EE8257 Information Security

Lecture 2

Mathematical Concepts Related to Cryptography

P. S. Ranaweera
E313
Department of Electrical and Information Engineering
Faculty of Engineering
University of Ruhuna

Outline

- Number Sets
- Divisibility
- Prime & Composed Numbers
- Divisors
- Co-Prime Numbers
- Fundamental Theorem of Arithmetic
- Euclidian Theorem
- Modular Arithmetic
- Permutations
- Substitution Box

Number Sets

- Prime Numbers ($\mathbb{P}$) ➔ {2,3,5,7,11,........}
- ~~Natural~~ Numbers ($\mathbb{N}$) ➔ {0,1,2,3,....}
- Integers ($\mathbb{Z}$) ➔ {....,-2,-1,0,1,2,....}
- Rational Numbers ($\mathbb{Q}$) ➔ $\mathbf{Q} = \{a/b : a, b \in \mathbf{Z}, b \neq 0\}$
- Real Numbers ($\mathbb{R}$) ➔ rational and irrational numbers
- Complex Numbers ($\mathbb{C}$) ➔ $\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}$

Divisibility

- If $a = kd$ where $a, d \in Z$ and k is an integer ➔ $d \mid a$
  - d divides a
  - Examples

$d \nmid a$

- If $d > 0$,
  - d is the ***Divisor*** of a
  - a is the ***Multiple*** of d
- Trivial Divisors
  - Trivial divisors of a ➔ 1 and a
- Non trivial divisors ➔ Factors
  - E.g. : 12 ➔ 2,3,4 and 6

Divisibility (Cont…)

Properties of divisibility :

1. $1|a$
2. $a|0, a \neq 0$
3. $(a|b \wedge b|a) \Longrightarrow a = \pm b$
4. $(a|b \wedge b|c) \Longrightarrow a|c$
5. $a|b \Longrightarrow a|bx \forall x \in Z$
6. $(a|b \wedge a|c) \Longrightarrow a|(bx + cy) \ \forall x, y \in Z$

Prime and Composed Numbers

- An integer $a > 1$ that has only trivial divisors 1 and a is called a ***Prime Number***
  - E.g.: 2,3,5,7,11,13,.......

- An integer $a > 1$ that is not a prime number, is called as a ***Composed Number***

- ***'Unit'*** or 1 : is neither prime nor composed

Prime and Composed Numbers (Cont…)

- If $n \in Z^+$ is a composed positive integer, then
  - $\exists$ a prime p, s.t.: $p|n$
  - Examples :
    - 20 ➔ 2 and 5

Divisors

- Common Divisor :
  - d is a divisor of both a and b, then ➔ d is the common divisor of both a and b
  - Mathematical expression
  - Examples
- Greatest Common Divisor

Greatest Common Divisor

- Let $a, b \in Z$, an integer $c \in Z^{+}$ is called ***Greatest Common Divisor*** (g.c.d.) if,
  - $c|a$ and $c|b$
  - For all common divisors of a and b denoted by d ➔ $d|c$

Relatively Prime (Co-Prime) Numbers

- a and b are Relatively Prime if, $\gcd(a,b)=1$
  - 14 and 15
  - 8 and 9

- If $a, b, p \in Z^{+}$, and

$$((\gcd(a, p)=1) \wedge (\gcd(b, p)=1)) \Rightarrow \gcd(ab, p)=1$$

Fundamental Theorem of Arithmetic

Unique Prime Factorization Theorem :

- Every integer $a > 1$ can be uniquely presented in the form:

$$a = p_1^{e_1} p_2^{e_2} \ldots\ldots\ldots p_n^{e_n}$$

p_i is prime

$e_i \in Z^+$

Euclidean Theorem

- For all non-negative integers a and b

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$$a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor \times b$$

Euclidean Algorithm

$$\text{function: } \gcd(|a|, |b|)$$

$$\text{if } \; b = 0$$

$$\text{then } \; \text{return } a$$

$$\text{else } \; \text{return } \gcd(b, a \bmod b)$$

Modular Arithmetic

- Is a Calculation system where all the calculations are done in '***modulo m***' ➔ **mod m**

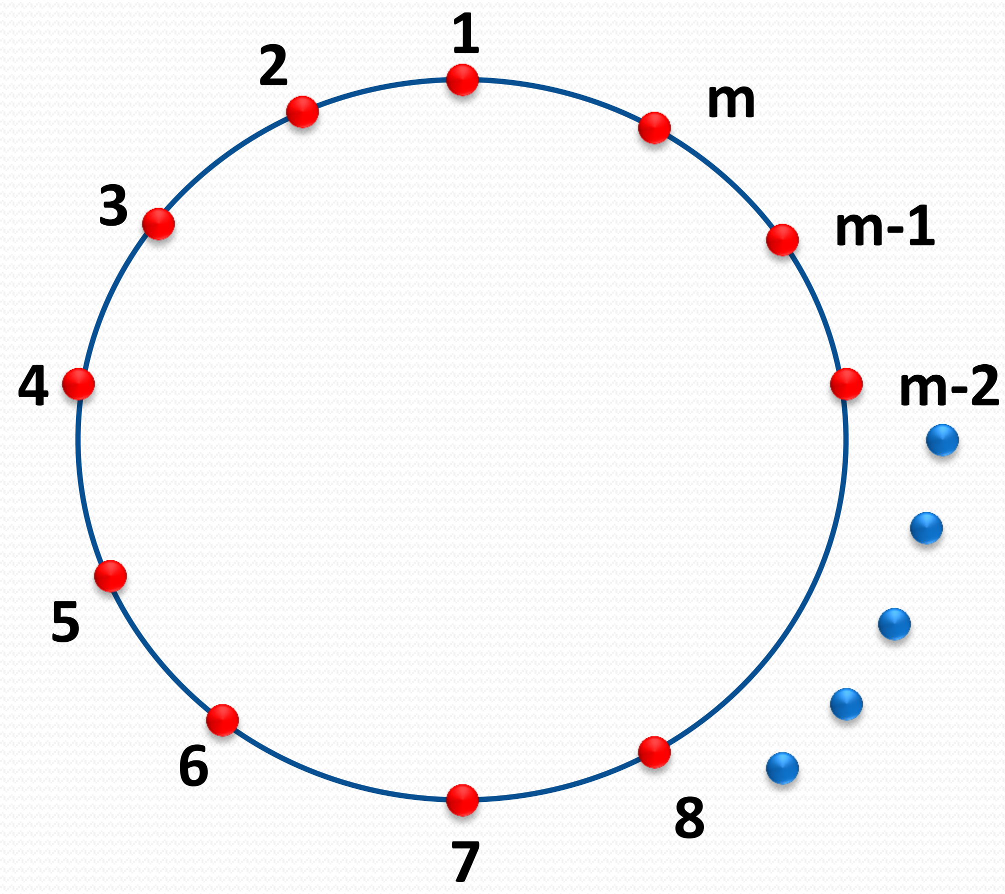
$$x \bmod m \equiv x - \left\lfloor \frac{x}{m} \right\rfloor \times m$$

- Shift Ciphers, RSA, Elgammal, Diffie-Hellman

Modular Arithmetic (Cont…)

