Ma/CS 6a

Class 1

By Adam Sheffer

Course Details

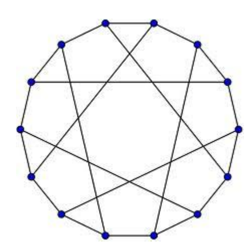
- Adam Sheffer.
- adamsh@caltech.edu
- 1:00 Monday, Wednesday, and Friday.
- http://www.math.caltech.edu/~2014-15/1term/ma006a/

Course Structure

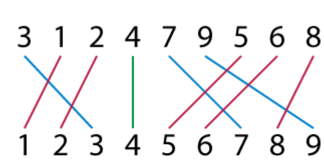
- No exam!
- Grade based on weekly homework assignments.
  - Due by noon on Thursdays.
- TAs: Victor Kasatkin and Henry Macdonald.
- Book: Discrete Mathematics, 2nd edition, by Norman Biggs.

What is in this Course?

- Combinatorics.
- Algorithms.
- Graph theory.
- Number theory.
- Group theory.
- Generating functions.
- …

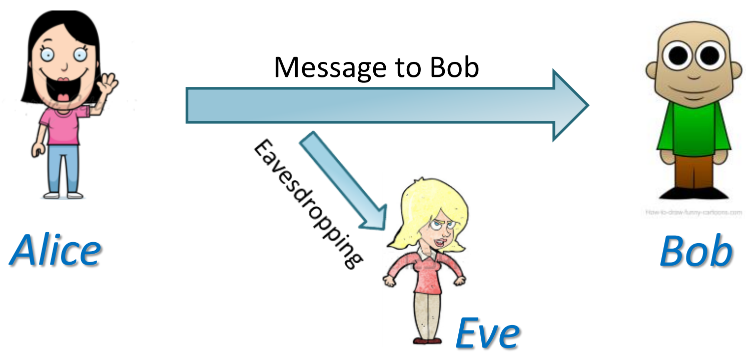


$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$



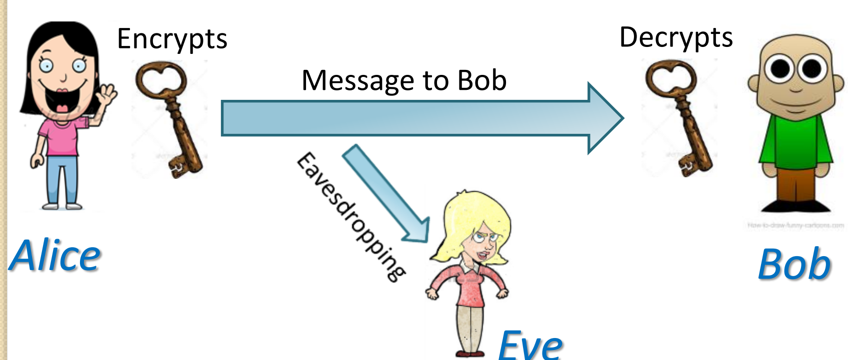
Our Problem: Encryption

- Alice needs to send bob a message.
- Eve can read the communications.
- Alice *encrypts* the message.



Classic Cryptography

- Alice and Bob exchange some information in advance, in a secure way.



Example: Atbash Cipher

- Replace each letter with a symbol, according to the sequence (*key*):

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

"My hovercraft is full of eels"

"Nb slevixizug rh ufoo lu vvoh"

Other Historical Ciphers

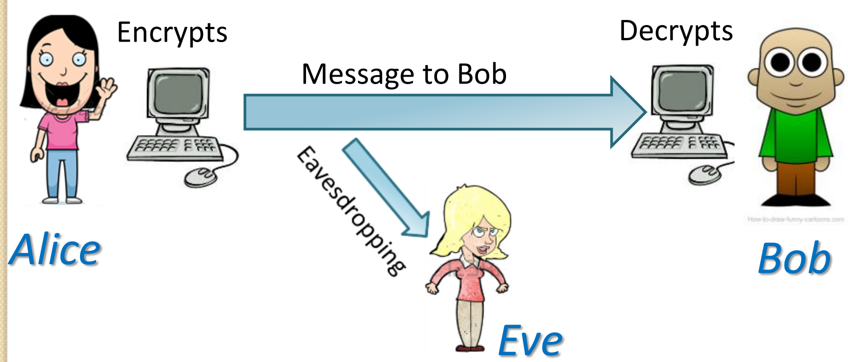
- Scytale transposition cipher, used by the Spartan military.

- The Enigma machine in World War II.

- Cipher runes.

