CS/MATH 111, Discrete Structures - Winter 2019. Discussion 4 - Number Theory and Cryptography

Andres, Sara, Elena

University of California, Riverside

January 29, 2019

Outline

Euler's Totient [1]

The totient $\varphi(n)$ of a positive integer $n > 1$ is defined to be the number of positive integers less than n that are coprime to n.

- $\varphi(1)$ is defined to be 1.
- If the prime factorization of n is given by: $n = p_1^{e_1} * \cdots * p_n^{e_n}$, then $\varphi(n) = n * (1 - \frac{1}{p_1}) * \cdots * (1 - \frac{1}{p_n})$.
- For example:
  - $9 = 3^2$, so $\varphi(9) = 9 * (1 - \frac{1}{3}) = 6$
  - $4 = 2^2$, so $\varphi(4) = 4 * (1 - \frac{1}{2}) = 2$
  - $15 = 3 * 5$, so $\varphi(15) = 15 * (1 - \frac{1}{3}) * (1 - \frac{1}{5}) = 15 * \frac{2}{3} * \frac{4}{5} = 8$

[1] For more info have a look at `https://tinyurl.com/kxtcf95`

Euler's Totient [2]

The totient $\varphi(n)$ of a positive integer $n > 1$ is defined to be the number of positive integers less than n that are coprime to n.

- When n is a prime number, then $\varphi(n) = n - 1$.
- When m and n are coprime, then $\varphi(m * n) = \varphi(m) * \varphi(n)$.
- If n is the product of two prime number, p and q, then $\varphi(n) = (p - 1) * (q - 1)$.
- For example: $\varphi(15) = \varphi(3) * \varphi(5) = 2 * 4 = 8$.

[2] For more info have a look at `https://tinyurl.com/y75o4ogh`

Outline

Problem 2

1. "Break" RSA by guessing the factorization of n.
2. Compute Eulers Totient Function $\varphi(n)$.
3. Compute the decryption exponent d by computing

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

   solve this by enumerating.
4. 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 $\pmod 4$

- Assume that $p_i = \{p_1, p_2, \cdots, p_k\}$, where $p_1 = 3$, are primes of the form:

$$p_i \equiv 3 \pmod 4$$

- We will construct a new one[3] by looking at

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

[3] $N = 4 \cdot (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 3$ 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, the prime factorization of N is

$$N = q_1^{e_1} \cdot q_2^{e_2} \cdot \ldots \cdot q_t^{e_t}$$

  and $\forall i \in \{1, 2, \cdots, t\} : q_i \equiv 1 \pmod 4$.
- So, $N \equiv 1 \pmod 4$, [N is prime!!!], which is a contradiction of our initial assumption.

$\blacksquare$

Outline

Conditions for parameters for RSA

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

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

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

- p and q are small...
- $p = q$
  - $\varphi(n) = (p-1)(q-1)$?
  - $\varphi(n) = (p-1)(p-1)$???
- Is double encription correct?
- Is double encription 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	$n = 133$ and $C = 7^5 \pmod{108}$
17	17	9	89	No	$p = q$
29	11	7	37	No	$e \cdot d \not\equiv 1 \pmod{\varphi(n)}$
3	7	5	5	Yes	$n = 21$ and $C = 7^5 \pmod{12}$

Outline

Miller-Rabin Primality Test

Primality is easy! [4]

- 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 $\sqrt{N}$.
- Most popular algorithms for primality testing are **probabilistic**; may output a composite number as a prime.

[4] A nice intro to primality tests at `https://tinyurl.com/m2aksy7`

Miller-Rabin Primality Test[6]

- Let n be a prime number[5]. Then $n-1$ is even and, therefore, not a prime.
- It can be written as:

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

  where s and d are positive integers, and d is odd.
- For each a (a random positive integer), we test two cases...
  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 an a, s.t. (1) and (2) are not true for all r, then n is not prime, it is a **composite** number.
- If either (1) or (2) are true, n can be prime. Testing again will increase that probability...

---

[5] $n > 2$

[6] A great resource at `https://tinyurl.com/yafmmzax`

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:
  - $a^d \pmod{n} = 174^{55} \pmod{221} = 47 \neq 1$
  - $a^{2^1 \cdot d} \pmod{n} = 174^{110} \pmod{221} = 220 \pmod{221} = -1$
- 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 $a = 137$:
  - $a^d \mod n = 137^{55} \mod 221 = 188 \neq 1$
  - $a^{2^1 \cdot d} \mod n = 137^{110} \mod 221 = 205 \neq -1$
- 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.

Reference

- Discrete Mathematics and Its Applications. Rosen, K.H. 2012. McGraw-Hill.
  Chapter 4: Number Theory and Cryptography.