Cryptography
ENEE/CMSC/MATH 456

Instructor: Dana Dachman-Soled

Lecture 1

1/28/2019

Syllabus Highlights

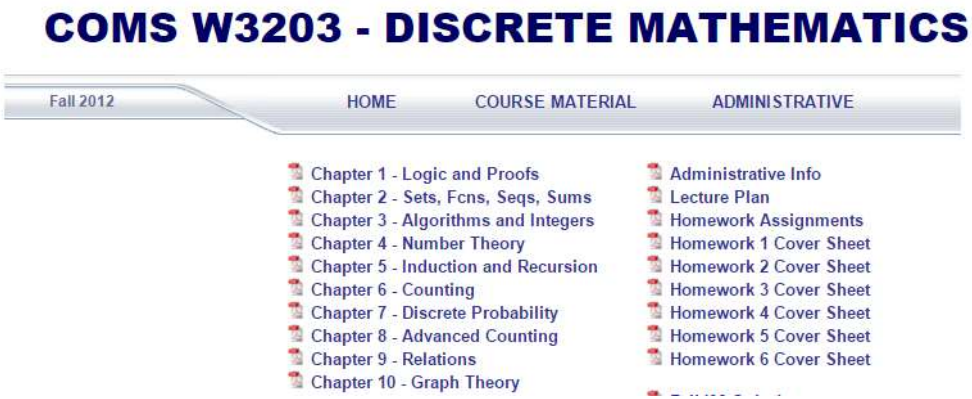
- Best way to contact me is via email:
  - danadach@ece.umd.edu
- My office hours: Mon 11am-noon, Fri 9-10am in 3407 AV Williams
- Our TA: Sandeep Raju
  - sraju410@terpmail.umd.edu
- TA Office hours: T, Th 3-4pm in 3412 AV Williams.
- Class url:
  - www.ece.umd.edu/~danadach/Cryptography_19

Syllabus Highlights cont'd

- Small Quizzes/Class Exercises
  - More on next slide
- Weekly homeworks (about 10-12 overall)
  - Late homework not accepted
  - Lowest grade will be dropped
- Grading Policy:
  - Small Quizzes/Class Exercises—5%
  - Homework—25%
  - Midterm—35%
  - Final—35% (not cumulative)
  - **Extra credit opportunity relating to current events
  - **Extra credit opportunity after the midterm
- Tentative midterm date: In class on Wednesday, March 13.

Reading Assignment/Quizzes

- Upcoming: Review of basic math, discrete math (combinatorics, probability).
- Read Chapters 1,2,3,6,7 of Prof. Jonathan Gross's lecture notes (link on course webpage):



- 5 short 5-question quizzes on Canvas, one for each chapter.
- Each quiz will be approx. .5% of total grade.
- ***Due on Feb. 15, 11:59pm.
- Additional resources: Rosen, K. H. (2012) Discrete Mathematics and Its Applications. (7th ed.).

Additional Announcements

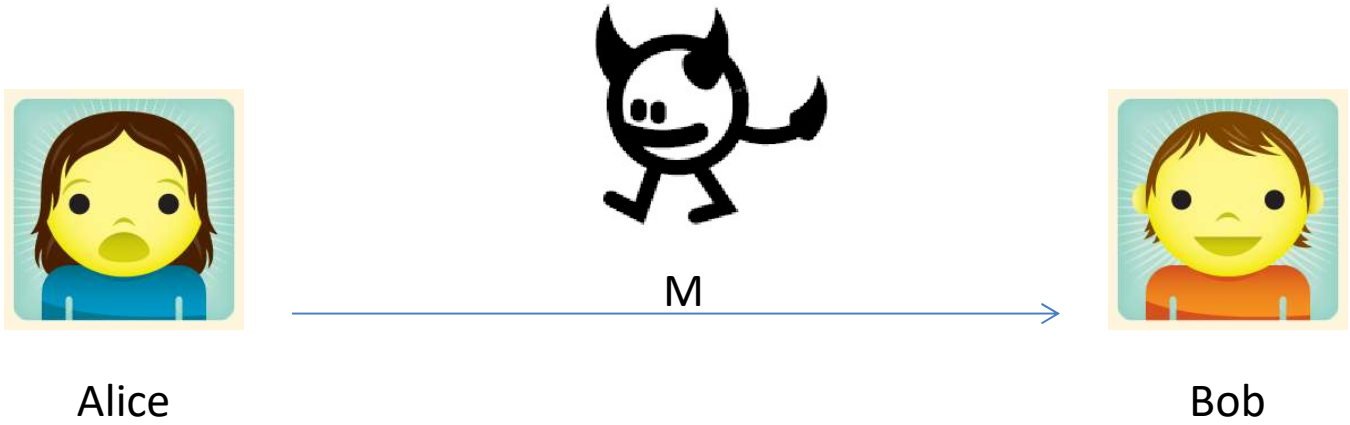
- Homework 1 is up on the course webpage. Due on 2/6 **by beginning of class.**
- There is a Piazza page for this course.
  - Watch out for email invite.
- Encourage students to collaborate on homework, ask questions on Piazza.
- Final submitted solutions must be *your own*.

Goals of Modern Cryptography

- Providing information security:
  - Data Privacy
  - Data Integrity and Authenticity

  in various computational settings.

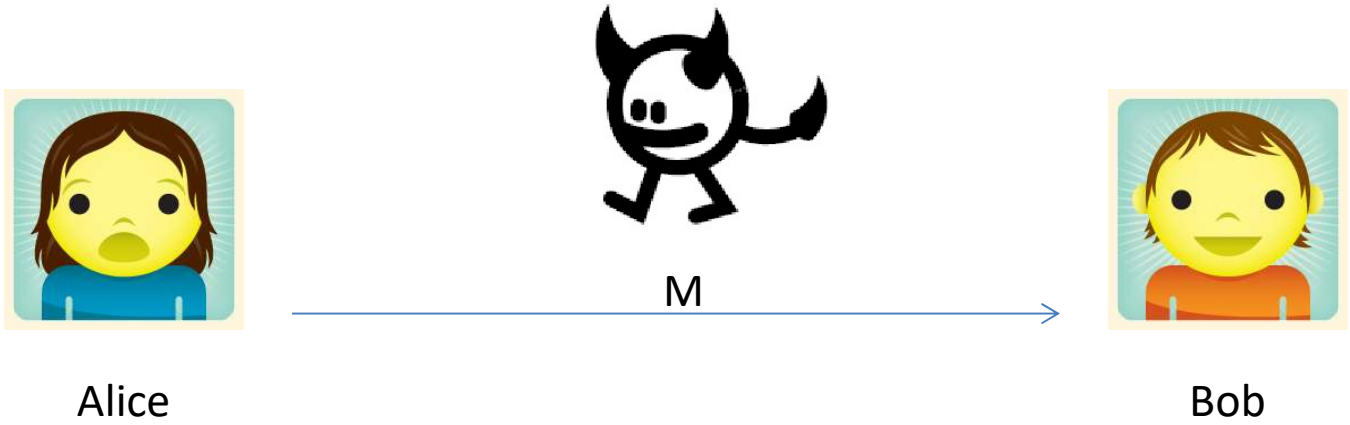
Data Privacy



The goal is to ensure that the adversary does not see or obtain the data (message) M.

- Example: M could be a credit card number being sent by shopper Alice to server Bob and we want to ensure attackers don't learn it.

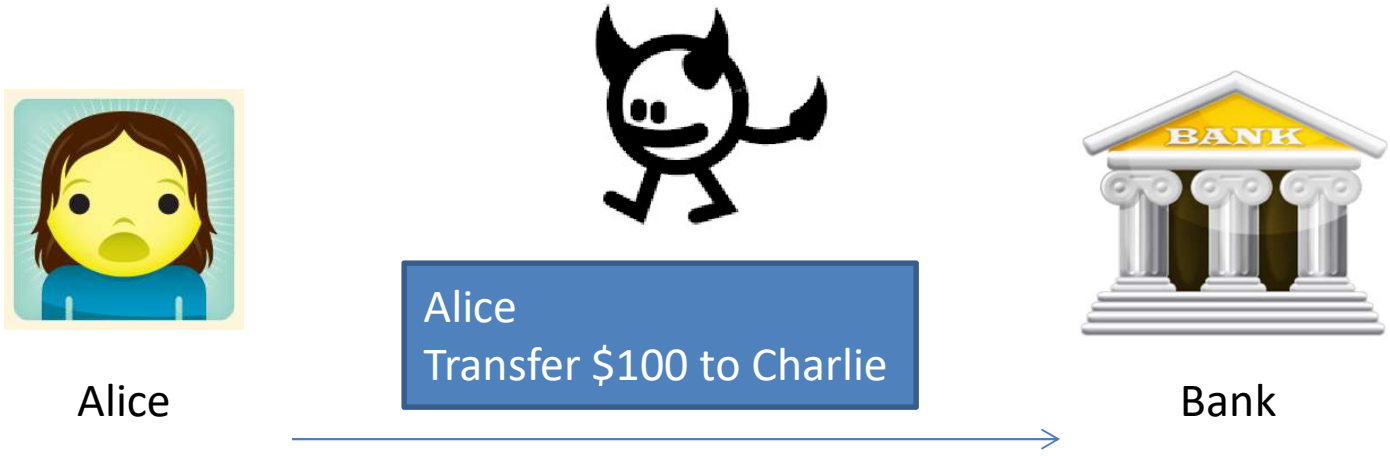
Data Integrity and Authenticity



The goal is to ensure that

- M really originates with Alice and not someone else.
- M has not been modified in transit.

Data Integrity and Authenticity



Adversary Eve might

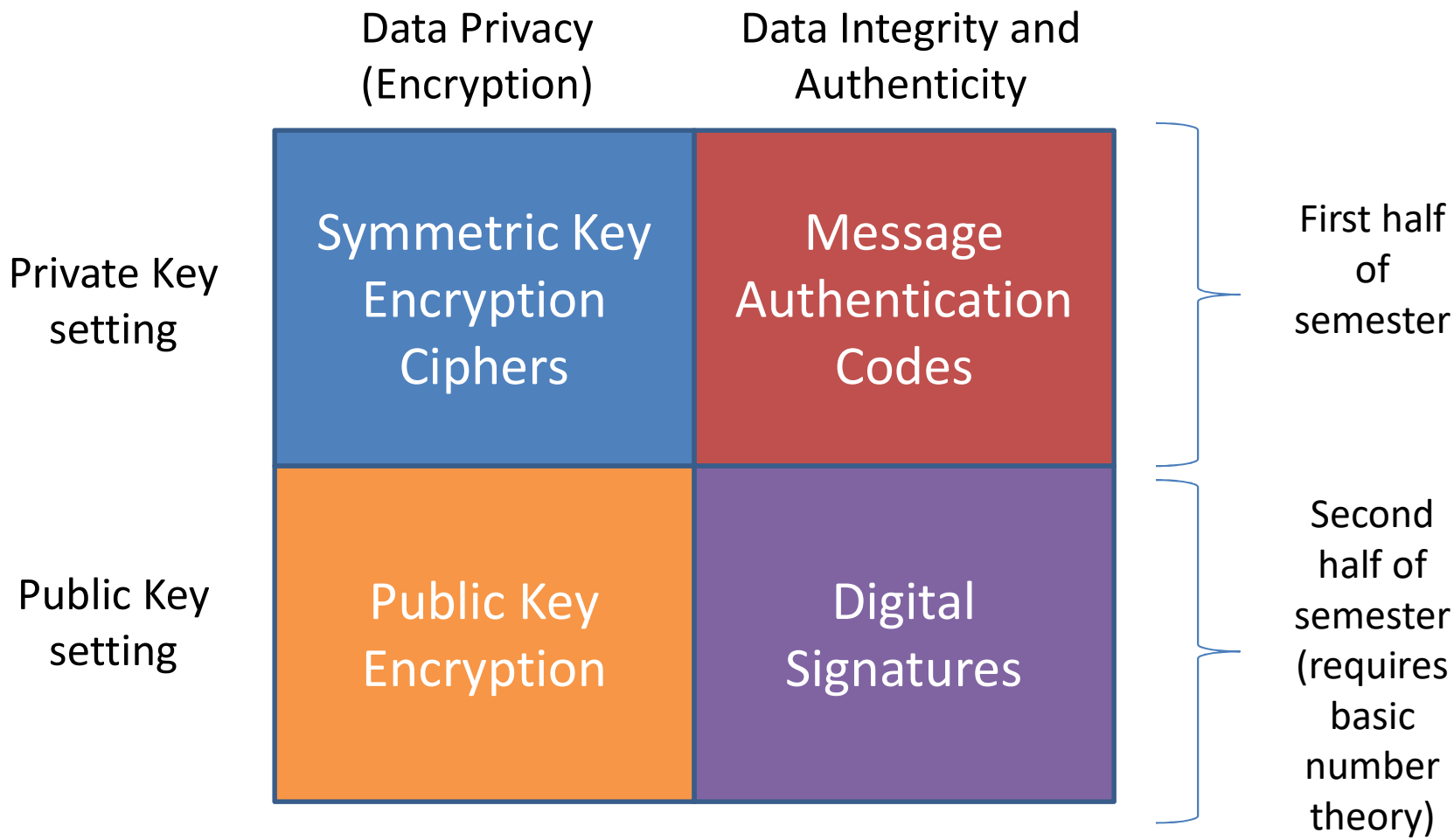
- Modify “Charlie” to “Eve”
- Modify “$100” to “$1000”

Integrity prevents such attacks.

General Topics

- Explore how to define security
  - What does it mean for something to be “secure”
  - Defining a threat model, placing computational restrictions
- Explore how to prove security
  - Mathematical proofs, proofs by reduction
  - Computational assumptions
- Learn about tools for building secure schemes
  - Tools for practical symmetric key constructions
  - Tools from number theory for public key constructions
- See lots of constructions of cryptographic schemes:
  - Symmetric key encryption (block ciphers, stream ciphers), Message Authentication codes (MAC), Collision-resistant hash functions, Key exchange, Public key encryption, Digital signatures.

What we will be doing this semester



Today:

- We will start on symmetric key encryption (also called ciphers).

Symmetric Key Encryption
(Historically called “ciphers”)

Kerckhoffs' Principle (1800s)

"The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience."

Today: Parties share a secret key which allows them to encrypt and decrypt, the scheme itself is public.

Advantages of open crypto design:

1. More suitable for large-scale usage.
   - All pairs of communicating parties can use the same scheme with different key.
2. Published designs undergo public scrutiny and are therefore likely to be stronger.
3. Public design enables the establishment of standards.

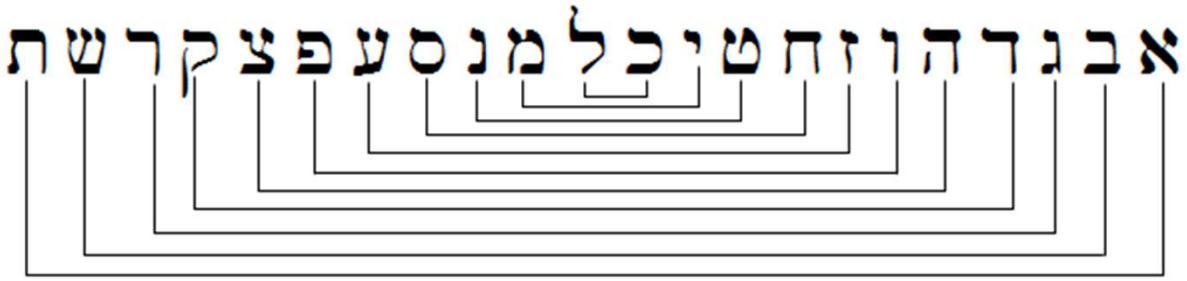
Historical Ciphers and their Cryptanalysis

For each cipher we discuss:

- What is the Encrypt algorithm?
- What is the Decrypt algorithm?
- What is the key space, key space size and secret key?
- How can it be broken?

Atbash Cipher (600 B.C.)

From Wikipedia: **Atbash** is a simple substitution cipher for the Hebrew alphabet. It consists in substituting *aleph* (the first letter) for *tav* (the last), *beth* (the second) for *shin* (one before last), and so on, reversing the alphabet. In the Book of Jeremiah.



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

helloworld → SVOOLDLIOW

Shift/Caesar Cipher (100 B.C.)

From textbook: One of the oldest recorded ciphers, known as Caesar's cipher is described in "De Vita Caesarum, Divus Iulius" ("The Lives of the Caesars, The Deified Julius"), written in approximately 110 C.E.

Example: Caesar cipher with shift 19.
Outer wheel is plaintext letter.
Inner wheel is ciphertext letter.

Discussion

- Previous schemes: Either scheme is fixed (no secret key) or key space is small.
- If cipher method is public (as prescribed by Kerckhoffs) then these are completely broken by "brute force" search.
- Conclusion: key space must be large for cipher to be secure against "brute force" search.
- Is large key space sufficient for security?

Scytale Cipher (600 B.C.)

From Wikipedia: From indirect evidence, the scytale was first mentioned by the Greek poet Archilochus, who lived in the 7th century BC. Other Greek and Roman writers during the following centuries also mentioned it, but it was not until Apollonius of Rhodes (middle of the 3rd century BC) that a clear indication of its use as a cryptographic device appeared. A description of how it operated is not known from before Plutarch (50-120 AD):

Thin sheet of papyrus wrapped around staff. Messages are written down the length of the staff.

In order to recover the message, a staff of equal diameter must be used.

Monoalphabetic Substitution (800 A.D.)

- Each plaintext character is mapped to a different ciphertext character in an arbitrary manner.

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

tellhimaboutme → GDOOKVCXEFLGCD

- Size of key space?
  - $26! \approx 2^{88}$
- Brute force search is intractable, but is there a better way to break this cipher?

Frequency Analysis

If plaintext is known to be grammatically correct English, can use frequency analysis to break monoalphabetic substitution ciphers: