ENEE 459-C
Computer Security

Public key encryption
(continue from previous lecture)

UNIVERSITY OF MARYLAND

Review of Secret Key (Symmetric) Cryptography

- Confidentiality
  - block ciphers with encryption modes
- Integrity
  - Message authentication code (keyed hash functions)
- Limitation: sender and receiver must share the same key
  - Needs secure channel for key distribution
  - Impossible for two parties having no prior relationship
  - Needs many keys for n parties to communicate

Concept of Public Key Encryption

- Each party has a pair (K, K^{-1}) of keys:
  - K is the **public** key, and used for encryption
  - K^{-1} is the **private** key, and used for decryption
  - Satisfies $\mathbf{D}_{K^{-1}}[\mathbf{E}_K[M]] = M$
- Knowing the public-key K, it is computationally infeasible to compute the private key K^{-1}
  - Easy to check K,K^{-1} is a pair
- The public-key K may be made publicly available, e.g., in a publicly available directory
  - Many can encrypt, only one can decrypt
- Public-key systems aka *asymmetric* crypto systems

Public Key Cryptography Early History

- Proposed by Diffie and Hellman, documented in “New Directions in Cryptography” (1976)
  1. Public-key encryption schemes
  2. Key distribution systems
     - Diffie-Hellman key agreement protocol
  3. Digital signature

- Public-key encryption was proposed in 1970 in a classified paper by James Ellis
  - paper made public in 1997 by the British Governmental Communications Headquarters

- Concept of digital signature is still originally due to Diffie & Hellman

Public Key Encryption Algorithms

- Almost all public-key encryption algorithms use either number theory and modular arithmetic, or elliptic curves
- RSA
  - based on the hardness of factoring large numbers
- El Gamal
  - Based on the hardness of solving discrete logarithm
  - Use the same idea as Diffie-Hellman key agreement

Facts About Numbers

- Prime number p:
  - p is an integer
  - $p \geq 2$
  - The only divisors of p are 1 and p
- Examples
  - $2, 7, 19$ are primes
  - $-3, 0, 1, 6$ are not primes
- Prime decomposition of a positive integer n:

$$n = p_1^{e_1} \times \ldots \times p_k^{e_k}$$

- Example:
  - $200 = 2^3 \times 5^2$

Fundamental Theorem of Arithmetic

The prime decomposition of a positive integer is unique

Greatest Common Divisor

- The greatest common divisor (GCD) of two positive integers $\boldsymbol{a}$ and $\boldsymbol{b}$, denoted $\gcd(\boldsymbol{a}, \boldsymbol{b})$, is the largest positive integer that divides both $\boldsymbol{a}$ and $\boldsymbol{b}$
- The above definition is extended to arbitrary integers
- Examples:

  $\gcd(18, 30) = 6$ $\qquad$ $\gcd(0, 20) = 20$

  $\gcd(-21, 49) = 7$
- Two integers a and b are said to be relatively prime if

  $$\gcd(\boldsymbol{a}, \boldsymbol{b}) = 1$$
- Example:
  - Integers 15 and 28 are relatively prime

Modular Arithmetic

- Modulo operator for a positive integer $\boldsymbol{n}$

  $$\boldsymbol{r} = \boldsymbol{a} \bmod \boldsymbol{n}$$

  equivalent to

  $$\boldsymbol{a} = \boldsymbol{r} + \boldsymbol{kn}$$

  and

  $$\boldsymbol{r} = \boldsymbol{a} - \lfloor \boldsymbol{a}/\boldsymbol{n} \rfloor \boldsymbol{n}$$

- Example:

  $$29 \bmod 13 = 3 \qquad 13 \bmod 13 = 0 \qquad -1 \bmod 13 = 12$$

  $$29 = 3 + 2\times 13 \qquad 13 = 0 + 1\times 13 \qquad 12 = -1 + 1\times 13$$

- Modulo and GCD:

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

- Example:

  $$\gcd(21, 12) = 3 \qquad \gcd(12, 21 \bmod 12) = \gcd(12, 9) = 3$$

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