Ma/CS 6a

Class 3: The RSA Algorithm

By Adam Sheffer

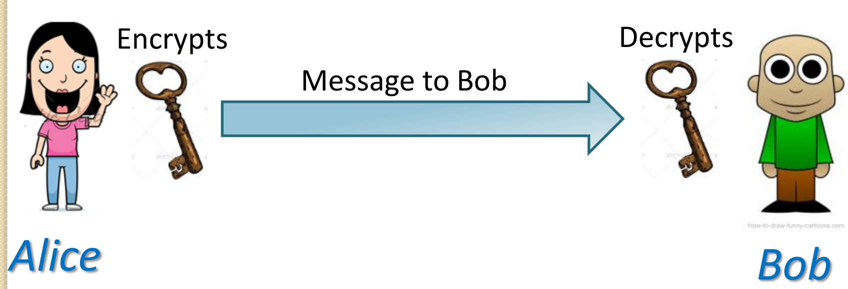
Reminder: Putnam Competition

- Signup ends Wednesday 10/08.
- Signup sheets available in all Sloan classrooms, Math office, or contact Kathy Carreon, *kcarreon@caltech.edu*.
- Math 17 is the Caltech Prep workshop. Liubomir Chiriac Instructor.

http://math.scu.edu/putnam/prizecJan.html

Reminder: 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.



Reminder #2: Congruences

- If $r = a \; mod \; m$ and $r = b \; mod \; m$, we say that "a is ***congruent*** to b modulo m", and write

$$a \equiv b \; mod \; m.$$

  - Equivalently, $m | (a - b)$.
- The numbers $3, 10, 17, 73, 1053$ are all congruent modulo 7.

Reminder: Some Congruent Properties

- **Addition.** If $a \equiv b \; mod \; m$ and $c \equiv d \; mod \; m$, then $a + c \equiv b + d \; mod \; m$.
- **Products.** If $a \equiv b \; mod \; m$ and $c \equiv d \; mod \; m$, then $ac \equiv bd \; mod \; m$.
- **Cancellation.** If $\mathrm{GCD}(k, m) = 1$ and $ak \equiv bk \; mod \; m$, then $a \equiv b \; mod \; m$.
- **Inverse.** If $\mathrm{GCD}(a, m) = 1$, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \; mod \; m$.

Warm-up: Division by Nine

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
- Is 123456789 divisible by 9?

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$
$$4 + 5 = 9$$

✓

Warm-up: Division by Nine (2)

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
  - **Proof.** Write a as $a_k a_{k-1} \cdots a_1 a_0$ where a_i is the $(i+1)$'th rightmost digit of a.

$$a - (a_0 + a_1 + \cdots + a_k) =$$
$$(a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots) - (a_0 + \cdots + a_k)$$
$$= a_1 \cdot 9 + a_2 \cdot 99 + a_3 \cdot 999 + \cdots$$

  - That is, $9 | a - (a_0 + a_1 + \cdots + a_k)$

Warm-up: Division by Nine (3)

- **Claim.** A number $a \in \mathbb{N}$ is divisible by 9 if and only if the sum of its digits is divisible by 9.
  - **Proof.** Write a as $a_k a_{k-1} \cdots a_1 a_0$ where a_i is the $(i-1)$'th rightmost digit of a.
  - We have: $9 | a - (a_0 + a_1 + \cdots + a_k)$.
  - Equivalently,
    $a \equiv (a_0 + a_1 + \cdots + a_k)\ mod\ 9.$

Casting Out Nines

- **Problem.** Is the following correct?
  $54{,}321 \cdot 98{,}765 = 5{,}363{,}013{,}565.$
- If this is correct, then
$54{,}321 \cdot 98{,}765 \equiv 5{,}363{,}013{,}565 \; mod\ 9.$

$$5+4+3+2+1 \equiv 6 \; mod\ 9$$
$$9+8+7+6+5 \equiv 2 \; mod\ 9$$
$$5+3+6+3+0+1+3+5+6+5 \equiv 1 \; mod\ 9.$$

$$6 \cdot 2 \not\equiv 1 \; mod\ 9$$

X

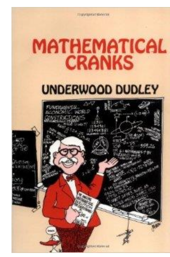
Casting Out Nines (cont.)

