Cryptography and Data Security (CSCE-544)

Major Addison Betances

Air Force Institute of Technology

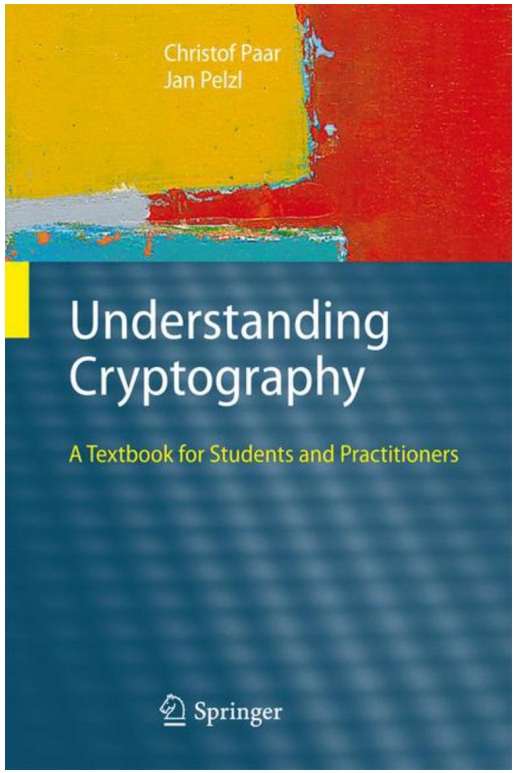
25-March-2019

Overview

Instructor

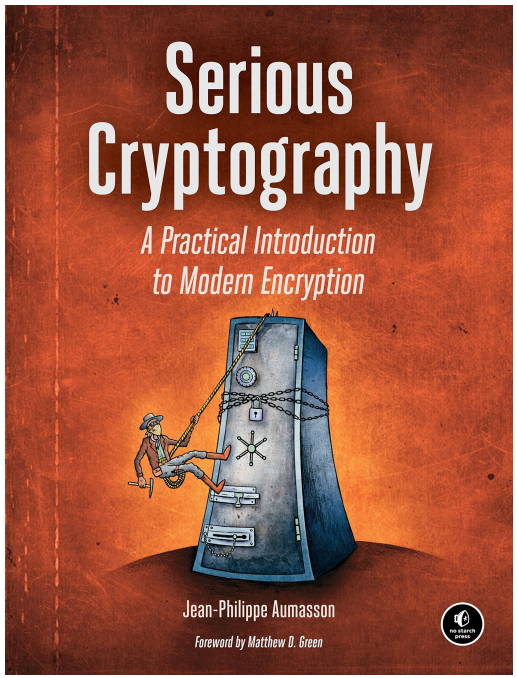
J. ADDISON BETANCES, Maj, USAF, Ph.D.
Assistant Professor
Department of Electrical and Computer Engineering
Comm: (937)255-3636 x3305
Cell: (509)301-5901
DSN: 750-3636 x3305
email: jbetance@afit.edu, addison.betances@gmail.com
Office Hours: By appointment.

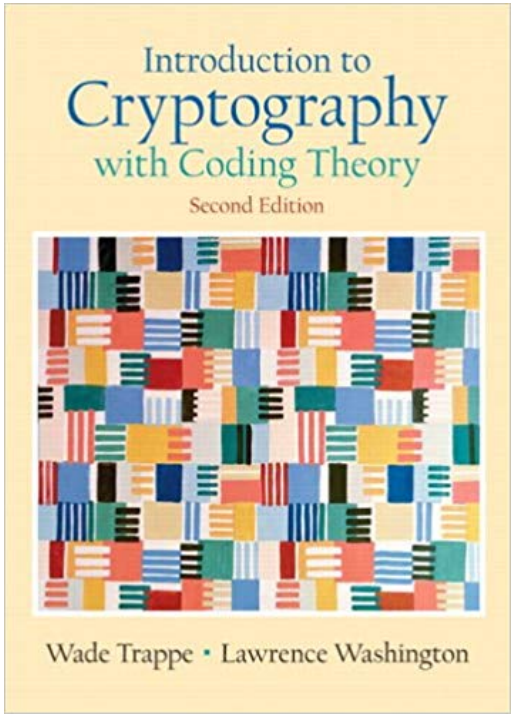
Required Text



Paar, C., and Pelzl, J., 2010, *Understanding Cryptography: A Textbook for Student and Practitioners*, Springer, ISBN 978-3-642-04100-6.

Additional References





Aumasson, Jean-Philippe, 2018, *Serious Cryptography: A Practical Introduction to Modern Encryption*, No Starch Press, 978-1593278267.

Trappe, W. and Washington L, 2005, *Introduction to Cryptography with Coding Theory (2nd Edition)*, Prentice Hall, ISBN 978-0131862395.

Course Description

This course presents the rudiments of data security. The emphasis is on cryptography, beginning with simple ciphers, extending through symmetric cryptography to asymmetric cryptography based on sophisticated number theory considerations. Other core topics include information theory, key management, hashing algorithms, message authentication codes and digital signatures.

Grades

Grade Distribution:

Assignments	35%
Midterm Exam	30%
Final Exam	35%
Total	100%

Examinations: Two exams will be given for this course: a midterm exam and the final exam. The final exam will be comprehensive. Exams are to be worked solely by the individual. There is to be no collaboration of work on exams. Exams will have an in-class portion and a take-home portion.

Homework: Homework must be individual effort. Other students may be consulted for approaches to solving problems but all work must be your own. Submit a hardcopy during class and email me a softcopy with all the source code used to solve the problems. Please do not "drop off" your work at my office.

Course Objectives

At the completion of this course, successful students will be able to:

1. Identify critical security requirements and choose appropriate security primitives to meet a range of data security needs.
2. Implement basic ciphers to include substitution ciphers, streaming ciphers, and parts of the Data Encryption Standard.
3. Understand information theory concepts underlying modern ciphers and hashing algorithms.
4. Comprehend mathematical concepts in group theory as it pertains to modern encryption in Integer rings, Galois fields, cyclic groups, the discrete logarithm problem and Elliptic curves.
5. Solve encryption and decryption functions using modular arithmetic, Euclidean and Extended Euclidean algorithm, the Chinese Remainder Theorem, prime factorization, and discrete logarithms.
6. Understand basic concepts for cryptographic and key distribution protocols.

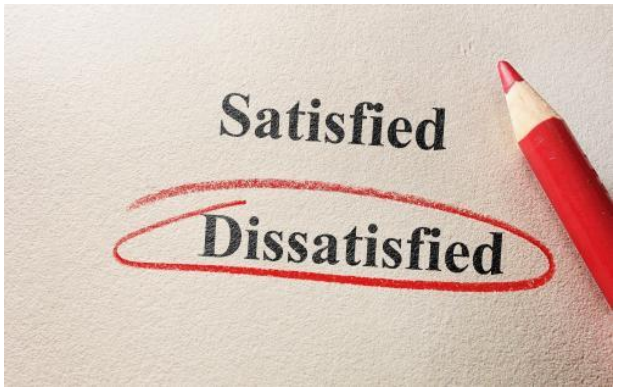
Policies

Attendance: Attendance at all class sessions and exams is mandatory for military and civilians assigned to AFIT as full-time students except for extenuating circumstances. Scheduled classes and exams are defined by the instructor and they are documented in the course schedule. Part-time students are expected to attend scheduled classes, and absences should be explained to the instructor. The student should provide advance notice, if possible. (References: Student Handbook, Graduate School Catalog)

