Welcome to:
Introduction to Cryptology
ENEE 459E/CMSC498R

Lecture 1

1/27/2015

Announcements

- Syllabus highlights:
  - Best way to contact me is via email: danadach@ece.umd.edu
  - My office hours: Tues 11am-12pm, Thurs 10am-11am in 3407 AV Williams
  - Our TA: Qian Wang email: qwang126@umd.edu
  - TA Office hours: Wed 3:30pm-5pm in 1143 AV Williams
  - Class url: www.ece.umd.edu/~danadach/Intro_Crypto_Spring_15

Announcements

- Syllabus highlights (cont’d):
  - Weekly homeworks (about 10-12 overall)
    - Late homework not accepted.
  - Grading policy:
    - Homework—30 %
    - Midterm Exam—35 %
    - Final Exam—35 % (not cumulative)
  - Tentative midterm date: In class on Thursday, March 12

Agenda

- What is modern cryptography all about?
- Goals of this course
- Symmetric key encryption schemes (ciphers) and Kerckhoff’s principle (Section 1.2)
- Historical ciphers (Section 1.3)
- Cryptanalysis of historical ciphers (Section 1.3)
- Towards a definition of security for an encryption scheme

Modern Cryptography

- Public Key Encryption

RSA Laboratories RSA

- Digital Signatures

SecurityInnovation THE APPLICATION SECURITY COMPANY NTRU Sign

- Secure Multiparty Computation

RCIM NEWS online edition

And lots more. . .

- Zero knowledge proofs
- Computing on encrypted data
- Fast verification
- Program obfuscation
- Steganographic secure computation
- Rational secure computation
- . . .

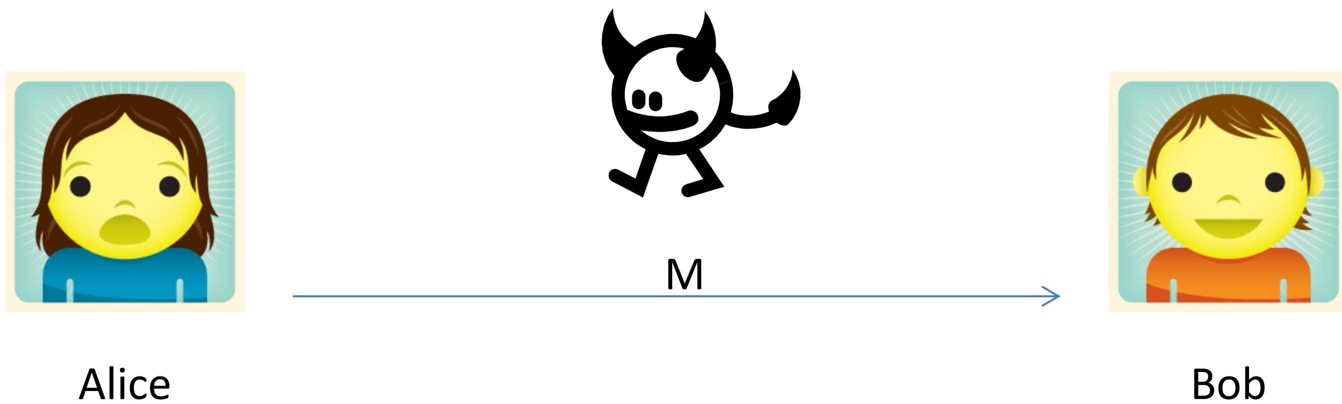
Goals of Modern Cryptography

Providing information security:

- Data Privacy
- Data Integrity and Authenticity

in various computational settings.

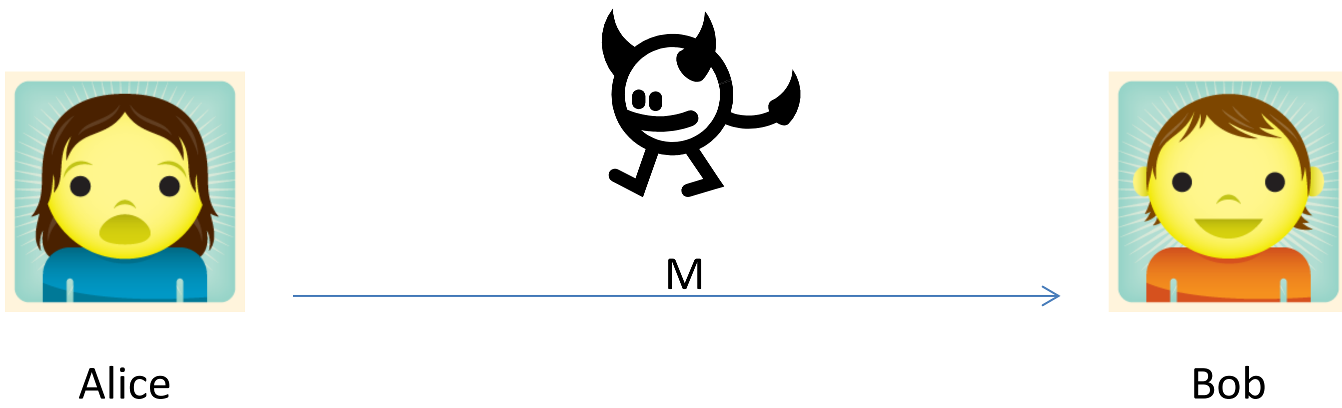
Data Privacy



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.

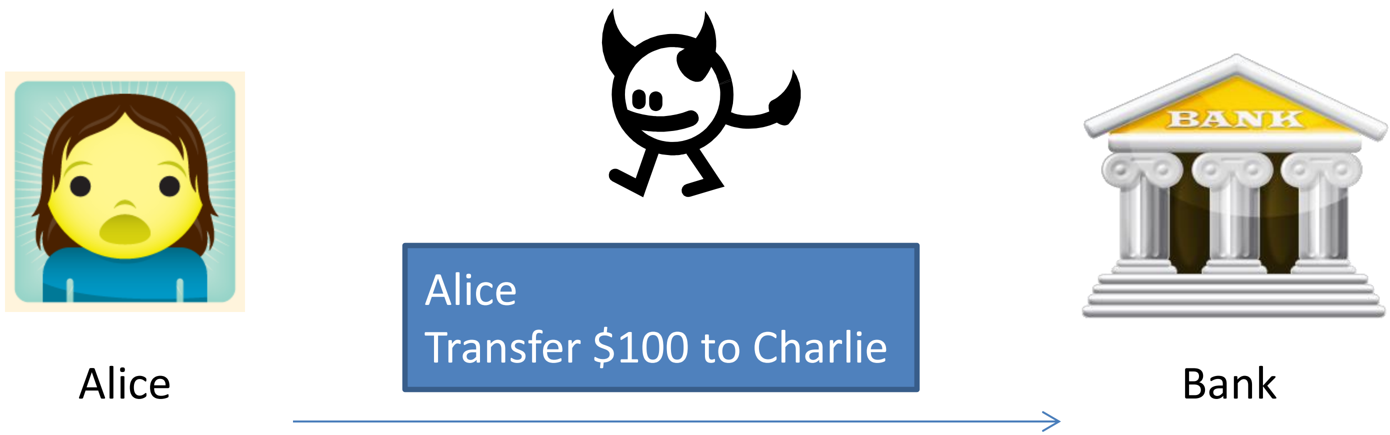
Data Integrity and Authenticity



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.

Medical Databases

Doctor

Reads F_A
Modifies F_A to F'_A

Get: Alice $\longrightarrow$

F_A $\longleftarrow$

Put: Alice, F'_A $\longrightarrow$

Database

Alice	F_A
Bob	F_B

Alice	F'_A
Bob	F_B

Privacy: F_A, F'_A contain confidential information and we want to ensure the adversary does not obtain them

Integrity and authenticity: Need to ensure

- doctor is authorized to get Alice's file
- F_A, F'_A are not modified in transit
- F_A is really sent by database
- F'_A is really sent by (authorized) doctor

Goals of this course

- 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 block-cipher constructions
  - Tools from number theory
- See lots of constructions of cryptographic schemes:
  - Symmetric key encryption, Message Authentication Codes (MAC), Collision-resistant hash functions, Key exchange, Public key encryption, Digital signatures.

Today and next few lectures:

- We will start by looking at Data Privacy in the most basic setting: Message transfer.
- This is also called Encryption.

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.

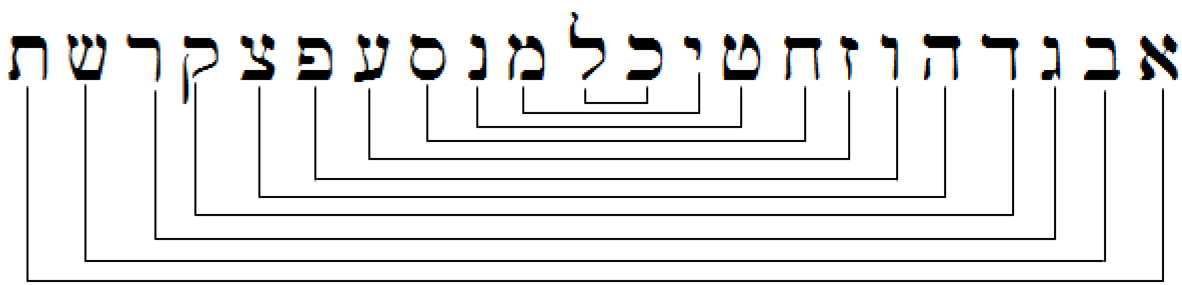
Historical Ciphers and their Cryptanalysis

For each cipher we discuss:

- What is the Encrypt algorithm?
- What is the Decrypt algorithm?
- What is the 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, לב קמי *Lev Kamai* (51:1) is Atbash for כשדים *Kasdim* (Chaldeans), and ששך *Sheshakh* (25:26; 51:41) is Atbash for בבל *Bavel* (Babylon).

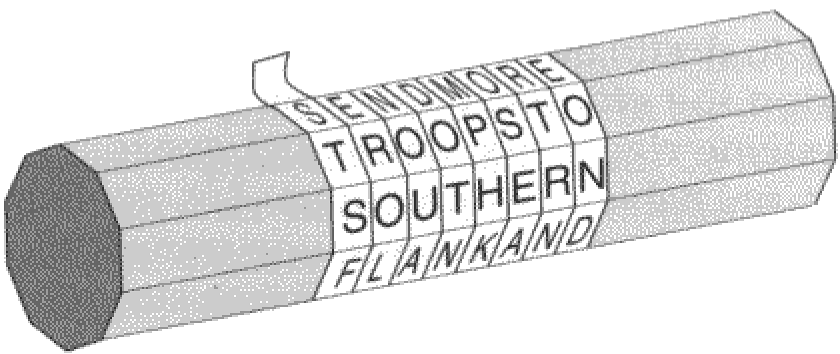


A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

helloworld → SVOOLDLIOW

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.

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?

Monoalphabetic Substitution (800 A.D.)

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

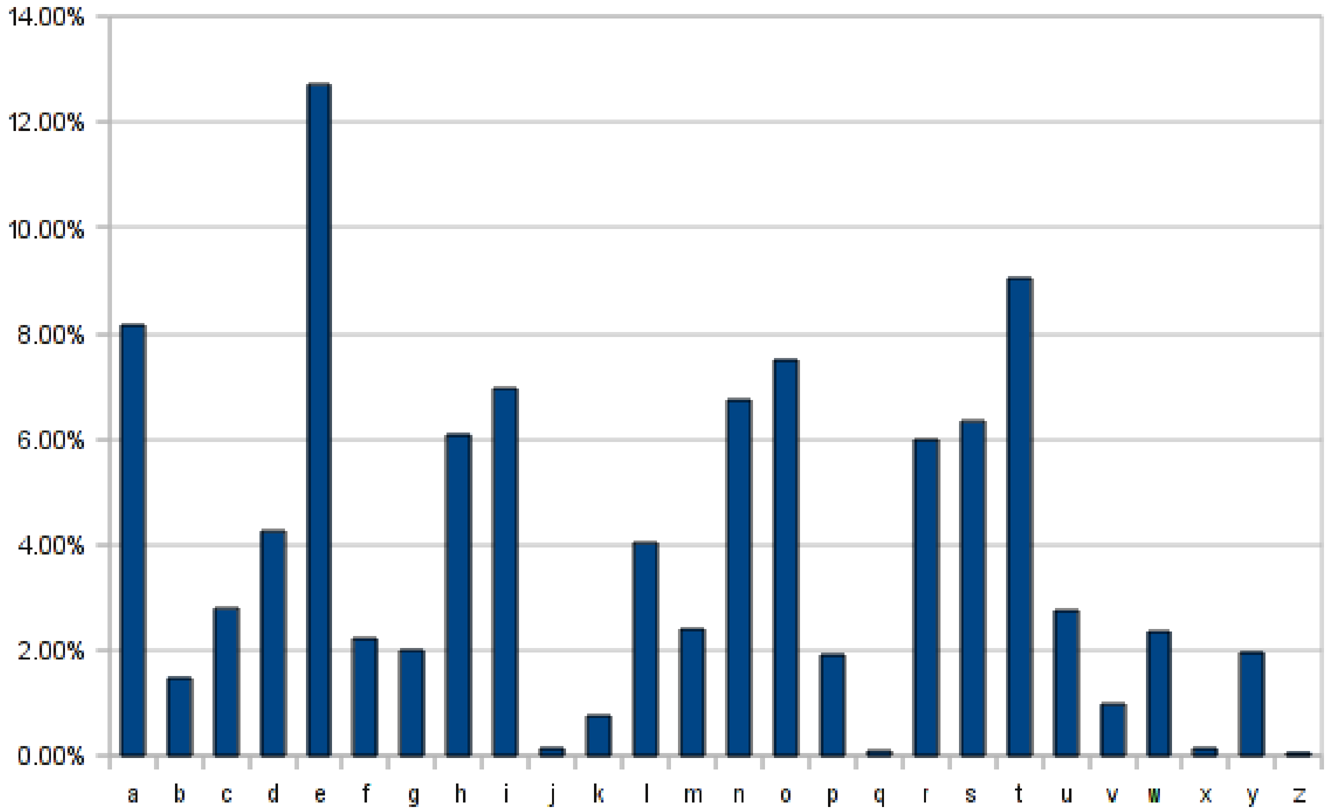
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	E	U	A	D	N	B	K	V	M	R	O	C	Q	F	S	Y	H	W	G	L	Z	I	J	P	T

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:



An Improved Attack on Shift/Caesar Cipher using Frequency Analysis

- Associate letters of English alphabet with numbers $0 \ldots 25$
- Let p_i denote the probability of the i-th letter in English text.
- Using the frequency table:

$$\sum_{i=0}^{25} {p_i}^2 \approx 0.065$$

- Let q_i denote the probability of the i-th letter in this ciphertext: # of occurrences/length of ciphertext
- Compute $I_j = \sum_{i=0}^{25} p_i \cdot q_{i+j}$ for each possible shift value j
- Output the value k for which I_k is closest to 0.065.