Lecture 8

Rivest-Shamir-Adelman (RSA)

CS 450/650

Fundamentals of Integrated Computer Security

- Mid-term review Oct. 15
- Mid-term Oct. 17

Two kinds of Cryptography

Symmetric

1) Alice and Bob agree on a cryptosystem
2) Alice and Bob agree on a key
3) Alice takes her plaintext message and encrypts it using the encryption algorithm and the key. This creates a ciphertext message
4) Alice sends the ciphertext message to Bob
5) Bob decrypts the ciphertext message with the same algorithm and key and reads it

Asymmetric

1) Alice and Bob agree on a public-key cryptosystem
2) Bob sends Alice his public key
3) Alice encrypts her message using Bob's public key and sends it to Bob
4) Bob decrypts Alice's message using his private key

RSA

- **RSA** is one of the first practical public-key cryptosystems and is widely used for secure data transmission.
- The encryption key is public and differs from the decryption key which is kept secret (asymmetric cipher)
- Its security is based on the practical difficulty of doing some mathematical operations
  - RSA: factoring the product of two large prime numbers, the factoring problem

- Fundamentals for RSA

Divisibility

- We say that a nonzero b divides a if a = mb for some m, where a, b, and m are integers
- b divides a if there is no remainder on division
- The notation b|a is commonly used to mean b divides a
- If b | a we say that b is a divisor of a

Properties of Divisibility

- If $a|1$, then $a = \pm 1$
- If $a|b$ and $b|a$, then $a = \pm b$
- Any b != 0 divides 0
- If $a|b$ and $b|c$, then $a|c$
- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary m and n
  - $2|4$ and $2|8$, the $2|(4m+8n)$

Division Algorithm

- Given any positive integer *n* and any nonnegative integer *a*, if we divide *a* by *n* we get an integer quotient *q* and an integer remainder *r* that obey the following relationship:
  - $a = qn + r,\quad where \quad 0 <= r < n;\ q = [a/n]$
  - E.g., a=21, n=10, then a=2*10+1, so q=2 and r=1

Greatest Common Divisor (GCD)

- greatest common divisor (GCD) of two positive integers
  - GCD: the largest number that divides both of them without leaving a remainder
- Two integers are relatively prime if their GCD is 1

Greatest Common Divisor (GCD)

- The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*
- Represented by *gcd*(*a, b*)
- Positive integer *c* is said to be the *gcd* of *a* and *b* if
  – *c* is a divisor of *a* and *b*
  – Any divisor of *a* and *b* is a divisor of *c*
- Example: gcd(6,8), gcd(8,16), gcd(9,10)

GCD Properties

- GCD should be positive
- So $gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$
- example: gcd(8,-6)
- We stated that two integers *a* and *b* are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that *a* and *b* are relatively prime if $gcd(a, b) = 1$

Modular Arithmetic

- If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n; the integer n is called the modulus
- Thus, for any integer a
  - $a = qn + r, \qquad 0 <= r < n; q = [a/n]$
  - $a \mod n = r$
- Example: 1) 11 mod 7 and 2) −11 mod 7

Congruent Modulo *n*

- If (a mod n) = (b mod n), we write as $a \equiv b$ mod n
  - a and b are said to be **congruent modulo** n
- Note that if $a \equiv 0$ mod n, then $n|a$
- e.g., $73 \equiv 4$ mod 23,
- example: $21 \equiv ? -9$ mod 10

- Exercise
  - a. $19 \equiv ? -19 \bmod 10$
  - b. $20 \equiv ? -20 \bmod 10$

Properties of Congruences

- Reflexive: $a \equiv a \bmod n$
- Symmetric: if $a \equiv b \bmod n$, then $b \equiv a \bmod n$
- Transitive: if $a \equiv b \bmod n$, and $b \equiv c \bmod n$, then $a \equiv c \bmod n$
- Exercise:
  – prove: if $n \mid (a - b)$, then $a \equiv b \bmod n$

Modular Arithmetic

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(11 \bmod 10) + (12 \bmod 10)] \bmod 10 = (11 + 12) \bmod 10$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(11 \bmod 10) - (12 \bmod 10)] \bmod 10 = (11 - 12) \bmod 10$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
  - $[(11 \bmod 10) \times (12 \bmod 10)] \bmod 10 = (11 \times 12) \bmod 10$

Modular Arithmetic

- for integer $n > 1$, if $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then
  - $a \pm c \equiv b \pm d \bmod n$ and
  - $ac \equiv bd \bmod n$
  - *e.g. 1=3 mod 2 and 0 = 4 mod 2, then 1*0*≡3*4 mod 2

Euler's Totient Function

- Euler's totient function, written ø (n), is defined as the number of positive integers less than *n* and relatively prime to *n*
- By convention, ø(1) = 1
- Examples: Ø(7) = 6, Ø(4) = 2
- For a prime p, Ø(p) = p-1
- Suppose we have two primes p and q, with p!=q. Then we have, for n=pq, Ø(n) = Ø(pq) = Ø(p)* Ø(q) = (p-1)(q-1)

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

- Exercises
- $\emptyset(8) = ?, \emptyset(9) = ?$