Policies

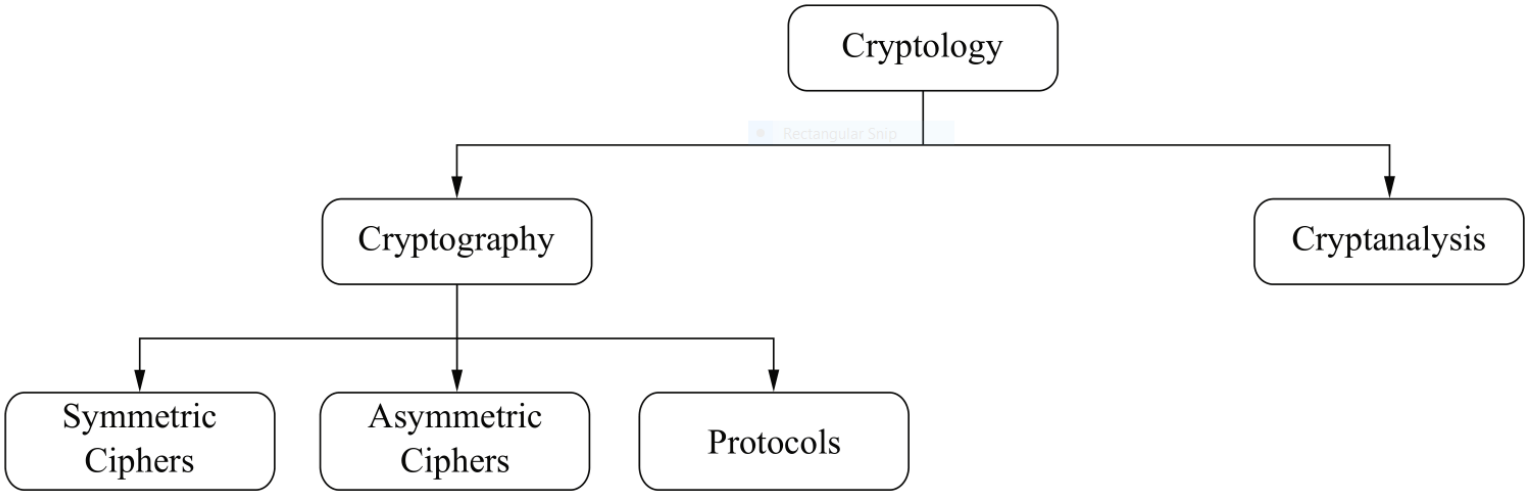
Academic Integrity: All students must adhere to the highest standards of academic integrity. Students are prohibited from engaging in plagiarism, cheating, misrepresentation, or any other act constituting a lack of academic integrity. Failure on the part of any individual to practice academic integrity is not condoned and will not be tolerated. Individuals who violate this policy are subject to adverse administrative action including disenrollment from school and disciplinary action. Individuals subject to the Uniform Code of Military Justice may be prosecuted under it. Violations by government civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (References: Student Handbook, ENOI 36 - 107, Academic Integrity)

Policies



Academic Grievance: AFIT and the Graduate School of Engineering and Management affirm the right of each student to resolve grievances with the Institution. Students are guaranteed the right of fair hearing and appeal in all matters of judgment of academic performance. Procedures are detailed in ENOI 36 - 138, Student Academic Performance Appeals.

Definitions



Overview of the field of cryptology

Cryptography: is the science of secret writing with the goal of hiding the meaning of a message.

Cryptanalysis: is the science and sometimes art of *breaking* cryptosystems.
Cryptanalysis is of central importance for modern cryptosystems: without people who try to break our crypto methods, we will never know whether they are really secure or not.

Definitions

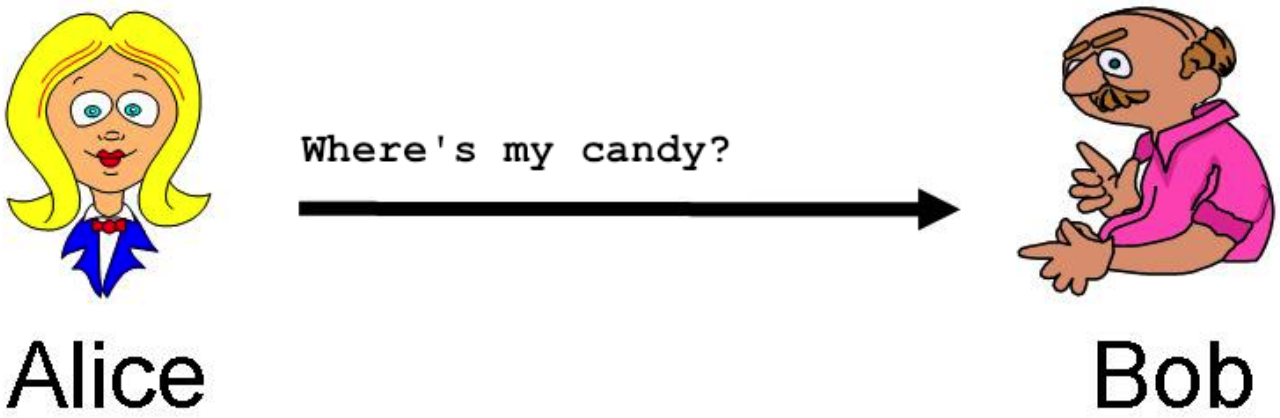
Symmetric Algorithms: are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.

