Lecture 6

Algebraic Structures (Groups, Rings, Fields) and Some Basic Number Theory

Read: Chapter 7 and 8 in KPS

Cryptosystems

Classified along three dimensions:

- Type of operations used for transforming plaintext into ciphertext
  - Binary arithmetic: shifts, XORs, ANDs, etc.
    - Typical for **conventional/symmetric** encryption
  - Integer arithmetic
    - Typical for **public key/asymmetric** encryption
- Number of keys used
  - Symmetric or conventional (single key used)
  - Asymmetric or public-key (2 keys: 1 to encrypt, 1 to decrypt)
- How plaintext is processed:
  - One bit at a time – "stream cipher"
  - A block of bits – "block cipher"

Finite Algebraic Structures

- Groups
  - Abelian
  - Cyclic
  - Generator
  - Group Order
- Subgroups
- Euclidean Algorithm
- CRT (Chinese Remainder Theorem)

3

3

GROUPs

DEFINITION: A nonempty set G and *operator* @, (G,@), is a *group* if:

•CLOSURE: for all x, y in G:

- (x @ y) is also in G

•ASSOCIATIVITY: for all x, y, z in G:

- (x @ y) @ z = x @ (y @ z)

•IDENTITY: there exists *identity element* I in G, such that, for all x in G:

- I @ x = x and x @ I = x

•INVERSE: for all x in G, there exist *inverse element* x^{-1} in G, such that:

- x^{-1} @ x = I = x @ x^{-1}

DEFINITION: A group (G,@) is **ABELIAN** if:

•COMMUTATIVITY: for all x, y in G:

- x @ y = y @ x

4

4

Groups (contd)

DEFINITION: An element g **in** G is a ***group generator*** of group (G,@) if:

for all x **in** G, **there exists i ≥ 0,** such that:

$$x = g^i = g \text{ @ } g \text{ @ } g \text{ @ } \dots \text{ @ } g \quad (\text{i times})$$

This means every element of the group can be generated by g using @.

In other words, G=<g>

DEFINITION: A group (G,@) is ***cyclic*** if a group generator exists!

- *All cyclic groups are **Abelian***

DEFINITION: Group ***order*** of a group (G,@) is ***the size of set G***, i.e., |G| or #{G} or ord(G)

DEFINITION: Group (G,@) is **finite** if ord(G) is finite.

5

5

Example: Integers Under Addition

G = **Z** = integers = { … -3, -2, -1, 0 , 1 , 2 …}

the group operator is "+", ordinary addition

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

- integers are closed under addition
- identity element with respect to addition is 0 (x+0=x)
- inverse of x is -x (because x + (-x) = 0)
- addition of integers is associative
- addition of integers is commutative (the group is **Abelian**)

6

6

Non-Zero Rationals under Multiplication

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = **Q** - {0} = {a/b} where a, b in **Z***

the group operator is "*", ordinary multiplication

- if a/b, c/d in Q-{0}, then: a/b * c/d = (ac/bd) in Q-{0}
- the identity element is 1
- the inverse of a/b is b/a
- multiplication of rationals is associative
- multiplication of rationals is commutative (the group is **Abelian**)

7

7

Non-Zero Reals under Multiplication

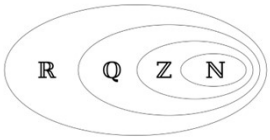
- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = **R** - {0}

the group operator is "*", ordinary multiplication

- if a, b in R - {0}, then a*b in R-{0}
- the identity is 1
- the inverse of a is 1/a
- multiplication of reals is associative
- multiplication of reals is commutative (the group is **Abelian**)

Remember:



8

8

Positive Integers under Exponentiation?

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = {0, 1, 2, 3…}

the group operator is "^", exponentiation

- closed under exponentiation
- cannot find an identity, thus also no inverse
- exponentiation of integers is NOT commutative,

x^y ≠ y^x (non-Abelian)

- exponentiation of integers is NOT associative,

(x^y)^z ≠ x^(y^z)

9

9

Integers mod N Under Addition

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = Z^{+}_{N} = positive integers mod N = {0 … N-1}

the group operator is "+", modular addition

- integers modulo N are closed under addition
- identity is 0
- inverse of x is -x (=N-x)
- addition of integers modulo N is associative
- addition integers modulo N is commutative (the group is **Abelian**)

10

10

Integers mod(p) (where p is Prime) under Multiplication

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = Z^*_p non-zero integers mod p, w/o zero = {1 … p-1}

the group operator is "*", modular multiplication

- integers mod p are closed under the * operator:
- Note that x is in Z^*_P iff GCD(x, p)=1 (GCD = Greatest Common Divisor)
- because if GCD(x, p) =1 and GCD(y, p) = 1
- then GCD(xy, p) = 1
- the identity is 1
- the inverse of x is u such that ux (mod p)=1
  - u can be found either by **Extended Euclidean Algorithm**
  - ux + vp = GCD(x, p) = 1 → (ux + vp) mod p = 1 mod p → ux mod p = 1 mod p
  - or by using Fermat's little theorem $x^{p-1} = 1 \pmod p$, $u = x^{-1} = x^{p-2}$
- * is associative
- * is commutative (so the group is **Abelian**)

11

11

Z^*_N : Non-zero Integers mod(N) Relatively Prime to N

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

G = Z^*_N

non-zero integers mod N = {1 …, x, … N-1} such that GCD(x, N)=1

- Group operator is "*", modular multiplication
- Group order ord(Z^*_N) = number of integers **relatively prime (or co-prime)** to N denoted by **phi(N), or Φ (N)**

- integers mod N are closed under multiplication:
  if GCD(x, N) =1 and GCD(y,N) = 1, GCD(x*y,N) = 1
- identity is 1
- inverse of x is from Euclidean algorithm:
  ux + vN = GCD(x,N) = 1 (mod N) → ux mod N = 1

or Euler's generalization of Fermat's little theorem:

$x^{\Phi(N)} = 1 \pmod N$ → $x^{-1} = u = x^{\text{phi}(N)-1}$

Φ (p) = p-1

- multiplication is associative
- multiplication is commutative (so the group is **Abelian**)

12

12

Subgroups

DEFINITION: (H,@) is a **subgroup** of (G,@) if:

- H is a subset of G
- (H,@) is a group

13

13

Subgroup Example

- *CLOSURE*
- *IDENTITY*
- *INVERSE*
- *ASSOCIATIVITY*
- *(Abelian) COMMUTAVITY*

Let (G,*), G = Z^*_7 = {1, 2, 3, 4, 5, 6}
Let H = {1, 2, 4} (mod 7)

Note that:
- H is closed under multiplication mod 7
- 1 is still the identity
- 1 is 1's inverse, 2 and 4 are inverses of each other
- Associativity holds
- Commutativity holds (H is **Abelian**)

14

14

Subgroup Example

Let (G,*), G = R-{0} = non-zero reals
Let (H,*), Q-{0} = non-zero rationals

H is a subset of G and both G and H are groups in their own right

15

15

Order of a Group Element

Let **x** be an element of a (multiplicative) finite integer group G.
The *order* of **x** is the smallest positive number k such that $\mathbf{x}^k = 1$

Notation: ord(x)

16

16

Order of an Element

Example: Z^*_7: multiplicative group mod 7

ord(1) = 1 because $1^1 = 1$
ord(2) = 3 because $2^3 = 8 = 1$
ord(3) = 6 because $3^6 = 9^3 = 2^3 = 1$
ord(4) = 3 because $4^3 = 64 = 1$
ord(5) = 6 because $5^6 = 25^3 = 4^3 = 1$
ord(6) = 2 because $6^2 = 36 = 1$

17

17

Theorem (Lagrange)

$\Phi(n)$ - order of G_n^*

largest order of any element!

order of g : smallest integer m such that $g^m \equiv 1 mod\ n$

Theorem (Lagrange): Let G be a multiplicative group. For any g in G, ord(g) divides ord(G).

COROLLARY 1:

$b^{\Phi(n)} \equiv 1 \bmod n \ \forall\ b \in Z_n^*$

because : $\Phi(n) = \text{ord}(Z_n^*)$

$ord(b) = \text{ord}(Z_n^*) / k = \Phi(n) / k$

thus : $b^{\Phi(n)} = b^{\Phi(n)/k * k} = 1^k = 1$

18

18

COROLLARY 2:
if p is prime then
$\forall b \in Z_p^*$
1) $b^p \equiv b \bmod p$
and
2) $\exists a \in Z_p$ ∍ $ord(a) = p - 1$
a – primitive element

