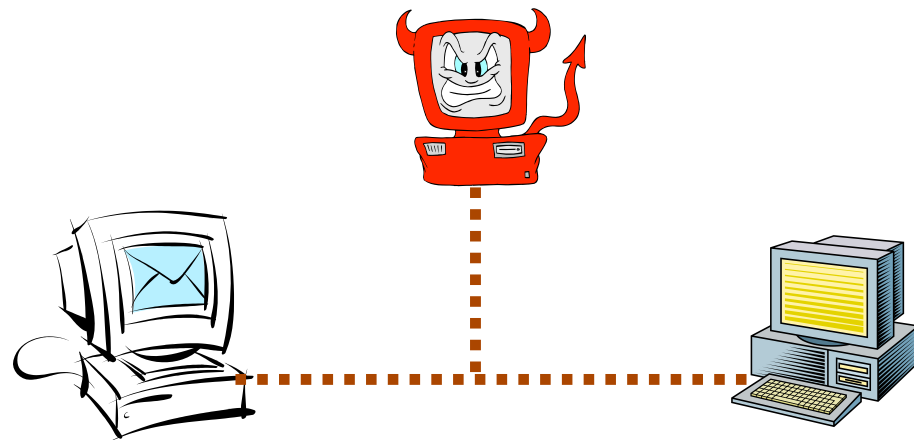
Example: Alice sends Bob a message: 'meet me today at 5', Carl intercepts the message and modifies it 'meet me tomorrow at 5', and then sends it to Bob.

Security Attacks: Examples

- Interruption

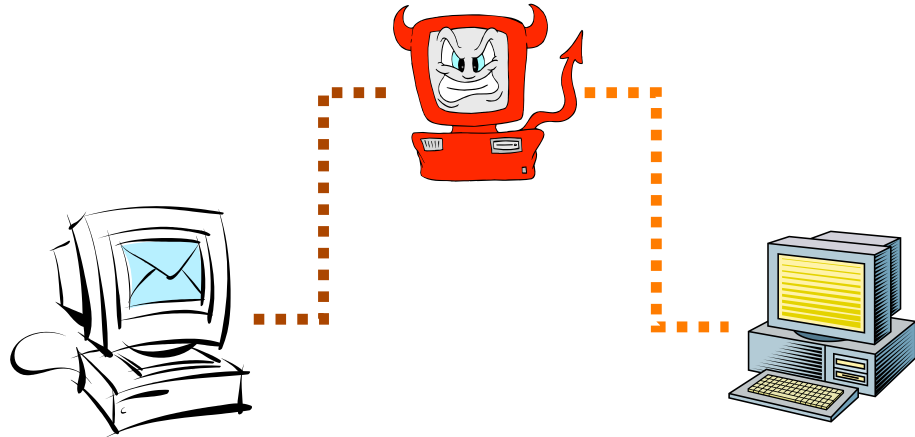


- Interception

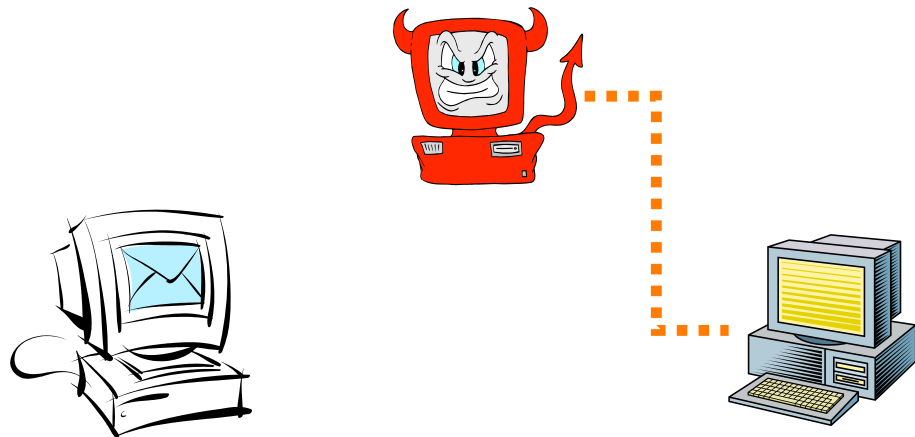


Security Attacks: Examples

- Modification

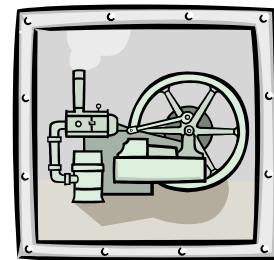


- Fabrication (injection)



Security Mechanisms

- **Cryptography:** protect data by performing operations on the data (for example encrypt data).
- **Software:** access limitations to in a database, in operating system protect each user from other users, networking: firewall.
- **Hardware:** use smartcards for authentication.
- **Policies:** define who has access to what resources.
- **Physical security:** control who has physical access to devices storing data.



