ENEE 459-C
Computer Security

Public key encryption
(continue from previous lecture)

UNIVERSITY OF MARYLAND

Euclid's GCD Algorithm

- Euclid's algorithm for computing the GCD repeatedly applies the formula

  $\gcd(\boldsymbol{a}, \boldsymbol{b}) = \gcd(\boldsymbol{b}, \boldsymbol{a} \bmod \boldsymbol{b})$

- Example
  - $\gcd(412, 260) = 4$

Algorithm *EuclidGCD*(***a, b***)
  Input integers ***a*** and ***b***
  Output gcd(***a***, ***b***)

  if ***b*** = 0
    return ***a***
  else
    return *EuclidGCD*(***b, a*** mod ***b***)

a	412	260	152	108	44	20	4
b	260	152	108	44	20	4	0

Proof of correctness

Algorithm ***EuclidGCD***(***a*, *b***)
  Input integers ***a*** and ***b***
  Output gcd(***a***, ***b***)

  if ***b*** = 0
    return ***a***
  else
    return ***EuclidGCD***(***b*, *a*** mod ***b***)

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

Multiplicative Inverses (1)

- The residues modulo a positive integer n are the set

  $$Z_n = \{0, 1, 2, \ldots, (n-1)\}$$

- Let x and y be two elements of Z_n such that

  $$xy \bmod n = 1$$

  We say that y is the multiplicative inverse of x in Z_n and we write $y = x^{-1}$

- Example:
  - Multiplicative inverses of the residues modulo 11

x	0	1	2	3	4	5	6	7	8	9	10
x^{-1}		1	6	4	3	9	2	8	7	5	10

Multiplicative Inverses (2)

Theorem

An element x of Z_n has a multiplicative inverse if and only if x and n are relatively prime

- Example
  - The elements of Z_{10} with a multiplicative inverse are $1, 3, 7, 9$

Corollary

If is p is prime, every nonzero residue in Z_p has a multiplicative inverse

Theorem

A variation of Euclid's GCD algorithm computes the multiplicative inverse of an element x of Z_n or determines that it does not exist

x	0	1	2	3	4	5	6	7	8	9
x^{-1}		1		7				3		9

Computing multiplicative inverses

- Compute the multiplicative inverse of a in Z_b
- Given two numbers **a** and **b**, there exist integers x and y such that
  - x**a + y****b = gcd(a,b)**
- Can be computed efficiently with the Extended Euclidean algorithm
- To compute the multiplicative inverse of a in Z_b ,use the Extended Euclidean algorithm to compute x and y such that x**a + y****b = 1**
- Then x the multiplicative inverse of a in Z_b

Extended Euclidean algorithm

Theorem

Given positive integers a and b, let d be the smallest positive integer such that

$$d = ia + jb$$

for some integers i and j.

We have

$$d = \gcd(a,b)$$

- Example
  - $a = 21$
  - $b = 15$
  - $d = 3$
  - $i = 3, j = -4$
  - $3 = 3 \cdot 21 + (-4) \cdot 15 = 63 - 60 = 3$

Algorithm *Extended-Euclid*(a, b)
 Input integers a and b
 Output gcd(a, b), i and j
  such that $ia+jb = gcd(a,b)$
 if $b = 0$
  return (a,1,0)
 (d′, x′, y′) = *Extended-Euclid*(b, a mod b)
 (d, x, y) = (d′, y′, x′ - [a/b]y′)
 return (d, x, y)

Powers

- Let p be a prime
- The sequences of successive powers of the elements of Z_p exhibit repeating subsequences
- The sizes of the repeating subsequences and the number of their repetitions are the divisors of $p - 1$
- Example ($p = 7$)

x	x^2	x^3	x^4	x^5	x^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1