Number Theory

CS 5158/6058 Data Security and Privacy

Spring 2018

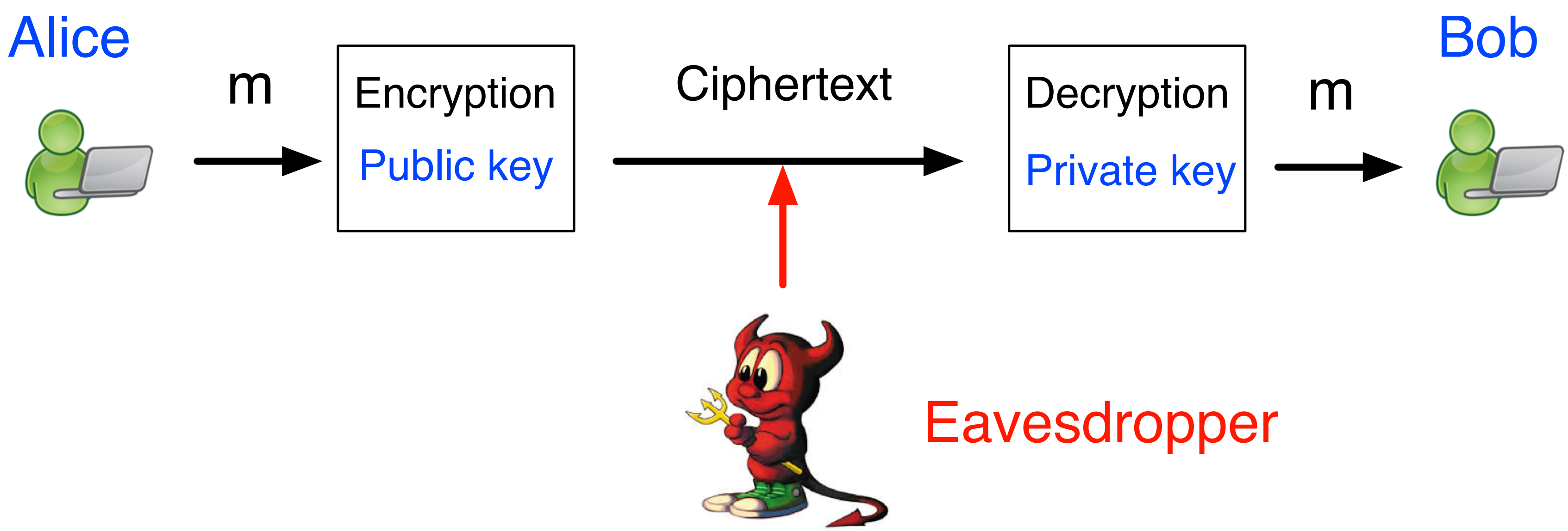
Instructor: Boyang Wang

Public-Key Cryptography

- Symmetric-Key Crypto:
  - Block Cipher and MAC
  - Need to share a private key in advance
  - Limit usage in practice: mainly military

- Public-Key Crypto (Diffie and Hellman,1976)
  - "*New Direction in Cryptography*"
  - Idea: No need to share a private key
  - Expend crypto usage to almost everywhere

Public-Key Encryption



- Alice obtains Bob’ public key from <u>public channels</u>
- Alice encrypts with public key
- Bob decrypts with private key

Prime and Composite

- A positive integer p>1 is a prime, if p has no factors, i.e., only two divisors, 1 and p; otherwise p is a composite
- Practice: Prime or Composite? 2, 3, 4, 5, 6,
    - 2: {1,2}, no factors, prime
    - 3: {1,3}, no factors, prime
    - 4: {1,2,4}, 1 factor, composite
    - 5: {1,5}, no factors, prime
    - 6: {1,2,3,6}, 2 factors, composite

Greatest Common Divisor

- For any integer $n > 1$, n is a product of primes
  - $4 = 2^2$, $5 = 5$, $10 = 2*5$, $100 = 2^2*5^2$

- Greatest Common Divisor
  - $c = \gcd(a, b)$, if $c \mid a$, $c \mid b$, and c is the greatest
  - E.g., $a = 12$, $b = 24$
    - common divisors: 1, 2, 3, 4, 6, 12
    - $\gcd(12, 24) = 12$

Greatest Common Divisor

- Greatest Common Divisor
  - c = gcd(a, b), if c | a, c | b, and c is the greatest
  - if gcd(a, b) = 1, a and b are relatively prime
  - E.g., gcd(9, 10) = 1, 9 and 10 are relatively prime
  - E.g., gcd(8, 10) = 2, 8 and 10 are not

  - If p is a prime, gcd(a, p) is either 1 or p
  - E.g., 7 is a prime, gcd(4, 7) = 1
  - 11 is a prime, gcd(44, 11) = 11

Greatest Common Divisor

- Greatest Common Divisor
  - $c = \gcd(a, b)$, if $c \mid a$, $c \mid b$, and c is the greatest

- Practice:
  - gcd(23, 100) = ??
  - gcd(24, 48) = ??
  - gcd(7, 29) = ??
  - gcd(100, 1000000000) = ??

Modulo

- For positive integers a and b
  - Unique q and r, s.t. $a = qb + r$, $0 <= r < b$
  - Modulo: $a = r \bmod q$

  - E.g., $q = 10$, $a = 11$, then $a = r = 1 \bmod q$
  - E.g., $q = 10$, then $a = 11$, $b = 21$, $c = 31$
    - $a = b = c = r = 1 \bmod q$
  - Practice: $q = 7$, $a = 51$
    - $a = ?? \bmod q$

Modular Arithmetic

- (Modular) addition, subtraction, multiplication
  - If a = a' mod q, and b = b' mod q
    - a + b = a' + b' mod q
    - a - b = a' - b' mod q
    - ab = a'b' mod q
- Example: q = 10, a = 12, b = 14,
    - a' = a = 2 mod q, b' = b = 4 mod q
    - a + b = 12 + 14 = 26 = 6 mod q
    - a' + b' = 2 + 4 = 6 mod q

Modular Arithmetic

- (Modular) addition, subtraction, multiplication
- Example: q = 10, a = 12, b = 14,
    - a’ = a = 2 mod q, b’ = b = 4 mod q

    - b - a = 14 - 12 = 2 mod q
    - b’ - a’ = 4 - 2 = 2 mod q

    - a*b = 12*14 = 168 = 8 mod q
    - a’*b’ = 2*4 = 8 mod q

Modular Arithmetic

- (Modular) addition, subtraction, multiplication

- Practice: $q = 10$, $a = 1345$, $b = 7893$,
  - what is $a + b \bmod q$?
  - what is $ab \bmod q$?

  - $a' = a = 5 \bmod q$, $b' = b = 3 \bmod q$
  - $a + b = a' + b' = 5 + 3 = 8 \bmod q$
  - $ab = a'b' = 5*3 = 15 = 5 \bmod q$

Modular Arithmetic

- (Modular) addition, subtraction, multiplication

- <u>Practice:</u> q = 7, a = 1987232, b = 234569,
    - what is a + b mod q?
    - what is ab mod q?

    - a’ = a = 2 mod q, b’ = b = 6 mod q
    - a + b = a’ + b’ = 2 + 6 = 8 = 1 mod q
    - ab = a’b’ = 2*6 = 12 = 5 mod q

Modular Division

- Modular division is not always defined
  - mod q only contains integers
    - E.g., $q = 7$, mod q includes $\{0, 1, 2, 3, 4, 5, 6\}$
  - $3/2 = 1.5$, not defined in mod q

  - $a/b = ab^{-1} \bmod q$ is defined only if b is invertible
  - b is invertible if there is an x, s.t. $bx = 1 \bmod q$
  - If $\gcd(b, q) = 1$, then b is invertible mod q
  - b^{-1} is the inverse of b mod q

Modular Division

- Modular division is not always defined
  - If gcd(b, q) = 1, then b is invertible mod q

- <u>Example:</u> b = 3, q = 7,
  - since gcd(3,7) = 1, b is invertible mod q
  - since 3*5 = 15 = 1 mod q, b^{-1} = 5 mod q
- <u>Practice:</u> b = 5, q = 11,
  - Is b invertible mod q?
  - If it is invertible, what is b's inverse?

Modular Division

- Modular division is not always defined
  - $a/b = ab^{-1} \bmod q$ is defined only if b is invertible
  - b is invertible if there is an x, s.t. $bx = 1 \bmod q$
  - If $\gcd(b, q) = 1$, then b is invertible mod q
  - b^{-1} is the inverse of b mod q

- <u>Practice:</u> $b = 5$, $q = 11$,
  - since $\gcd(5,11) = 1$, b is invertible mod q
  - since $5*9 = 45 = 1 \bmod q$, $b^{-1} = 9 \bmod q$

Group

- Let G be a set, define a binary operation $\circ$
  - A function with two inputs from G
  - Write $\circ(g,h) = g \circ h$
- Set G is a group, if
  - Closure: for all g,h in G, $g \circ h$ in G
  - Identity: there is e in G, s.t., $e \circ g = g = g \circ e$
  - Inverse: for all g in G, there is h, s.t. $g \circ h = e$
  - Associativity: $(g \circ h) \circ k = g \circ (h \circ k)$
  - <u>Abelian group</u> if commutative, i.e., $g \circ h = h \circ g$

Group

- $|G|$: order of group G,
  - i.e., number of elements in G
- Focus on finite and abelian groups
  - Identity is unique in group G
  - Each element has a unique inverse in G

- Operation $\circ$ is just a symbol
  - If additive (g+h), identity is 0, inverse -h
  - If multiplicative (g*h), identity is 1, inverse h^{-1}

Examples of Group

- The set of integers, {…, -3, -2, -1, 0, 1, 2, 3, …}
  - An abelian group under addition (identity 0)
    - $0 + g = g + 0 = g$
    - Each element has an inverse, $-1 + 1 = 0$
  - Not a group under multiplication
    - use 1 as identity
    - 3 has no inverse
    - 1/3 is not a member of this set

Examples of Group

- The set of real numbers {…, -1/2, -1, 0, 1, 1/2, …}
  - A group under addition
    - Identity is 0
  - Not a group under multiplication
    - Identity 1
    - 0 has no inverse, e.g., 0 * ?? = 1
  - Without 0, a group under multiplication
    - Identity 1
    - Each element has an inverse, e.g., 2 * 1/2 = 1

Examples of Group

- Set Z_N: {0, 1, …, N-1}, a subset of Z
  - Addition modulo N,
    - i.e., a + b = a + b mod N
  - Abelian group under addition modulo N
    - Identity is 0,
    - Each element has an inverse:
      - 2 + (N - 2) = 0 mod N
  - Order of group is N:
    - N elements in total

Examples of Group

- <u>Example:</u> Set Z_{11}: {0, 1, …, 10}, an abelian group under addition mod 11
  - Identity is 0, order of group is 11
  - Closure: g + h is still an element of Z_{11}
    - g = 3, h = 6, 3 + 6 = 9 mod 11
    - g = 8, h = 10, 8 + 10 = 18 = 7 mod 11
  - Inverse: g + h = 0, h is inverse of g
    - g = 5, h = 6, 5 + 6 = 11 = 0 mod 11
    - 6 is inverse of 5

Examples of Group

- <u>Example:</u> Set Z_{11}: {0, 1, …, 10}, an Abelian group under addition mod 11
  - What is the identity of this group?
  - What is the order of this group?
  - What is the inverse of element 8?

  - Group identity is 0
  - Group order is 11
  - 3 + 8 mod 11 = 0, so 3 is inverse of 8

Examples of Group

- Practice: Set Z_{23}: {0, 1, …, 22}, an Abelian group under addition mod 23
  - What is the identity of this group?
  - What is the order of this group?
  - What is the inverse of element 8?

  - Group identity is 0
  - Group order is 23
  - 15 + 8 mod 23 = 0, so 15 is inverse of 8

Exponentiation in Group

- Exponentiation on element g with integer x means computing ∘ operation (x-1) times on element g
  - x: an integer;
  - g: an element of group
  - If G is additive, then $g+g+\ldots+g = xg$
  - If G is multiplicative, then $gg\ldots g = g^x$
- Example of Exponentiation:
  - G is additive, $x = 2$, $g = 6$, then $6 + 6 = 12$
  - G is multiplicative, $x = 2$, $g = 6$, then $6*6 = 36$

Exponentiation in Group

- If the order of group G is $m = |G|$,
  - Exponentiation on element g with integer m is equal to the identity of G

  - If G is additive,
    - for any element g, $mg = 0$ (identity is 0)
  - If G is multiplicative
    - for any element g, $g^m = 1$ (identity is 1)

Exponentiation in Group

- If the order of group G is $m = |G|$,
  - Exponentiation on element g with integer x is equal to exponentiation on element g with integer (x mod m)
  - If G is additive, identity is 0, $mg = 0$
    - $x = qm + r$, for unique q and r
    - $xg = (qm + r)g = qmg + rg = 0 + rg$
    - since $x = r \bmod m$
    - $xg = rg = (x \bmod m)g$

Exponentiation in Group

- An additive group, order m, element g, integer x
  - for any element, $mg = 0$ (identity is 0)
  - $g+g+\ldots g = xg = (x \bmod m)g$

- Example: $Z_{15} = \{0, 1, 2, \ldots, 14\}$
  - $m = 15$, identity is 0
  - if $g = 1$, $m*g = 15*1 = 15 = 0 \bmod Z_{15}$
  - if $g = 2$, $m*g = 15*2 = 30 = 0 \bmod Z_{15}$
  - if $g = 3$, $m*g = 15*3 = 45 = 0 \bmod Z_{15}$
  - if $g = 14$, $m*g = 15*14 = 210 = 0 \bmod Z_{15}$

Exponentiation in Group

- An additive group, order m, element g, integer x
  - for any element, $mg = 0$ (identity is 0)
  - $g+g+\ldots g = xg = (x \bmod m)g$

- Example: $Z_{15} = \{0, 1, 2, \ldots, 14\}$
  - $m = 15$, identity is 0, $g = 11$
  - if $x = 152$, $x*g = 152*11 = (152 \bmod m)*11 = 2*11 = 22 = 7 \pmod{Z_{15}}$
  - if $x = 50$, $x*g = 50*11 = (50 \bmod m)*11 = 5*11 = 55 = 10 \pmod{Z_{15}}$

Exponentiation in Group

- <u>Practice:</u> $Z_{15} = \{0, 1, 2, \ldots, 14\}$, group order $m = 15$
  - Q1: element $g = 7$, integer $x = 218$, $x*g = ?$
  - Q2: element $g = 11$, integer $x = 31$, $x*g = ?$

  - $x*g = 218*7 = (218 \bmod m)*7 = (218 \bmod 15)*7$
    $= 8*7 = 56 = 11 \bmod Z_{15}$
  - $x*g = 31*11 = (31 \bmod m)*11 = (31 \bmod 15)*11$
    $= 1*11 = 11 \bmod Z_{15}$
- mod m is for integer, mod Z_{15} is for group element

Exponentiation in Group

- If the order of group G is $m = |G|$,
  - Exponentiation on element g with integer x is equal to exponentiation on element g with integer (x mod m)
  - If G is multiplicative, identity is 1, $g^m = 1$
    - $x = qm + r$, for unique q and r
    - $g^x = g^{(qm + r)} = g^{qm}g^r = 1*g^r$
    - since $x = r \bmod m$
    - $g^x = g^r = g^{(x \bmod m)}$

Exponentiation in Group

- Group G, group order m,
  - A function f_e G—>G: exponentiation on element g with integer e
    - If G is additive, $f_e(g) = e*g$,
    - If G is multiplicative, $f_e(g) = g^e$
  - If gcd(e,m)=1, then f_e is a permutation (bijection)

Exponentiation in Group

- A function f_e G—>G: $f_e(g) = e*g$ (additive group)
  - If gcd(e,m)=1, then f_e is a permutation (bijection)

- E.g., Z_5 ={0, 1, 2, 3, 4} is an additive group,
  - if e = 2, gcd(e,m) = gcd(2,5) = 1
  - $f_e(0) = 2*0 = 0$; $f_e(1) = 2*1 = 2$; $f_e(2) = 2*2 = 4$;
  - $f_e(3) = 2*3 = 6 = 1$ mod Z_5;
  - $f_e(4) = 2*4 = 8 = 3$ mod Z_5
  - f_e :{0, 2, 4, 1, 3} a permutation of Z_5

Additional Reading

Chapter 8, *Introduction to Modern Cryptography, Drs. J. Katz and Y. Lindell, 2nd edition*