CS/MATH 111, Discrete Structures - Fall 2018.
Discussion 4 - Number Theory and Cryptography

Andres, Sara, Elena

University of California, Riverside

October 18, 2018

Outline

Problem 2

- "Break" RSA by guessing the factorization of n
- Compute Eulers Totient Function

$$\phi(n)$$

- Compute the decryption exponent d by computing

$$e^{-1} \pmod{\phi(n)}$$

  solve this by enumerating.
- Using private key pair (d, n), decrypt the messages by

$$M = C^d \pmod{n}$$

  C stands for the encrypted messages.

Problem 2

- Show computation for 3 letters in Latex: step-by-step, explaining everything;
- For the remaining message:
  Need to write a program (any language) – Attach the program or compute by hand. All the computations attach (It is ok if written in pen).
- Decode the message

Outline

Infinitely many primes, congruent to 3 mod 4

- Assume that

$$p_1 = 3, \cdots, p_k$$

are primes of the form

$$p_j \equiv 3 \pmod{4}$$

- We will construct a new one by looking at

$$N = 4 \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_k) - 1$$

or

$$N = 4 \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 3$$

would also work.

Infinitely many primes, congruent to 3 mod 4

- $N = 4 \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_k) - 1 \equiv 3 \pmod 4$
- Let q be a prime factor of N, s.t. $q \mid N$, then:
  - $q \not\equiv 0 \pmod 4$ [q should not be prime]
  - $q \not\equiv 2 \pmod 4$ [N is odd]
  - $q \not\equiv 3 \pmod 4$ [q should be part of $\{p_1, p_2. \cdots, p_k\}$]
  - $q \equiv 1 \pmod 4$
- Then, $N = q_1 \cdot q_2 \cdot \ldots \cdot q_t$ and $\forall i \in \{1, 2, \cdots, t\} : q \equiv 1 \mod 4$.
- So, $N \equiv 1 \mod 4$, which is a contradiction of our initial definition of N.

Infinitely many primes, congruent to 3 mod 4

- First, none of the primes p_j divides N: note that $p_j|N+1$, so if we had $p_j|N$, then we would have $p_j|(N+1)-N=1$: contradiction.
- Now we observe that at least one of the prime factors of N has the form $p \equiv 3 \mod 4$ (in fact, N is odd).
- Hence if such a prime does not exist, then all prime factors of N have the form $p \equiv 1 \pmod 4$; but then we would have $N \equiv 1 \pmod 4$ contradicting the construction of N.

Outline

Conditions for parameters for RSA

What if ???
$gcd(e, \phi(n)) > 1$

$$d \equiv e^{-1} \pmod{\phi(n)}$$

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

- p and q are small...
- $p = q$
  - $\phi(n) = (p-1)(q-1)$?
  - $\phi(n) = (p-1)(p-1)$???
- Is double inscription correct?
- Is double inscription more secure?

Example

p	q	e	d	correct?	Encrypt $M = 7$ if correct. Justify if not correct.
6	11	5	29		
19	7	5	37		
17	17	9	89		
29	11	7	37		
3	7	5	5		

Example

p	q	e	d	correct?	Encrypt $M = 7$. Justify.
6	11	5	29	No	6 is not prime
19	7	5	37	No	$e \cdot d \not\equiv 1 \pmod{\phi(n)}$
17	17	9	89	No	$p = q$
29	11	7	37	No	$e \cdot d \not\equiv 1 \pmod{\phi(n)}$
3	7	5	5	Yes	$n = 21$ and $C = 7^5 \pmod{21}$

Outline

Miller-Rabin Primality Test

Primality is easy!

- A primality test is a test or algorithm for determining whether an input number is prime.
- N is prime if it has no divisors less or equal to $\sqrt{N}$.
- Prove, that all primes are of the form $6k \pm 1$.
- Most popular algorithms for primality testing are **probabilistic**; may output a composite number as a prime.

Miller-Rabin Primality Test

- Let n be a prime number[1]. Then $n - 1$ is even and we can write it as $2^s \cdot d$
- So we have:

$$n - 1 = 2^s \cdot d$$

  where s and d are positive integers, and d is odd.
- For each a in $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$, either...
  1. $a^d \equiv 1 \pmod{n}$ or
  2. $a^{2^r \cdot d} \equiv -1 \pmod{n}$, For all $0 \leq r \leq s - 1$.
- If we can find a, s.t. (1) and (2) are not true for all r, then n is not prime.

[1] $n > 2$

Example

Is $n = 221$ prime?

- We write $n - 1 = 220 = 2^2 \cdot 55$, so $s = 2$ and $d = 55$.
- We randomly select a number a s.t. $1 < a < n - 1$. Let $a = 174$.
- We proceed to compute:
  - $a^{2^0 \cdot d} \mod n = 174^{55} \mod 221 = 47 \neq 1, -1$
  - $a^{2^1 \cdot d} \mod n = 174^{110} \mod 221 = 220 = -1$
- Since $220 \equiv 1 \mod n$, either 221 is prime, or 174 is a **strong liar** for 221.
- Keep trying...

Example

Is $n = 221$ prime?

- We write $n - 1 = 220 = 2^2 \cdot 55$, so $s = 2$ and $d = 55$.
- We try another random a, this time let $a = 137$:
  - $a^{2^0 \cdot d} \mod n = 137^{55} \mod 221 = 188 \neq 1, -1$
  - $a^{2^1 \cdot d} \mod n = 137^{110} \mod 221 = 205 \neq 1, -1$
- Hence 137 is a **witness** for the compositeness of 221, and 174 was in fact a strong liar.
- Factors of 221 are 13 and 17.