Cryptography

Discrete Mathematics

Courtesy of Andrei Bulatov

Previous lecture

- *Modular arithmetic and inverses*
- *Applications*
- *Systems of linear congruences*
- *The Chinese Remainder Theorem*
  - *The system of linear congruences*

    $x \equiv a_i \pmod{m_i}$

    where each m_i, m_j *are relatively prime has a unique solution*

    $x \equiv a_1M_1M_1^{-1} + \ldots + a_kM_kM_k^{-1} \pmod{m}$

Sun Tzu's Puzzle

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Diophantine equations

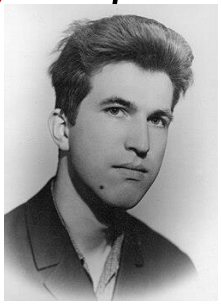
- *Systems of linear congruences are examples of a larger class of equations of massive importance in mathematics: Diophantine equations*
- *Diophantine equations are equations of the form*

  $$ax^n + by^m + cz^p + \ldots = d$$

  where x, y, z, … are unknown integers to be solved for
- *Linear congruences are Diophantine equations of the form*

  $$x = y + mz$$
- *Hilbert's tenth problem*

  Devise an algorithm which can solve any Diophantine equation
- *Hilbert's tenth problem was closed in 1970 by Yuri Matiyasevich, who showed no such algorithm can exist*

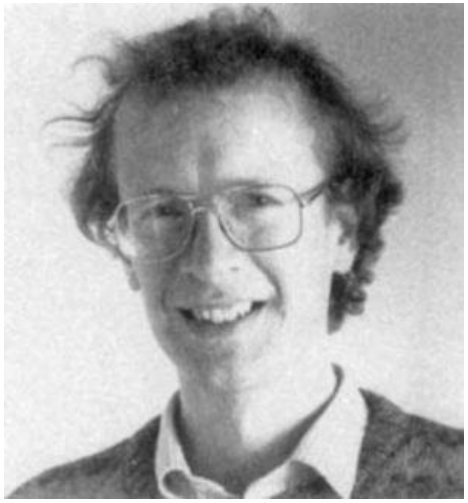


Fermat's Theorem

- **Fermat's Great (Last) Theorem**.
  For any $n > 2$, the equation $x^n + y^n = z^n$ does **not** *have integer solutions $x, y, z > 0$*

- *It had remained unproven for 358 years (posed in 1637, proved in 1995)*

- *Andrew Wiles proved it in 1995 with a 100 page proof using group theory, Galois theory, and tools from algebraic geometry*



Fermat's Little Theorem

- **Fermat's Little Theorem.**

  If p is prime and a is an integer not divisible by p, then

  $$a^{p-1} \equiv 1 \pmod{p}$$

- *Clearly, it suffices to consider only residues modulo p.*

$\mathbb{Z}_5$

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Fermat's Little Theorem (cntd)

- *Recall the definition of Euler's totient function:*

  φ(m) = # of integers up to m which are relatively prime to m

- *Euler's theorem (Improves Fermat's little theorem)*

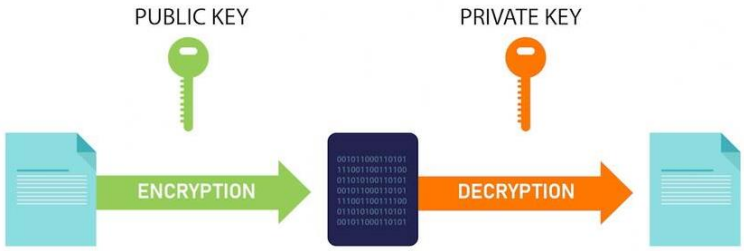
  For any relatively prime integers m and a,

  $$a^{\varphi(m)} \equiv 1 \pmod{m}$$

- *Example:* $\mathbb{Z}_8$

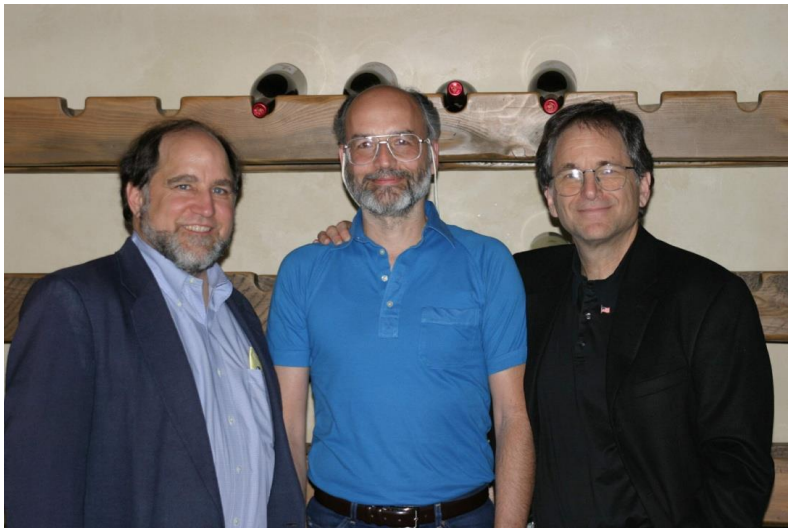
Public Key Cryptography

- *The internet is built on cryptography --- private data (like banking) is encrypted so that an eavesdropper can't read it*
- *The Caesar cipher from last class is an example of encryption*
- *In it, a key is used to both encrypt and decrypt*
- *If the same key is used to encrypt and decrypt, anyone who can send you messages can also read your messages!*
- *Public key cryptosystems solve this problem by using different keys for encryption and decryption:*
  - *a public encryption key, and a private decryption key*