What Is Cryptography ?

- **Cryptography**: the study of mathematical techniques related to aspects of information security.
- **Cryptanalysis**: the study of mathematical techniques for attempting to defeat information security services.
- **Cryptology**: the study of cryptography and cryptanalysis.



Cryptographic Primitives

- Encryption
- Key management
- Hash functions
- Digital signatures
- Certificates and CAs



Symmetric and Public Cryptography

- Symmetric cryptography:
 - Parties that communicate, share a secret.
 - Used mainly to encipher/decipher data.
 - Examples: DES, Blowfish, AES, RC4.



How obtain the secret key in the first place ?

- Public cryptography:
 - Each party has a PAIR (P, S) of keys: P is the **public** key and S is the **secret** key.
 - Used mainly to distribute keys and create digital signatures.
 - Examples: RSA, ElGamal.



What is a Cryptosystem?

Plaintext: data to be 'hidden' or protected

Ciphertext: the result of applying a crypto operation
on the data

encryption

decryption

plaintext $\xrightarrow{\quad}$ ciphertext $\xrightarrow{\quad}$ ciphertext

Definition

A **cryptosystem** is a five-tuple (P, C, K, E, D) , s. t.:

1. P is a finite set of possible plaintexts
2. C is a finite set of possible ciphertexts
3. K , the keyspace, is the set of possible keys
4. For each $k \in K$, there are
 - encryption rule $e_k, e_k: P \rightarrow C$,
 - decryption rule $d_k, d_k: C \rightarrow P$,
 - s.t. $d_k(e_k(x)) = x$

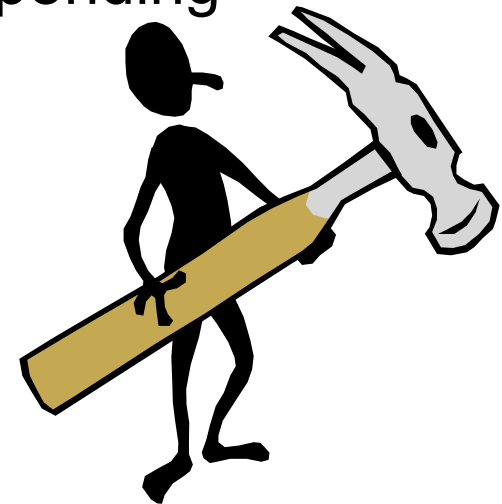
Going Back to Cryptanalysis...

- There are different methods of breaking a cipher, depending on:
 - the type of information available to the attacker
 - the interaction with the cipher machine.



Breaking Ciphers...

- **Ciphertext-only attack:** The cryptanalyst knows only the ciphertext. Sometimes the language of the plaintext and the cipher are also known. Goal: find the plaintext and the key.
- NOTE: any encryption scheme vulnerable to this type of attack is considered to be completely insecure.
- **Known-plaintext attack:** The cryptanalyst knows several pairs of ciphertext and corresponding plaintext. The goal is to find the key used to encrypt these messages or a way to decrypt any new messages that use that key.

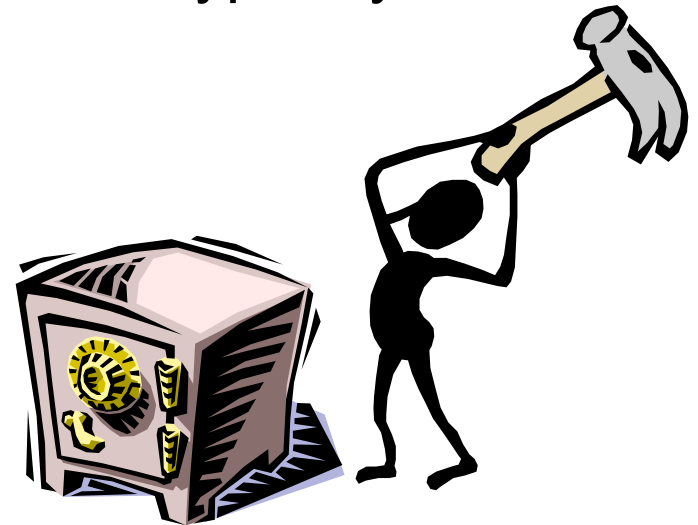


Breaking Ciphers (2)

- **Chosen-plaintext attack**

The cryptanalyst knows a number of encrypted messages, and he can also encrypt any message he chooses. The goal is to deduce the key used in the other encrypted messages or decrypt any new messages using that key.

- It can be **adaptive**, the choice of plaintext depends on the ciphertext received from previous requests.



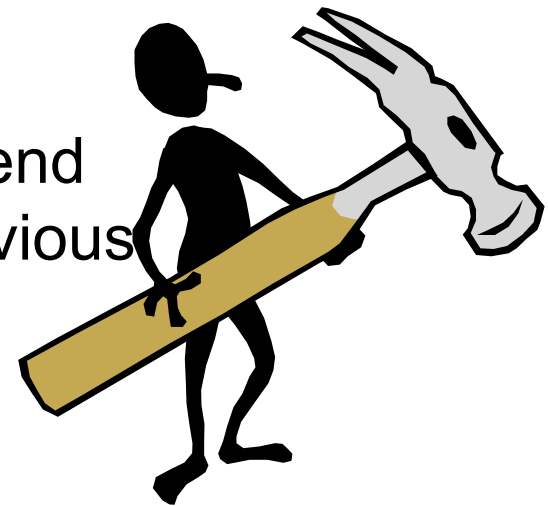
Breaking Ciphers (3)

- **Chosen-ciphertext attack**

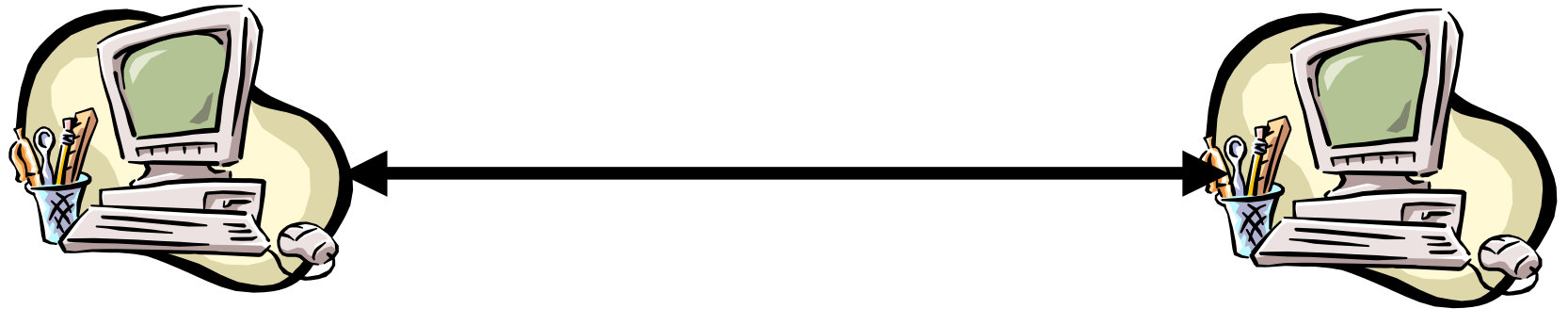
Similar to the chosen-plaintext attack, but the cryptanalyst can choose the ciphertext, not the plaintext. The goal is to obtain the key.

- **It can also be adaptive**

The choice of ciphertext may depend on the plaintext received from previous requests.



Protocols



Definition:

A network protocol defines rules for:

- sending/receiving packets
- the format and type of the packets
- actions in response of receiving a certain type of packets ...

A cryptographic protocol also specifies what cryptographic mechanisms are used.

Attacks on Protocols

- **Known-key attack**

This attack uses previously used keys to determine new keys used for encryption.

- **Replay attack**

In this type of attack, an attacker records a communication session and later on replays that session.

- **Impersonation attack**

This attack deceives the identity of one of the legitimate parties.

Attacks on Protocols

- **Dictionary attack**

This attacks usually targets passwords. The attacker uses a dictionary of plaintext/ciphertext encrypted with all possible keys.

- **Forward search attack**

This attack is similar with the dictionary attack and is used if the message space is small or predictable, with the goal of decrypting messages.

- **Interleaving attack**

Impersonation or other deception involving selective combination of information from parallel sessions; it is an attack against authentication.

Models for Evaluating Security

- **Unconditional security**

The adversary has unlimited computational resources. Analysis is made by using probability theory. Perfect secrecy: observation of the ciphertext provides no information to an adversary.

- **Complexity-theoretic security**

The adversary is assumed to have polynomial computational power. The analysis uses complexity theory; Polynomial attacks although feasible, in practice can be computationally infeasible.

Models for Evaluating Security

- **Provable security:** Proof of security relies on the difficulty of solving a well-known and supposedly difficult problem (example: computation of discrete logarithms).
- **Computational security (practical security):** Measures the amount of computational effort required to defeat a system. Sometimes related to the hard problems, but no proof of equivalence is known.
- **Ad hoc security (heuristic security):** Variety of convincing arguments that every successful attack requires more resources than the ones available to an attacker. Unforeseen attacks remain a threat.

Summary

- Cryptography is an important mechanism used to defend against attacks on computers and networks.
- Encryption schemes and protocols can be attacked in several ways, classified depending on the computational power and the amount of information available to the attacker.



Recommended Reading for Next Lecture

- Chapter 1 from Stinson