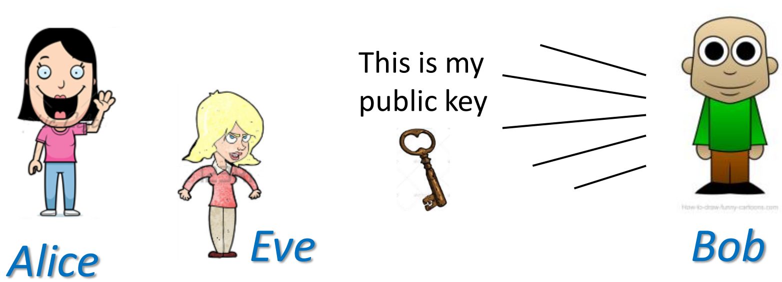
The Internet

- **Problem.** When performing a secret transaction over the internet, we cannot securely exchange information in advance.



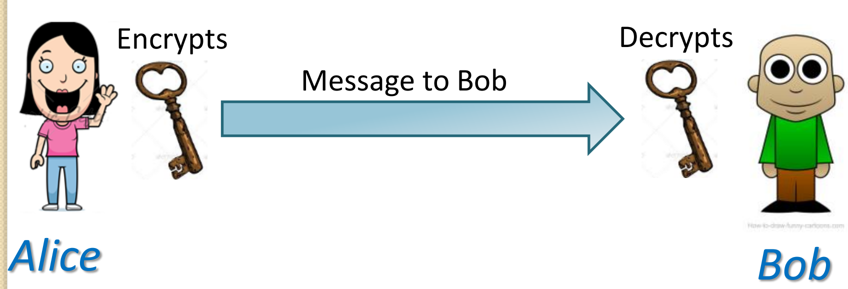
Public-key Cryptography

- **Idea.** Use a *public key* which is used for *encryption* and a *private key* used for *decryption*.
- Bob generates both keys. Keeps the private key and publishes the public one.



Public-key Cryptography

- **Idea.** Use a *public key* which is used for *encryption* and a ***private key*** used for ***decryption***.
- Alice encrypts her message with Bob's public key and sends it.



Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (***decrypt*** using a public key).

Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (*decrypt* using a public key).
- **Bad example.** The public key is the number k. We encrypt a number a as $a \cdot k$. The adversary can divide by k…

Public-key Cryptography

- Eve has the public key and the encrypted message.
- We need an action that is easy to do (*encrypt* using a public key) but very difficult to reverse (*decrypt* using a public key).

Prime factorization

Integers

- We consider the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

- The expression "$a \in \mathbb{Z}$" means that a is *in* the set $\mathbb{Z}$.
- For example, we have

$$1 \in \mathbb{Z}, \qquad 10^2 \in \mathbb{Z}.$$

- On the other hand

$$0.3 \notin \mathbb{Z}, \qquad \sqrt{2} \notin \mathbb{Z}.$$

Division

- Given two integers $a, b \in \mathbb{Z}$, we say that a divides b (or $a|b$) if there exists $s \in \mathbb{Z}$ such that $b = sa$.
- True or false:

$3|12$ ✓ $\qquad$ $12|3$ ✗

$3|-15$ ✓ $\qquad$ $-3|3$ ✓

$-7|0$ ✓ $\qquad$ $0|-7$ ✗

$0|0$ ✓

Our First Proof

- **Claim.** If $a|b$ an $b|c$ then $a|c$.
- **Proof.**
  - There exists $s \in \mathbb{Z}$ such that $b = as$.
  - There exists $t \in \mathbb{Z}$ such that $c = bt$.
  - Therefore, $c = ast$.
  - Setting $r = st$, we have $c = ar$.

Our Second Proof

- **Claim.** If $a|b$ and $b|a$ then $a = \pm b$.
- **Proof.**
  - There exists $s \in \mathbb{Z}$ such that $a = sb$.
  - There exists $t \in \mathbb{Z}$ such that $b = ta$.
  - That is, $a = sta$.
  - $st = 1$ so either $s = t = 1$ or $s = t = -1$.

Prime Numbers

- A *natural number* is an integer that is non-negaive. The set of natural numbers:
$$\mathbb{N} = \{0,1,2,3, \dots\}.$$

- A number of $\mathbb{N} \setminus \{0,1\}$ is said to be *prime* if its only positive divisors are one at itself.

Proof by Induction

- **Claim (Prime decomposition).** Every natural number $n \geq 2$ is either a prime or a product of primes.
- **Proof.**
  - Induction basis: The claim holds for 2.
  - Induction step: Assume that the claim holds for every natural number smaller than n.
  - If n is a prime, the claim holds for n.
  - Otherwise, we can write $n = ab$.
  - By the induction hypothesis, both a and b are either primes or a product of primes.
  - Thus, n is a product of primes.