RSA Cryptosystem

- *The most famous and widespread pubkey system is RSA*
- *RSA stands for the names of the inventors: Rivest, Shamir, Adleman*



From left to right:
Ron Rivest
Adi Shamir
Len Adleman

- *RSA is defined by*
  - *a number $n = pq$, where p and q are large primes (e.g. 512 digits), and*
  - *a number e relatively prime with $\varphi(n) = (p - 1)(q - 1)$*
- *n and e are the public encryption keys, while p and q are private*

RSA Encryption

- *Let M be the plaintext message, written as a number*
- *The encryption ciphertext is the residue*

$$C \equiv M^e \pmod{n}$$

- *Example.*
  - *Let $p = 43$, $q = 59$, so $n = 43 \cdot 59 = 2537$*
  - *Choose $e = 13$ which is relative prime with $\varphi(n) = 42 \cdot 58 = 2436$*
  - *Encrypt the message STOP with the public key n, e*
- *Solution.*

  Step 1: Translate the letters of STOP into numbers in in groups of 2: 1819 1415

  Step 2: Encrypt each group of 4 by: $C \equiv M^{13} \pmod{2537}$

  $1819^{13} \equiv 2081 \pmod{2537}$

  $1415^{13} \equiv 2182 \pmod{2537}$

  Step 3: Send the ciphertext 2081 2182

RSA Decryption

- *Let d by the inverse of e modulo $\varphi(n)$*
  - *Note: d exists because e is relatively prime with $\varphi(n) = (p-1)(q-1)$*
- *Claim: if $C \equiv M^e \pmod n$, then $C^d \equiv M \pmod n$*
- *Proof:*

  Since $de \equiv 1 \pmod{\varphi(n)}$, $de = 1 + k\,\varphi(n)$

  Now $C^d \equiv (M^e)^d \equiv M^{de} \equiv M^{1 + k\,\varphi(n)} \pmod n$

  By Fermat's little theorem,

  $$M^{k\,\varphi(n)} = (M^{\varphi(n)})^k \equiv 1^k \equiv 1 \pmod n$$

  So $C^d \equiv M \cdot M^{k\,\varphi(n)} \equiv M \pmod n$

Example

- *Let p = 43, q = 59, e = 13 as before*
- *We want to decrypt the message 0981 0461*
- *Solution:*

  Step 1: compute d = 937 as the inverse of 13 modulo 2436

  Step 2: decrypt each block as $M \equiv C^{937} \pmod{2436}$

  $0981^{937} \equiv 0704 \pmod{2537}$

  $0461^{937} \equiv 1115 \pmod{2537}$

  Step 3: Convert back to letters:

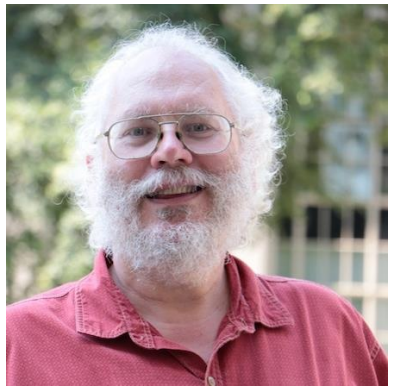
  07 04 11 15

  H E L P

Why RSA Works

- *RSA is predicated on factoring large numbers being HARD*
- *Specifically, we can decrypt RSA knowing just the inverse of e modulo $\varphi(n)$, but computing $\varphi(n)$ requires knowing the prime factorization of n*
- *Best current (classical) algorithm for computing factorizations:*
  Number field sieve, running time O(exp($\sqrt[3]{m}$))
  where m is the length of n
- *For m=400, this is billions of years*
- *RSA Challenge: Factor a published number n=pq, get a prize*
- *The current record is RSA-250. Next one is RSA-260:*
  22112825529529666435281085255026230927612089502470015394413748319128822941402001986512729726569746599085900330031400051170742204560859276357953757185954298838958709229238491006703034124620545784566413664540684214361293017694020846391065875914794251435144458199

Quantum computing



- *With quantum computers, the situation changes drastically*
- *In 1994, Peter Shor proved that a computer operating on the principles of quantum (rather than classical) mechanics can efficiently (i.e. quickly) factor larger integers*
- *The quantum computers in existence today can NOT factor RSA-2048 yet...*
  - *… But maybe in 10 years time?*
- *Many current public key cryptosystems are also now broken (in theory) by quantum computers*
- *Post-quantum cryptography develops quantum-safe cryptography so that secrets today will not be public tomorrow!*

Practice

Exercises from the Book:

7th edition: 17, 20, 31, 33, 35 (page 284 – 285)

8th edition: 17, 20, 31, 33, 35 (page 301)