Cryptography
ENEE/CMSC/MATH 456

Instructor: Dana Dachman-Soled

Lecture 1

1/24/2024

Syllabus Highlights

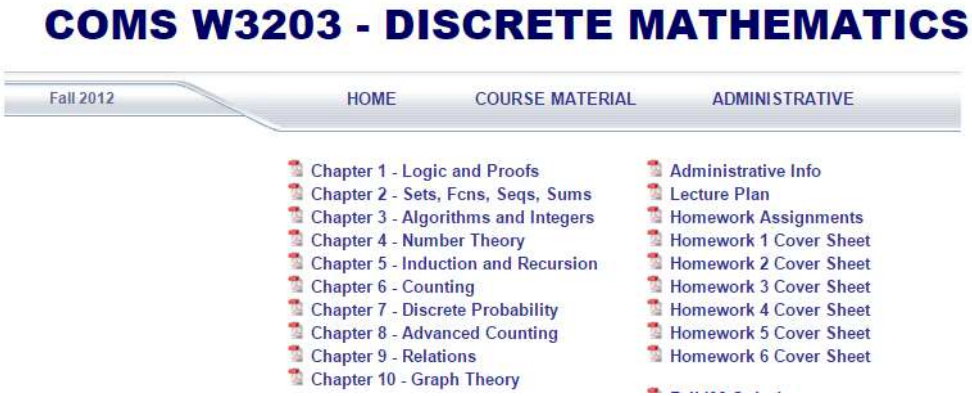
- Best way to contact me is via email:
  - danadach@umd.edu
- My office hours: Wed 9:30-10:30am in Iribe 5238
- Our TA:
  - Russel Chiu (email: rchiu@umd.edu)
- TA Office hours: M/W 11am-noon in Iribe 5161
- Class url:
  - www.ece.umd.edu/~danadach/Cryptography_24

Syllabus Highlights cont'd

- In Class and Online Quizzes
  - More on next slide
- Bi-weekly homeworks (about 5-6 overall)
  - See syllabus for late homeworks policy
  - Lowest grade will be dropped
- Grading Policy:
  - In-Class and Online Quizzes—25%
  - Homework—25%
  - Midterm—25%
  - Final—25% (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.
- ***Due on Jan 31, 11:59pm.
- Additional resources: Rosen, K. H. (2012)Discrete Mathematics and Its Applications. (7th ed.).

Additional Announcements

- In-Class quiz every lecture starting from Lecture 3

  - 10 min at end of class
  - Needed information will be provided on the quiz sheet

- Homework due dates on Canvas are **tentative** and will be updated once the homework is assigned.

  -Encourage students to collaborate on homework

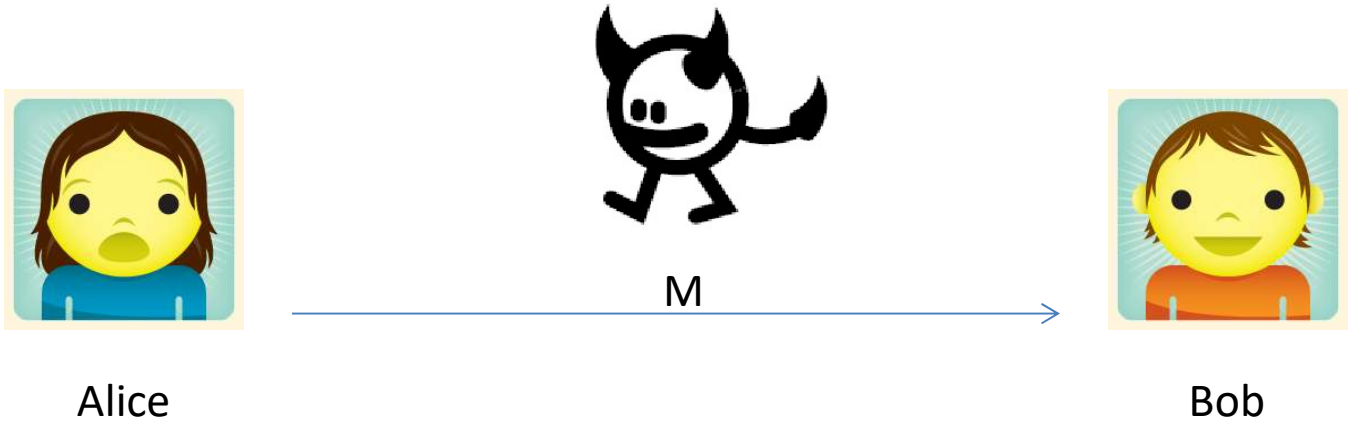
  - Final submitted solutions must be *your own*.

Goals of Modern Cryptography

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

  in various computational settings.

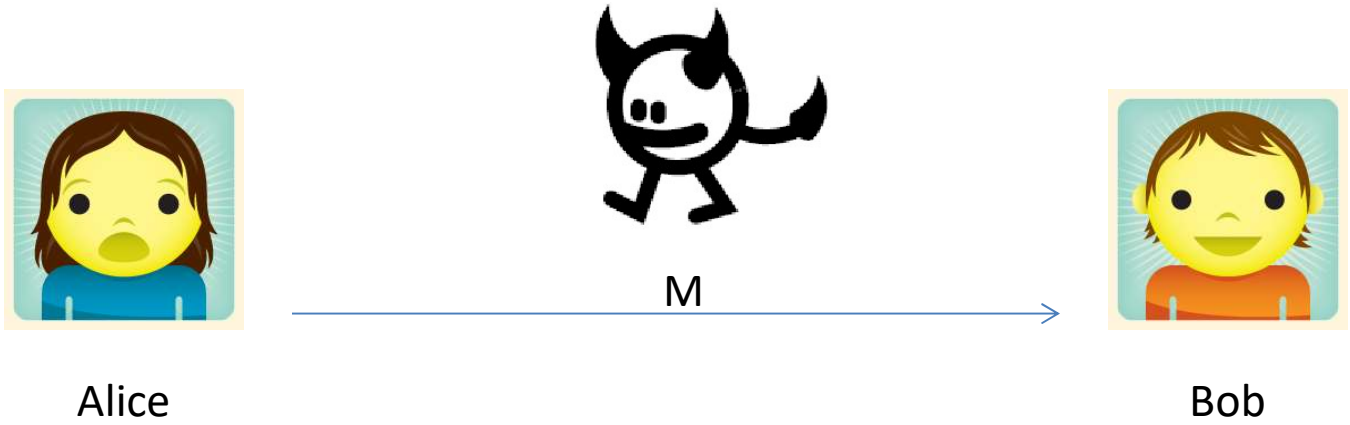
Data Privacy



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.

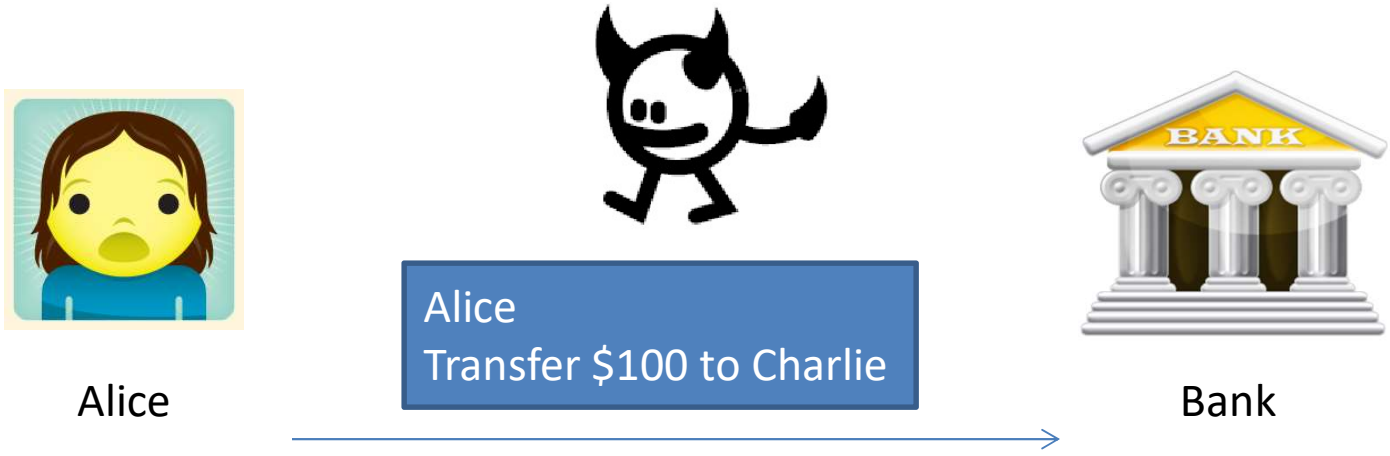
Data Integrity and Authenticity



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”

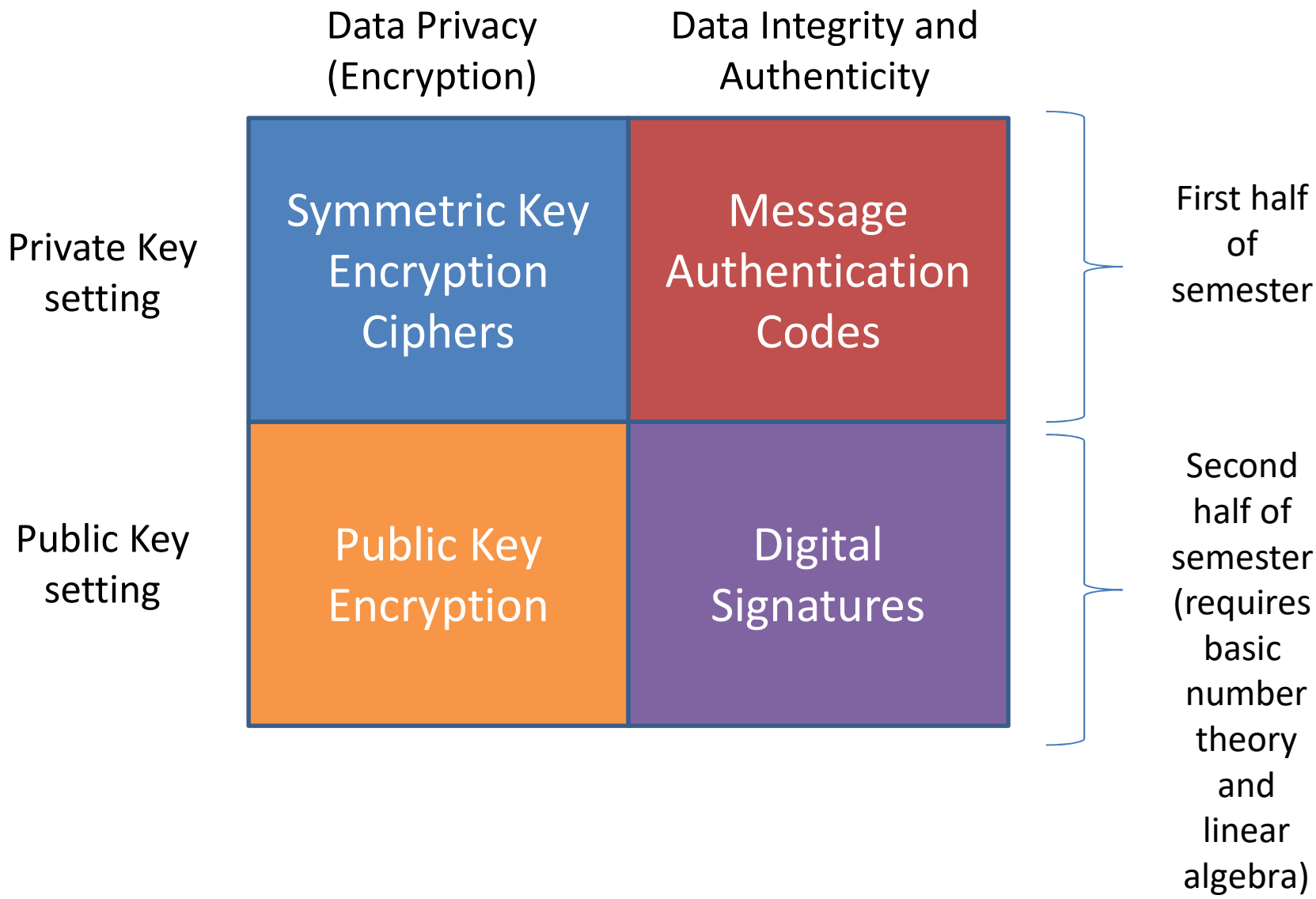
Integrity prevents such attacks.

What this Course is All About

- Has: A lot of mathematical formalism, mathematical proofs, **probability theory**, combinatorics, analysis of algorithms, number theory, linear algebra

- Does not have: Almost no programming, no implementation, not a history or popular culture course.

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?

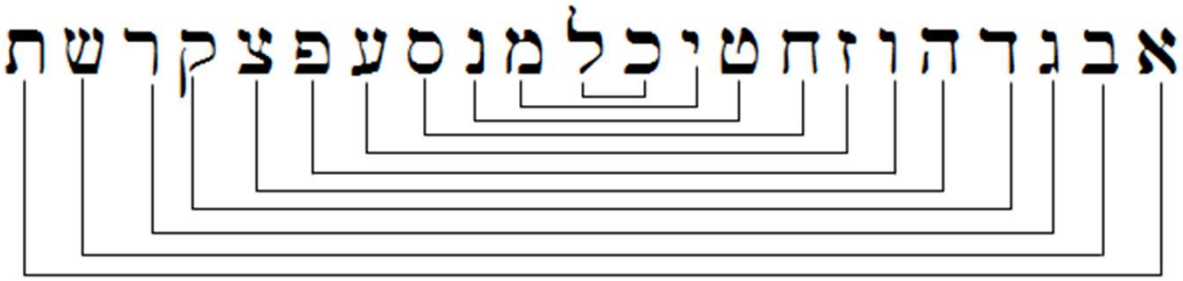
Atbash Cipher (600 B.C.)

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.

Does not follow Kerckhoff

Key Space : ϕ

Size : 0



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.

Key Space: $\{0, \ldots, 25\}$

Size: 26

How to break: Brute Force Search

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.

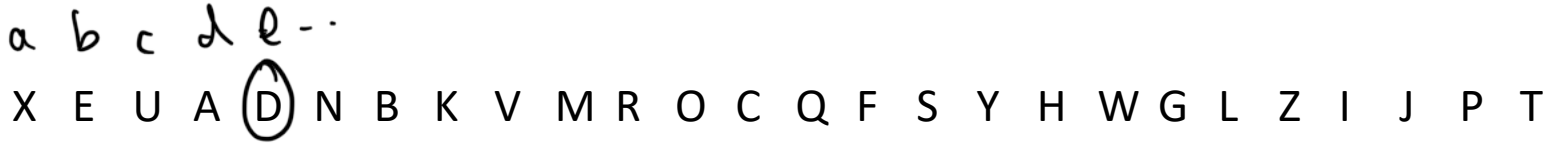
Key Space: All possible diameters

Size: quite huge

Another Alg: try reading out every k^{th} letter for $1 \le k \le$ msg length.

Monoalphabetic Substitution (800 A.D.)

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



tellhimaboutme → **GDOOKVCXEFLGCD**

- Size of key space?

Key Space: all permutations

from

$[0 \ldots 25] \rightarrow [0 \ldots 25]$

Monoalphabetic Substitution (800 A.D.)

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

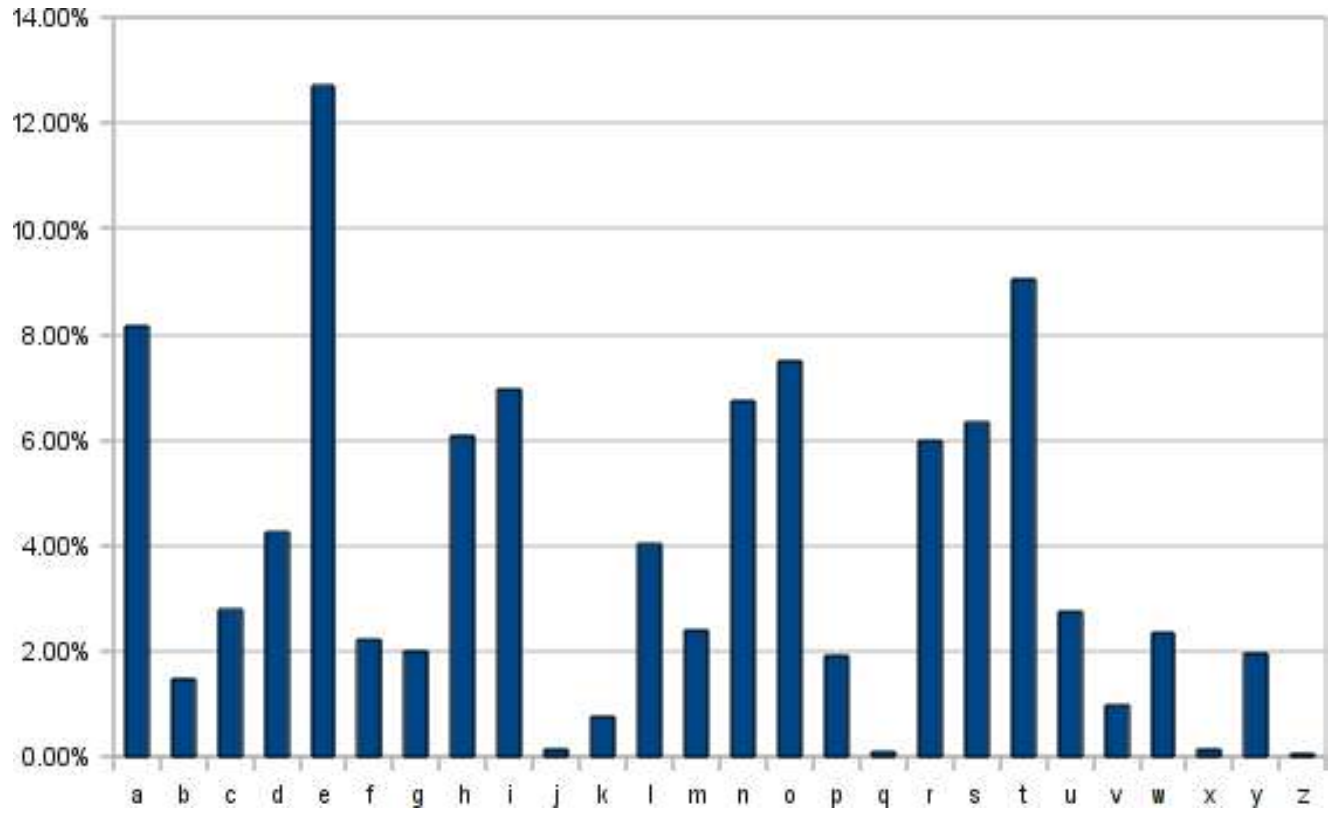
X E U A D N B K V M R O C Q F S Y H W G L Z I J P T

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 $0\ldots25$
- 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.

Vigenere Cipher (1500 A.D.)

- Poly-alphabetic shift cipher: Maps the same plaintext character to different ciphertext characters.
- Vigenere Cipher applies multiple shift ciphers in sequence.
- Example:

Plaintext:	t	e	l	l	h	i	m	a	b	o	u	t	m	e
Key:	c	a	f	e	c	a	f	e	c	a	f	e	c	a
Ciphertext:	V	E	Q	P	J	I	R	E	D	O	Z	X	O	E

Breaking the Vigenere cipher

- Assume length of key t is known.
- Ciphertext $C = c_1, c_2, c_3, \ldots$
- Consider sequences
  - $c_1, c_{1+t}, c_{1+2t}, \ldots$
  - $c_2, c_{2+t}, c_{2+2t}, \ldots$
  - . .
- For each one, run the analysis from before to determine the shift k_j for each sequence j.

Kasiski's Method

- How to determine the key length?
- Look for repeated patterns of length 3 in the ciphertext
- These likely correspond to the word "the" appearing multiple times in the same relative position.
- The distances between the occurrences of the 3-letter pattern will be multiples of the key length.
- Taking the greatest common divisor of the distances yields the key length.