Introduction to Modern Cryptography

Instructor: Prof. Benny Chor

School of Computer Science

Tel- Aviv Univ.

Administrative Details

- Grade –exam (60-70%), homework (30-40%).
- Exam on January $30^{th,}$ 2002.
- Homework submition in pairs.
- 4-5 ``dry'' assignments.
- 1-2 "wet" assignments (in MAPLE).
- Office hours: By e-appointment.
- E-mail: benny@cs.tau.ac.il

Course Outline

- Encryption
- Data integrity
- Authentication and identification
- Digital signatures
- Number theory
- Randomness and pseudo-randomness
- Cryptographic protocols
- Real world security systems

Related & Highly Recommended

Dr. Amir Herzberg Course on

E-Commerce

Given on Wednesdays' mornings

Prerequisites:

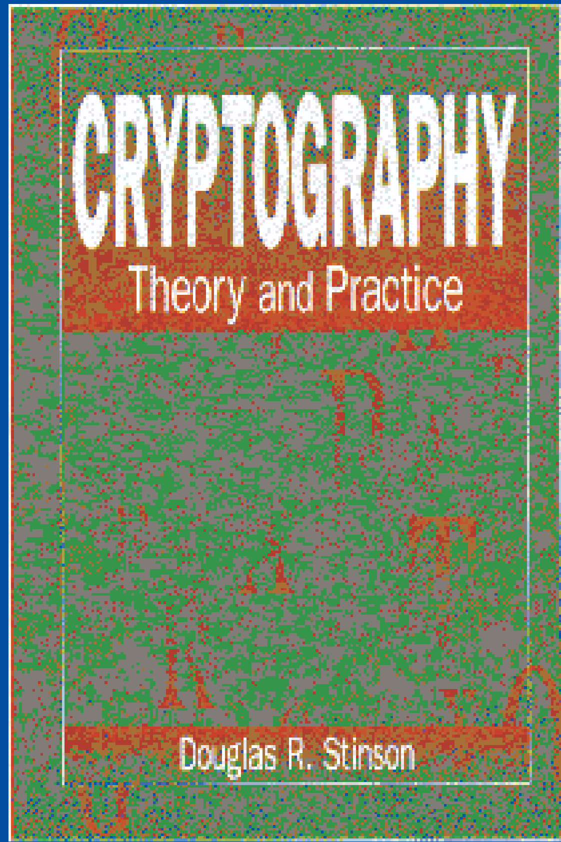
Linear Algebra

Probability

Computational Models

“Mathematical Maturity”

Bibliography



- Text Book:
  Cryptography Theory and Practice, D. Stinson, CRC Press, 1996.
  (should be available at the library in 3-4 weeks)

- Recommended:
  - *Handbook of Applied Cryptography* Menezes, Van Oorschot, Vanstone (free download at http://www.cacr.math.uwaterloo.ca/hac)
  - *Applied Cryptography*, B. Schneier

Good Crypto Courses on the Web

- Hugo Krawczyk course at the Technion.
- Ron Rivest course at MIT.
- Dan Boneh course at Stanford.
- Phil Rogaway Course at UC Davis.
- Eli Biham course at the Technion.
- Doug Stinson course at Waterloo.

Encryption

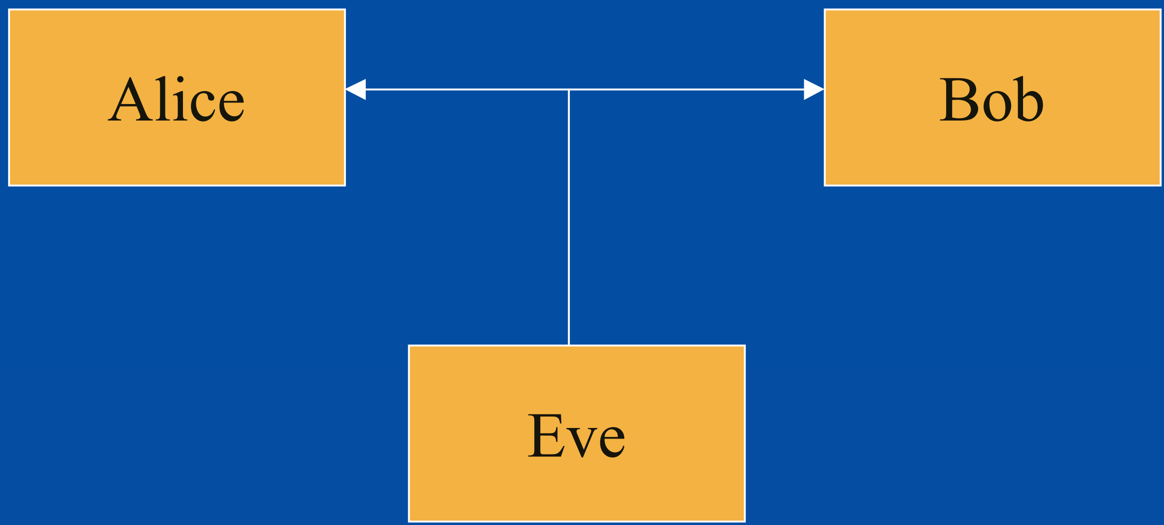
Definitions

- Encryption function (& algorithm): E
- Decryption function (& algorithm): D
- Encryption key k_1
- Decryption key k_2
- Message space (usually binary strings)
- For every message m: $D_{k2}(E_{k1}(m)) = m$

Communication Model

1. Two parties – Alice and Bob
2. Reliable communication line
3. Shared encryption scheme: E, D, k_1, k_2
4. Goal: send a message *m* confidentially

Threat Model



4. Goal: send a message *m* confidentially

Security Goals

Possibilities:

- No adversary can determine *m*
- No adversary can determine <u>any</u> information about *m*
- No adversary can determine any <u>meaningful</u> information about m.

Adversarial model

- Eve attempts to discover information about m
- Eve knows the algorithms *E,D*
- Eve knows the message space
- Eve has at least partial information about $E_{k1}(m)$
- Eve does not know k_1, k_2

Examples – bad ciphers

- Shift cipher
- Conclusion – large key space required
- Substitution cipher
- Large key space, still “easy” to break

Substitution cipher

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	W	H	O	V	I	B	P	L	C	J	Q	X	D	K	R	Y	E	S	Z	A	F	T	M	G	N	U

Example:

- plaintext: attack at dawn
- ciphertext: waaoq wa vwmk

Size of key space: 26!=403291461126605635584000000

$\sim 4 \times 10^{28}$ large enough

Additional definitions

- Plaintext – the message prior to encryption
  (“attack at dawn”, “sell MSFT at 57.5”)
- Ciphertext – the message after encryption
  (“ÈÁÏÚÎ ÁÚÎÔË‡ÎÎÚÎ”,“jhhfoghjklvhgbljhg”)
- Symmetric key – encryption scheme where $k_1 = k_2$
  (classical cryptography)

Perfect Cipher

- Plaintext space – $\{0,1\}^n$
- Given a ciphertext C the probability that $D_{k2}(C)=P$ for any plaintext P is equal to the apriori probability that P is the plaintext.

  In other words:

  $$Pr[\text{plaintext}=\text{P}|C] = Pr[\text{plaintext}=\text{P}]$$
- Probabilities are over the key space and the plaintext space.

Example – One Time Pad

- Plaintext space - $\{0,1\}^n$
- Key space - $\{0,1\}^n$
- The scheme is symmetric, key *k* is chosen at random
- $E_k(P) = C = P \oplus K$
- $D_k(C) = C \oplus K = P$

Pros and Cons

- Claim: the one time pad is a perfect cipher.
- Problem: size of key space.
- Theorem (Shannon, rest his soul): A cipher is perfect only if its key space is at least the size of its message space.

Computational Power

- Time
- Hardware
- Storage
- Theoretical – polynomial time
- Practical – 2^{64} is feasible, 2^{80} is infeasible

Security Model

- Eavesdropping
- Known plaintext
- Chosen plaintext
- Chosen ciphertext
- Adaptive chosen text attacks
- Physical access
- Physical modification of messages