Asymmetric Algorithms or **Public-key cryptography**: is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.

Definitions

Cryptographic Protocols: Roughly speaking, crypto protocols deal with the application of cryptographic algorithms. Symmetric and asymmetric algorithms can be viewed as building blocks with which applications such as secure Internet communication can be realized. The Transport Layer Security (TLS) scheme, which is used in every Web browser, is an example of a cryptographic protocol.

Alice and Bob



Alice and **Bob** are the canonical "protagonist" of the crypto world, frequently used in illustrations to demonstrate how a cryptographic system works.

Eve

Eve is the canonical "antagonist" of the crypto world, always trying to **eave**sdrop messages between **Alice** and **Bob**.

Things Eve would like to do

- Read the message
- Find the Key - allowing her to read all messages encrypted with that key
- Corrupt Alice's message so Bob thinks Alice is saying something different
- Pretend to be Alice while Bob still thinks he is in communication with Alice

Which tenets of the Information Security model do these represent?

Cryptographic Information Security

CIANA

- **C**onfidentiality
- Data **I**ntegrity
- **A**vailability
- **N**on-repudiation
- **A**uthentication

Cryptanalysis methods

Ciphertext Only: Attackers only sees ciphertext

- Exhaustive key search (brute force)
- Frequency analysis

Known plaintext: Attacker has both the ciphertext and (a portion of) the plaintext (headers of packets)

Chosen plaintext: Attacker has temporary access to the encryption machine and can make encryptions of her own plaintexts

Chosen ciphertext: Attacker obtains temporary access to the decryption machine and can decrypt several message

Kerchoffs's principle

When assessing security, assume the adversary knows the method being used Don't assume that an obfuscation of the method is enough to prevent an adversary from determining it.

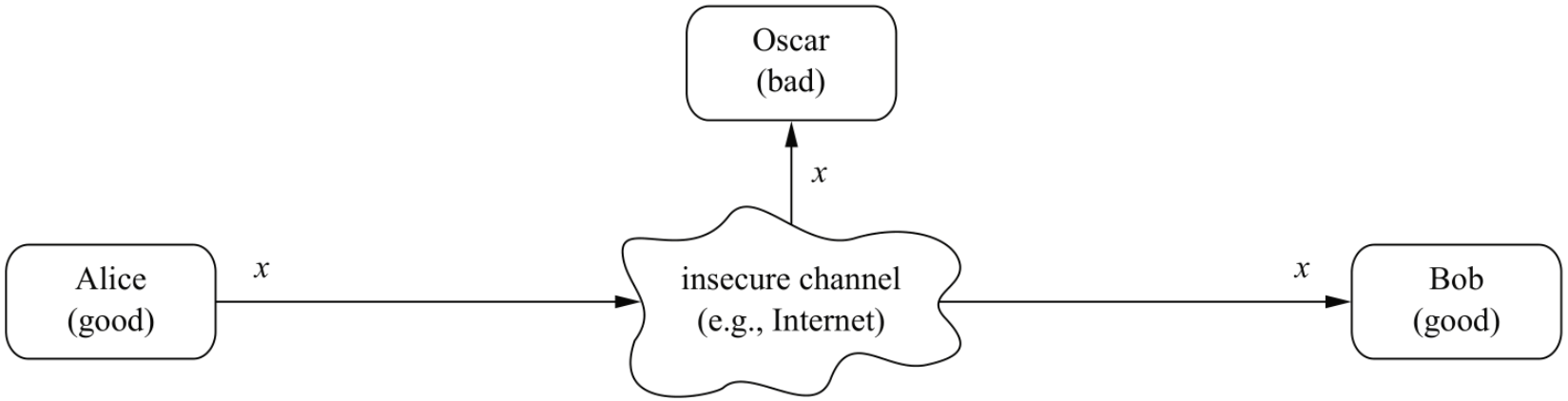
- Assume attacker knows the encryption algorithm
- Implication #1: Security lies in protecting the key rather than the algorithm.

Kerchoffs's principle

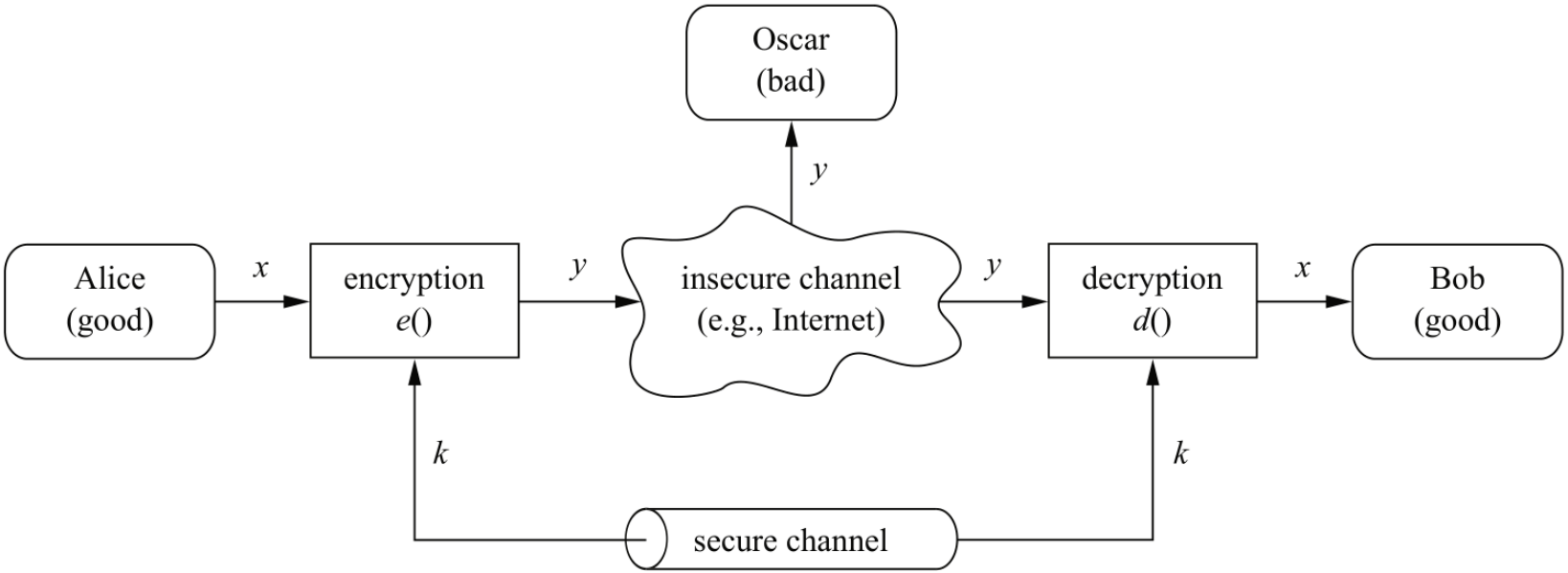
The system must be practically, if not mathematically, indecipherable:

- It should not require secrecy, and it should not be a problem if it falls into enemy hands;
- It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
- It must be applicable to telegraph communications;
- It must be portable, and should not require several persons to handle or operate;
- Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

Communication Over an Insecure Channel



Eve or **Oscar** can listen to the communication between **Alice** and **Bob**. The name **Oscar** was chosen to remind us of the word opponent.



Symmetric-key cryptosystem

- x is called *plaintext* or *cleartext*
- y is called *ciphertext*
- k is called the key
- the set of all possible keys is called the key space

Easy Challenge

The following code has been encrypted using a Caeser Shift Cypher. Obtain the **plaintext** using **cyphertext only** cryptanalysis. Spaces have been substituted with *, to simplify the cryptanalysis.

VJKU*KU*XGT_*GCU_

Challenge!!!

The following code has been encrypted using a Caeser Shift Cypher. Obtain the **plaintext** using **cyphertext only** cryptanalysis.

RGHESZBHOGDQRZ_QDZMNSZRDBTQD