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:

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

$\gcd(-21, 49) = 7$

- 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:

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