Φ (p) = p-1

Example: in Z^*_{13}
primitive elements are:
{2, 6, 7, 11}

19

Euclidean Algorithm

Purpose: compute GCD(x,y)
GCD = Greatest Common Divisor
Recall that:

b^{-1} – *multiplicative inverse* of b,

$b * b^{-1} \equiv 1 \bmod n$

$\forall b \in Z_n^* \exists b^{-1} \Leftrightarrow \gcd(b,n) = 1$



$Euclidian\ (n,b) = 1 \Rightarrow \exists b^{-1}$

20

Euclidean Algorithm (contd)

$$init: \; r_0 = x \quad r_1 = y$$
$$q_1 = \lfloor r_0 / r_1 \rfloor \qquad r_2 = r_0 \bmod r_1$$
$$\ldots = \ldots$$
$$q_i = \lfloor r_{i-1} / r_i \rfloor \qquad r_{i+1} = r_{i-1} \bmod r_i$$
$$\ldots = \ldots$$
$$q_{m-1} = \lfloor r_{m-2} / r_{m-1} \rfloor \qquad r_m = r_{m-2} \bmod r_{m-1}$$
$$(r_m == 0)?$$
$$OUTPUT \; r_{m-1}$$

Example: x=24, y=15

1. 1 9
2. 1 6
3. 1 3
4. 2 0

Example: x=23, y=14

1. 1 9
2. 1 5
3. 1 4
4. 1 1
5. 4 0

21

21

Extended Euclidean Algorithm

Purpose: compute GCD(x,y) and inverse of y (if it exists)

$$init: \; r_0 = x \quad r_1 = y \quad t_0 = 0 \quad t_1 = 1$$
$$q_1 = \lfloor r_0 / r_1 \rfloor \qquad r_2 = r_0 \bmod r_1 \qquad t_1 = 1$$
$$\ldots = \ldots$$
$$q_i = \lfloor r_{i-1} / r_i \rfloor \qquad r_{i+1} = r_{i-1} \bmod r_i \qquad t_i = t_{i-2} - q_{i-1} t_{i-1} \bmod r_0$$
$$\ldots = \ldots$$
$$q_{m-1} = \lfloor r_{m-2} / r_{m-1} \rfloor \qquad r_m = r_{m-2} \bmod r_{m-1} \qquad t_m = t_{m-2} - q_{m-1} t_{m-1} \bmod r_0$$

$$if (r_m = 1) \; OUTPUT \; t_m \; else \; if (rm = 0) \; OUTPUT \; "no \; inverse"$$

22

22

Extended Euclidean Algorithm (contd)

$$q_i = \lfloor r_{i-1} / r_i \rfloor \qquad r_{i+1} = r_{i-1} mod\ r_i \qquad t_i = t_{i-2} - q_{i-1} t_{i-1}\ mod\ r_0$$

Example: x=87 y=11

I	R	T	Q
0	87	0	--
1	11	1	7
2	10	80	1
3	1	8	--

Inverse of 11 in Z^*_{87} is 8

23

23

Extended Euclidean Algorithm (contd)

Example: x=93 y=87

$$q_i = \lfloor r_{i-1} / r_i \rfloor \qquad r_{i+1} = r_{i-1} mod\ r_i \qquad t_i = t_{i-2} - q_{i-1} t_{i-1}\ mod\ r_0$$

I	R	T	Q
0	93	0	--
1	87	1	1
2	6	92	14
3	3	15	2
4	0	62	--

No Inverse Exists

24

24

Chinese Remainder Theorem (CRT)

The following system of ***n*** modular equations (congruences)

$$x \equiv a_1 \ mod \ m_1$$
$$\ldots$$
$$x \equiv a_n \ mod \ m_n$$

(all m_i-s relatively prime).

Has a unique solution:

$$x = \sum_{i=1}^{n} a_i \left(\frac{M}{m_i} \right) y_i \ mod \ M$$

where:

$$M = m_1 * \ldots * m_n$$

$$y_i = \left(\frac{M}{m_i} \right)^{-1} \ mod \ m_i$$

25

CRT Example

$$\begin{pmatrix} x \equiv 5 \ mod \ 7 \\ x \equiv 3 \ mod \ 11 \end{pmatrix}$$

$$x = [5(M / m_1) y_1 + 3(M / m_2) y_2] mod \ M$$
$$M = 77$$
$$M / m_1 = 11$$
$$M / m_2 = 7$$
$$y_1 = 11^{-1} \ mod \ 7 = 4^{-1} mod \ 7 = 2$$
$$y_2 = 7^{-1} \ mod \ 11 = 8$$
$$x = (5 * 11 * 2 + 3 * 7 * 8) mod \ 77 = 47$$

26