- Is the *casting out nines* technique always correct in verifying whether $a \cdot b = c$?
  - If the calculation $mod\ 9$ is wrong, the original calculation must be wrong.
  - If the calculation $mod\ 9$ is correct, the original calculation might still be wrong!

$$1 \cdot 2 \equiv 11 \; mod\ 9.$$

Casting Out Nines Crank

- In the 1980's, a crank wrote a 124-page book explaining ***the law of conservations of numbers*** that he "developed for 24 years".
- This law "was perfected with 100% effectiveness".
- The book is basically 124 pages about the casting out nines trick. It does not mention that the method can sometimes fail.



Fermat's Little Theorem

- **Theorem.** For any prime p and integer a,

$$a^p \equiv a \; mod \; p.$$

- Examples:

$$15^7 \equiv 15 \equiv 1 \; mod \; 7$$

$$20^{53} \equiv 20 \; mod \; 53$$

$$2^{1009} \equiv 2 \; mod \; 1009$$

Pierre de Fermat

Fermat's Little Theorem

- **Theorem.** For any prime p and integer a,

$$a^p \equiv a \bmod p.$$

- **Proof.** By induction on a:
  - We now prove only the case of $a \geq 0$.
  - Induction basis: Obviously holds for $a = 0$.
  - Induction step: Assume that the claim holds for a. In a later lecture we prove
    $$(a+b)^p \equiv a^p + b^p \bmod p.$$
  - Thus:
    $$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p.$$

A Corollary

- **Corollary.** If $a \in \mathbb{N}$ is not divisible by a prime p then $a^{p-1} \equiv 1 \bmod p$.
- **Proof.**
  - We have $\mathrm{GCD}(a, p) = 1$.
  - Fermat's little theorem: $a^p \equiv a \bmod p$.
  - Combine with cancelation property: If $\mathrm{GCD}(k, m) = 1$ and $ak \equiv bk \bmod m$, then $a \equiv b \bmod m$.

Euler's Totient Function

- *Euler's totient $\varphi(n)$* is defined as follows: Given $n \in \mathbb{N} \setminus \{0\}$, then

$$\varphi(n) = |\{x \mid 1 \leq x < n \text{ and } \mathrm{GCD}(x, n) = 1\}|.$$

- In more words: $\varphi(n)$ is the number of natural numbers $1 \leq x \leq n$ such that x and n are relatively prime.

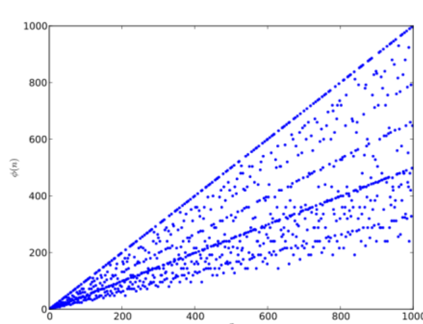
$$\varphi(12) = |\{1,5,7,11\}| = 4$$

Leonhard Euler

The Totient of a Prime

- **Observation.** If p is a prime number, then
$$\varphi(p) = p - 1.$$

The first thousand values of $\varphi(n)$:



Euler's Theorem

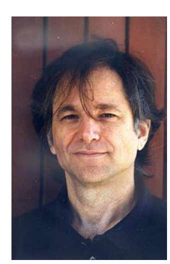
- **Theorem.** For any pair $a, n \in \mathbb{N}$ such that $GCD(a, n) = 1$, we have
$$a^{\varphi(n)} \equiv 1 \; mod \; n.$$
- This is a generalization of the claim $a^{p-1} \equiv 1 \; mod \; p$ (when p is prime).

The RSA Algorithm

- Public key cryptosystem.
- Discovered in 1977 by *R*ivest, *S*hamir, and *A*dleman.
- Still extremely common!

Ron Rivest

Adi Shamir



Leonard Adleman

RSA Public and Private Keys

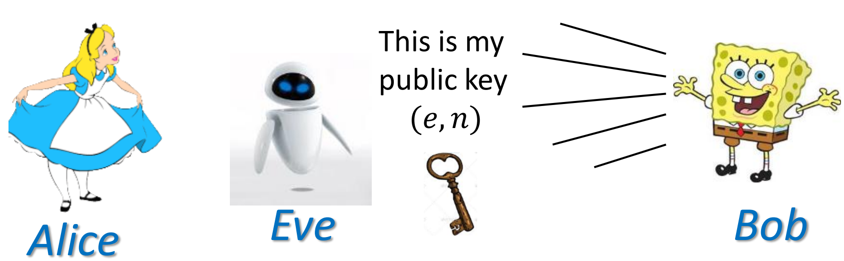
1. Choose two LARGE primes p, q (say, 500 digits).
2. Set $n = pq$.
3. Compute $\varphi(n)$, and choose $1 < e < \varphi(n)$ such that $\mathrm{GCD}\big(e, \varphi(n)\big) = 1$.
4. Find d such that $de \equiv 1 \bmod \varphi(n)$.

Public key. n and e.

Private information. p, q, and d.

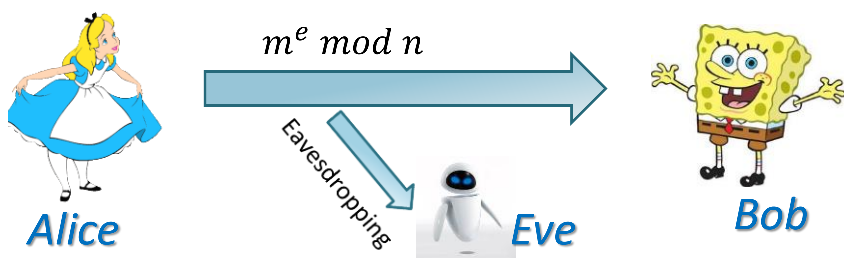
Preparing for Secure Communication

- Bob generates p, q, n, d, e, and transmits only e and n.



Encrypting a Message

- Alice wants to send Bob the number $m < n$ without Eve deciphering it.
- Alice uses n, e to calculate $X = m^e \ mod \ n$, and sends X to Bob.



Decrypting a Message

- Bob receives message $X = m^e \ mod \ n$ from Alice. Then he calculates:

$$X^d \ mod \ n \equiv m^{ed} \ mod \ n$$
$$\equiv m^{1+k\cdot\varphi(n)} mod \ n \equiv m \ mod \ n.$$

$de \equiv 1 \ mod \ \varphi(n)$

Euler's Theorem: $m^{\varphi(n)} \equiv 1 \ mod \ n$

Slightly cheating since the theorem requires $GCD(m, n) = 1$

RSA in One Slide

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q.
    sets $n = pq$ and finds $\varphi(n)$.
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$.
  - Find d such that $de \equiv 1 \ mod\ \varphi(n)$.
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e \ mod\ n$.
- Bob receives X.
  Calculates $X^d \ mod\ n$.

Example: RSA (with small numbers)

- Bob wants to generate keys:
  - Arbitrarily chooses primes $p = 61$ and $q = 53$.
    $n = 61 \cdot 52 = 3233$. $\varphi(3233) = 3120$.
  - Chooses $e = 17$ $(GCD(3120,17) = 1)$.
  - For $de \equiv 1 \ mod\ 3120$, we have $d = 2753$.
- Alice wants to pass bob $m = 65$.
  - Receives n, e from Bob. Returns
    $m^e = 65^{17} \equiv 2790 \ mod\ 3233$.
- Bob receives $X \equiv 2790 \ mod\ 3233$.
  Calculates $X^d = 2790^{3233} \equiv 65 \ mod\ 3233$.

Some Details

- Bob needs to:
  - Find two large primes p, q.
  - Calculate n, d, e.
- Alice needs to
  - Use n, e to calculate $X = m^e \; mod \; n$.
- Eve must not be able to
  - Use n, e, X to find m.
- Bob needs to:
  - Use n, d, X to find m.

That is: Easy to compute a large power $mod \; n$. Hard to compute a large "root" $mod \; n$.

Taking Large Roots

- Eve has n, e, and Alice's message $X \equiv m^e \; mod \; n$.
- If Eve can compute $X^{1/e} \; mod \; n$, she can read the message! (i.e., if she can factor n).
- So far nobody knows how to compute this in a reasonable time.
- Or do they?

Computing a Large Power

- **Problem.** How can we compute

$$65^{2^{4000}}\ mod\ 9721?$$

- A naïve approach:

$$65^2 \equiv 4225\ mod\ 9721$$
$$65^3 \equiv 65 \cdot 65^2 \equiv 2437\ mod\ 9721$$
$$65^4 \equiv 65 \cdot 65^3 \equiv 2869\ mod\ 9721$$
$$\dots$$

- This approach requires 2^{4000} (about $1.3 \cdot 10^{1204}$) steps. *Impossible!*

Computing a Large Power – Fast!

- **Problem.** How can we compute

$$65^{2^{4000}}\ mod\ 9721?$$

$$65^2 \equiv 4225\ mod\ 9721$$
$$65^4 \equiv 65^2 \cdot 65^2 \equiv 2869\ mod\ 9721$$
$$65^8 \equiv 65^4 \cdot 65^4 \equiv 7195\ mod\ 9721$$
$$65^{16} \equiv 65^8 \cdot 65^8 \equiv 3700\ mod\ 9721$$
$$\dots$$

Only 4000 steps. *Easy!*

A Small Technical Issue

- What if we calculate a^b where b is not a power of two?
- We calculate $a, a^2, a^4, a^8, a^{16}, a^{32}, \ldots$
- Every number can be expressed as a sum of distinct powers of 2.

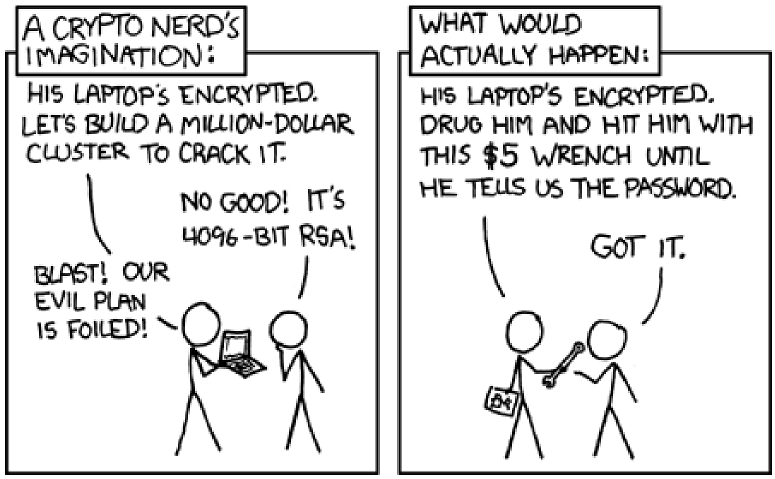
$$57 = 32 + 16 + 8 + 1$$

$$a^{57} = a^{32}a^{16}a^8a$$

What is Left to Do?

- Bob wants to generate keys:
  - Arbitrarily chooses primes p and q.
    $n = pq$ find $\varphi(n)$.
  - Chooses e such that $\mathrm{GCD}(\varphi(n), e) = 1$.
  - Find d such that $de \equiv 1\ mod\ \varphi(n)$.
- Alice wants to pass bob m.
  - Receives n, e from Bob.
  - Returns $X \equiv m^e\ mod\ n$.
- Bob receives X.
  Calculates $X^d\ mod\ n$.

The End


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.