Proof by Contradiction

- **Claim.** There exist infinitely many prime numbers.
  - **Proof.** Assume, for contradiction, that there exists a finite set of primes
    $$P = \{p_1, p_2, p_3, \dots, p_n\}.$$
  - The number $p_1 p_2 \cdots p_n + 1$ is not prime, since it is not in P.
  - The number $p_1 p_2 \cdots p_n + 1$ is prime, since it cannot be divided by any of the primes of P.
  - *Contradiction! So there must be infinitely many primes!*

More Division Properties

- **Claim.** Given two numbers $a, b \in \mathbb{N}$, there are unique $q, r \in \mathbb{N}$ such that $r < b$ and
  $$a = qb + r.$$
- We say that q and r are the *quotient* and the *remainder* of dividing a with b.
- We write $r = a \bmod b$.
- *Proof by algorithm!*

Our First Algorithm

- **Input.** Two numbers $a, b \in \mathbb{N}$.
- **Output.** Two number $q, r \in \mathbb{N}$ such that $a = qb + r$ and $r < b$.

- $q \leftarrow 0$ and $n \leftarrow a$.
- While $n \geq b$:
  - $n \leftarrow n - b$.
  - $q \leftarrow q + 1$.
- $r \leftarrow n$

$a = 12 \quad b = 5$

$q = 0 \quad n = 12 \quad r = ?$

$q = 1 \quad n = 7 \quad r = ?$

$q = 2 \quad n = 2 \quad r = ?$

$r = 2$

Greatest Common Divisor

- We say that d is a *common divisor* of a and b (where $a, b, d \in \mathbb{N}$) if $d|a$ and $d|b$.
- The *greatest common divisor* of a and b, denoted $\text{GCD}(a, b)$, is a common divisor c of a and b, such that
  - If $d|a$ and $d|b$ then $d \leq c$.
  - Equivalently, if $d|a$ and $d|b$ then $d|c$.

Examples: GCD

- What is $\mathrm{GCD}(18{,}42)$? *6*
- What is $\mathrm{GCD}(50{,}100)$? *50*
- What is $\mathrm{GCD}(6364800, 1491534000)$?
  - $\mathrm{GCD}(2^7 \cdot 3^2 \cdot 5^2 \cdot 13 \cdot 17, 2^4 \cdot 3^7 \cdot 5^3 \cdot 11 \cdot 31)$?

$$= 2^4 \cdot 3^2 \cdot 5^2 = 3600.$$

- What can we do when dealing with numbers that are too large to factor?

GCD Property

- **Claim.** If $a = bq + r$ then

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$

- **Example.**

$$66 = 21 \cdot 3 + 3$$

$$\Downarrow$$

$$GCD(66{,}21) = GCD(21{,}3) = 3.$$

Computing GCD: General approach

- **Problem.** Compute $\mathrm{GCD}(a,b)$.
  - Find $q_1, r_1 \in \mathbb{Z}$ such that $a = q_1 b + r_1$.
  - Since $\mathrm{GCD}(a,b) = \mathrm{GCD}(b, r_1)$, it suffices to compute the latter.
  - Find $q_2, r_2 \in \mathbb{Z}$ such that $b = q_2 r_1 + r_2$.
  - Since $\mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2)$, it suffices to compute the latter.
  - …
  - Continue until obtaining a zero remainder (then the divider is the required GCD).

The Euclidean Algorithm

- **Input.** Two numbers $a, b \in \mathbb{N}$.
- **Output.** $\mathrm{GCD}(a,b)$.

- $r \leftarrow a \bmod b$.
- While $r \neq 0$:
  - $a \leftarrow b$.
  - $b \leftarrow r$.
  - $r \leftarrow a \bmod b$.
- Output b.

$a = 78 \quad b = 45$

$$
\begin{array}{lll}
a = 78 & b = 45 & r = 33 \\
a = 45 & b = 33 & r = 12 \\
a = 33 & b = 12 & r = 9 \\
a = 12 & b = 9 & r = 3 \\
a = 9 & b = 3 & r = 0
\end{array}
$$

Proof of GCD Property

- **Claim.** If $a = bq + r$ then

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$

- **Proof.**
  - Since $r = a - bq$, every common divisor of a and b is also a divisor of r. Thus,
    $$\mathrm{GCD}(a, b) | \mathrm{GCD}(b, r)$$
  - Since $a = bq + r$, every common divisor of b and r is also a common divisor of a. Thus,
    $$\mathrm{GCD}(b, r) | \mathrm{GCD}(a, b).$$

The End

- The Voynich manuscript: