

# **ENEE 457: Computer Systems Security**

## **Lecture 5**

### **Public Key Crypto I: Number Theory Essentials**

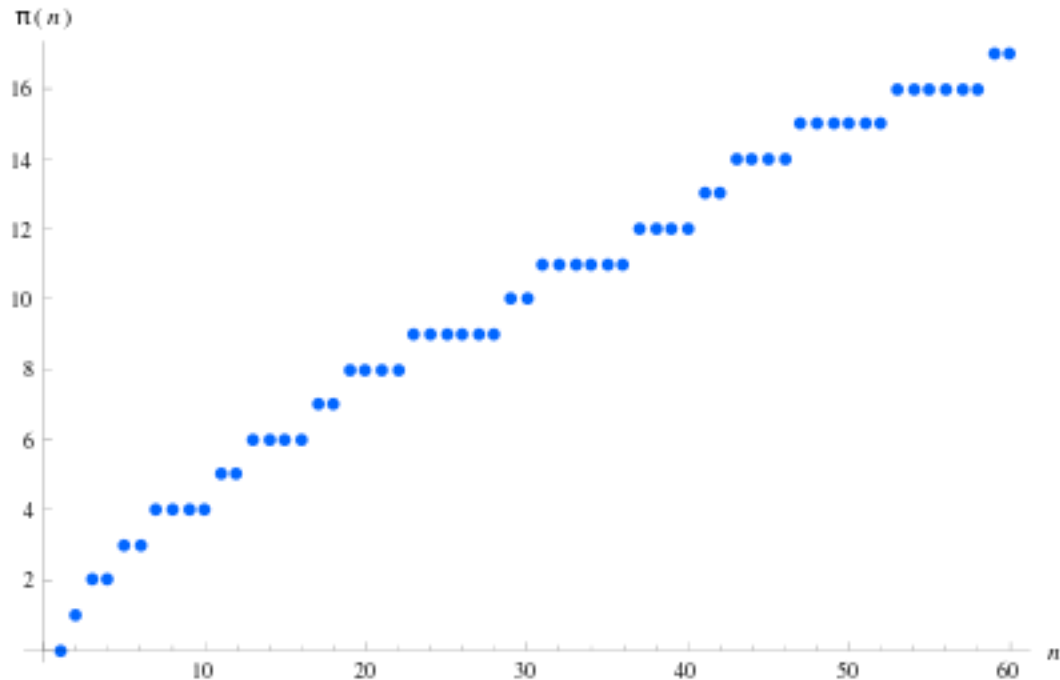
**Charalampos (Babis) Papamanthou**



Department of Electrical and Computer Engineering  
University of Maryland, College Park

# Prime numbers

- A number  $x$  is prime if its only divisors are  $x$  and 1
- There are approximately  $n/\log n$  prime numbers less than  $n$



# Modulo $N$ arithmetic

- We denote with  $x \bmod N$  the remainder of division  $x/N$
- E.g.,  $18 \bmod 4 = 2$ ,  $16 \bmod 2 = 0$
- If  $x \bmod N = y \bmod N$  we write  $x = y \bmod N$
- For example  $4 = 16 \bmod 3$
- You can add, subtract, multiply
- E.g.,  $6 = 18 \bmod 4$  gives (mult. by 4)  $24 = 72 \bmod 4$
- But you cannot divide!

# Beware of division modulo N

- Can you divide?
- $6 = 18 \pmod{4}$
- Try to divide by 2
- $3 = 9 \pmod{4} \rightarrow \text{WRONG!!}$
- What happened?
- **2 DOES NOT HAVE AN INVERSE MOD 4**

# Greatest common divisor (gcd) of a and b

- Definition:  $\text{gcd}(a,b)$  is the greatest integer dividing both a and b
- Property:  $\text{gcd}(a,b)$  is the smallest positive integer d satisfying  $d = i*a + j*b$  for some integers a,b
- Example:  $\text{gcd}(8,20)=4$ .  $4=(1)*20-2*8$
- No positive number smaller than 4 can be derived by taking linear combinations of 8 and 20.

# Proof

- Suppose  $d$  is the smallest positive integer  $d$  satisfying  $d = i*a + j*b$  for some  $i$  and  $j$ . Then we show that  $d = \gcd(a,b)$
- Since  $d = i*a + j*b$ , any common divisor of  $a$  and  $b$  is a divisor of  $d$  as well. But a number is always greater or equal than its divisors, so  $d \geq \gcd(a,b)$
- It is  $a = h*d + (a \bmod d)$  so  $a \bmod d = a - hd$
- But  $d = i*a + j*b$
- So  $a \bmod d = a - hd = a - h(i*a + j*b) = (1-hi)a + (-hj)b$
- But  $a \bmod d < d$  and  $d$  is the smallest positive integer such that  $d = i*a + j*b$  so it has to be the case that  $a \bmod d = 0$  which means  $d$  divides  $a$ .
- By a similar argument we get that  $d$  divides  $b$
- Thus  $d$  is a divisor of both  $a$  and  $b$ , so this implies  $d \leq \gcd(a,b)$
- Therefore  $d = \gcd(a,b)$

# Computing the gcd

- Property:
  - $\gcd(a,b) = \gcd(b, a \bmod b)$
- Why?
  - All common divisors of  $a,b$  are common divisors of  $b$  and  $a \bmod b$ :  $a=dx, b=dt, a \bmod b =d L$
  - All common divisors of  $b, a \bmod b$  are common divisors of  $a$  and  $b$ :  $b = fx, a \bmod b=ft, a=f T$
- So  $a$  and  $b$  and  $b$  and  $a \bmod b$  have exactly the same divisors, so gcd should also be the same
- Example
  - $(412,260) \rightarrow (260,152) \rightarrow (152,108) \rightarrow (108,44) \rightarrow (44,20) \rightarrow (20,4) \rightarrow (4,0)$

# How much time do we need to compute the gcd?

- $O(\max(\log a, \log b))$



# Inverses mod N

- An element  $x$  has an inverse mod  $N$  iff  $\gcd(x, N) = 1$
- If  $x$  has an inverse mod  $N$  then there exists  $y$  such that
  - $x * y = 1 \pmod N$  which implies  $x*y = k*N + 1$  which gives  $x*y - k N = 1$ . Therefore 1 needs to be the gcd of  $x$  and  $N$
  - If  $\gcd(x, N) = 1$  then  $i*x + j*N = 1$  then  $i*x = 1 \pmod N$

# Great Common Divisor Algorithm

Algorithm *EuclidGCD*( $a, b$ )

Input integers  $a$  and  $b$

Output  $\text{gcd}(a, b)$

if  $b = 0$

    return  $a$

else

    return *EuclidGCD*( $b, a \bmod b$ )

- Proof: We need to prove that  $\text{GCD}(\mathbf{a}, \mathbf{b}) = \text{GCD}(\mathbf{b}, \mathbf{a} \bmod \mathbf{b})$
- FACTS
  - Every divisor of  $\mathbf{a}$  and  $\mathbf{b}$  is a divisor of  $\mathbf{b}$  and  $(\mathbf{a} \bmod \mathbf{b})$ : This is because  $(\mathbf{a} \bmod \mathbf{b})$  can be written as the sum of  $\mathbf{a}$  and a multiple of  $\mathbf{b}$ , i.e.,  $\mathbf{a} \bmod \mathbf{b} = \mathbf{a} + k\mathbf{b}$ , for some integer  $k$ .
  - Similarly, every divisor of  $\mathbf{b}$  and  $(\mathbf{a} \bmod \mathbf{b})$  is a divisor of  $\mathbf{a}$  and  $\mathbf{b}$ : This is because  $\mathbf{a}$  can be written as the sum of  $(\mathbf{a} \bmod \mathbf{b})$  and a multiple of  $\mathbf{b}$ , i.e.,  $\mathbf{a} = k\mathbf{b} + (\mathbf{a} \bmod \mathbf{b})$ , for some integer  $k$ .
  - Therefore the set of all divisors of  $\mathbf{a}$  and  $\mathbf{b}$  is **the same** with the set of all divisors of  $\mathbf{b}$  and  $(\mathbf{a} \bmod \mathbf{b})$ . Thus the greatest should also be the same.

# Groups in Mathematics

- A group is a set,  $G$ , together with an operation  $\cdot$  (called the group law of  $G$ ) that combines any two elements  $a$  and  $b$  to form another element, denoted  $a \cdot b$  or  $ab$ . To qualify as a group, the set and operation,  $(G, \cdot)$ , must satisfy four requirements known as the group axioms:
- **Closure:** For all  $a, b$  in  $G$ , the result of the operation,  $a \cdot b$ , is also in  $G$ .
- **Associativity:** For all  $a, b$  and  $c$  in  $G$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
- **Identity element:** There exists an element  $e$  in  $G$ , such that for every element  $a$  in  $G$ , the equation  $e \cdot a = a \cdot e$  holds. Such an element is unique, and thus one speaks of the identity element.
- **Inverse element:** For each  $a$  in  $G$ , there exists an element  $b$  in  $G$ , commonly denoted  $a^{-1}$  (or  $-a$ , if the operation is denoted "+"), such that  $a \cdot b = b \cdot a = e$ , where  $e$  is the identity element.
- If commutativity holds, the group is called abelian

# Examples of groups

- The set of integers  $\{\dots, -2, -1, 0, 1, 2\}$  is a group under addition but not under multiplication (why?).
- The set of integers modulo  $N$   $\{0, 1, \dots, N-1\}$  is a group under addition (this group is denoted  $Z_N$ )
- Is the set of reals a group under multiplication?
- The set of integers modulo  $N$  that have multiplicative inverses modulo  $N$  is a group under multiplication. We denote this group as  $Z^*_N$ 
  - $Z^*_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$
  - $Z^*_7 = \{1, 2, 3, 4, 5, 6\}$  (since 7 is a prime)

# Order of a group

- Order of a group is the number of elements in a group.
- Can be infinite
- $\text{ORDER}(\mathbb{Z}_N) = \text{ORDER}(\{0, 1, \dots, N-1\}) = N$
- Let  $(G, +)$  be a group of order  $m$ . Then for every element  $g$  of the group  $g * m = 0$
- Or if  $(G, *)$  is a group of order  $m$ . Then for every element  $g$  of the group  $g^m = 1$
- Take all element  $g_1, g_2, \dots, g_m$ . Fix arbitrary  $g$  from the group. Then we claim
  - $(g_1 * g) * (g_2 * g) * \dots * (g_m * g) = g_1 * g_2 * \dots * g_m$
  - This gives  $g^m = 1$
- $g^x = g^{\{x \bmod m\}}$ 
  - $g^x = g^{\{k * m + (x \bmod m)\}} = (g^m)^k * g^{\{x \bmod m\}} = g^{\{x \bmod m\}}$

# What is the order of $Z^*_N$ ?

- Assume  $N = p * q$  where  $p$  and  $q$  are primes  $> 1$
- Order of  $Z^*_N$  is  $(p - 1) (q - 1)$
- Denoted  $\phi(N)$
- What if  $N$  is itself a prime?
- Then order of  $Z^*_p$  is  $p - 1$

# Can we define a bijection (permutation)?

- Let  $G$  be a group of order  $m$
- If  $\gcd(e, m) = 1$  then  $g^e$  is a bijection
- Suppose not. Then  $x^e = y^e$  for  $x \neq y$  which implies  $x = y$ , contradiction
- So looks like number theory gives us permutations without tables!

# Cyclic groups

- Let  $G$  be a group
- The order of an element  $x$  in the group is the smallest positive integer  $o$  such that
  - $x^o = 1$
- If there exists an element  $g$  in the group that whose order is equal to the order of the group then
  - The group is called cyclic
  - All elements of the group can be generated by  $g$  as  $g^0, g^1, \dots, g^{m-1}$
- Example
  - Consider  $\mathbb{Z}_{15}$ . Order is 15. It is cyclic because for  $g = 1$  we have
    - $g^{15} = 1^{15} = 0$
    - For all other  $i < 15$  it is  $1^i \neq 0 \pmod{15}$
- If the order is prime,  $G$  is cyclic and all the elements (but the identity) can serve as generators
- $\mathbb{Z}_p^*$  is also cyclic. Example,  $\mathbb{Z}_7^*$  is cyclic with 3 but not 2 as a generator



# Computational Assumption 1: DLog

- We will be using some assumptions about problems considered to be hard
- Discrete logarithm problem
- Let  $G$  be a cyclic group of order  $q$  and let  $g$  be a generator of  $G$
- Output an element  $h = g^x$ . Keep  $x$  secret
- Then it is very difficult (exponential in the bitlength of  $q$ ) to figure out  $x$
- **What would be a naïve algorithm for that?**

# Computational Assumption 2: RSA

- Given  $N = pq$ , where  $p$  and  $q$  are primes, it is difficult to figure out  $p$  and  $q$
- This is known as factoring assumption
- We will see an encryption scheme whose security is based on RSA
- We will see a hash function whose security is based on DLog

# Chinese remainder theorem

- Let  $N=pq$ . Let
  - $x \bmod p = a_1$
  - $x \bmod q = a_2$
- Then
  - $x \bmod N = a_1 * q * \text{inverse}(q \text{ in } \mathbb{Z}_p) + a_2 * p * \text{inverse}(p \text{ in } \mathbb{Z}_q) \bmod N$
  - **Let's prove it**
  - This can be used to compute  $W^x \bmod N$ , for big  $W^x$ , more efficiently
  - How?
- Use of theorem
  - Say you want to compute  $18^{25} \bmod 35$  ( $35 = 5*7$ )
  - Compute  $18^{25} \bmod 5 = 18^{(25 \bmod 4)} \bmod 5 = 18^1 \bmod 5 = 3 = a_1$
  - Compute  $18^{25} \bmod 7 = 18^{(25 \bmod 6)} \bmod 7 = 18^1 \bmod 7 = 4 = a_2$
  - Note that  $\text{inverse}(5 \text{ in } \mathbb{Z}_7)=3$  and  $\text{inverse}(7 \text{ in } \mathbb{Z}_5)=3$
  - Therefore the solution we are looking for is  $3*7*3+4*5*3 \bmod 35= 18$
- Used in the decryption procedure of RSA: Why cannot it be used in the encryption?