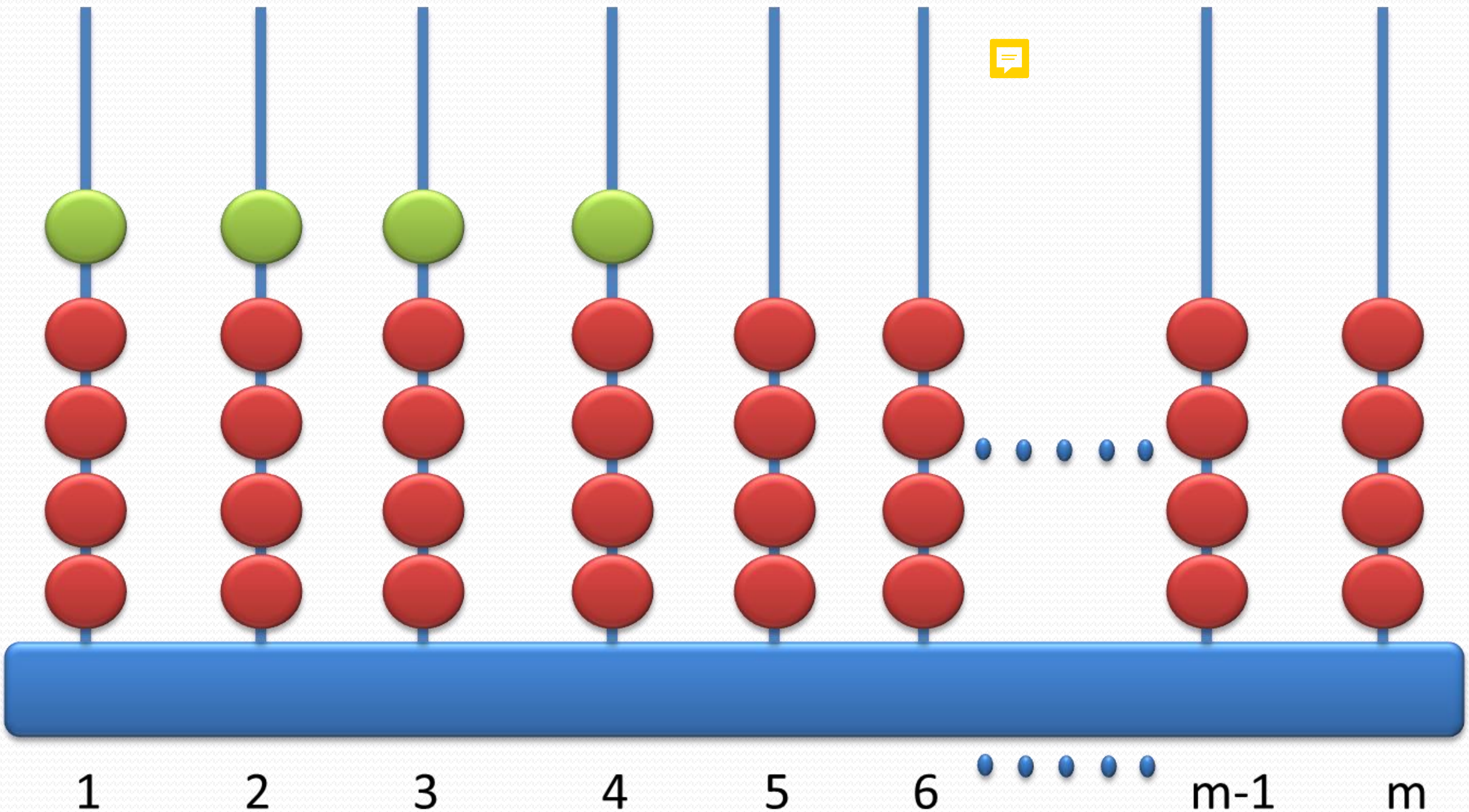
Understanding Modular Concept

- Circular Representation



Modular Arithmetic (Cont…)

- ABACUS



Modular Arithmetic (Cont…)

Properties :

- Reflexivity : $x \bmod m \equiv x, x \in Z$
- Symmetry : $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$
- Transitivity :

$$(a \equiv b \bmod m) \wedge (b \equiv c \bmod m) \Rightarrow a \equiv c \bmod m$$

- If, $a \equiv b \bmod m \Rightarrow m \mid (b-a)$ OR $a = b + km, k \in Z$
- Residue classes

$$a \bmod m = \{a, a \pm m, a \pm 2m, \ldots\ldots., a \pm km\} \bmod m, k \in Z$$

Modular Arithmetic (Cont…)

Theorem:

$$if\,, \quad a \equiv b \bmod m \text{ and } c \equiv d \bmod m$$

$$-a = -b \bmod m,\ (a + c) = (b + d) \bmod m$$

$$ac = bd \bmod m$$

Modular Arithmetic (Cont…)

Modular Inverse:

- Additive Inverse
- Multiplicative Inverse

Modular Arithmetic (Cont…)

Additive Modulo Inverse:

$$-x \bmod m$$

- Number which should be added to x, in order to obtain $0 \bmod m$

- E.g.: $-4 \bmod 7 = 3$

Modular Arithmetic (Cont…)

Multiplicative Modulo Inverse: $x^{-1} \bmod m$

- Number which should be multiplied by x, in order to obtain $1 \bmod m$
- E.g.: $7^{-1} \bmod 10 = 3$

- Multiplicative Modulo Inverse does not always exist
- x and m should be ***co-prime*** ➔ $\gcd(x, m) = 1$

Modular Arithmetic (Cont…)

Totient Function:

$$\phi(m)$$

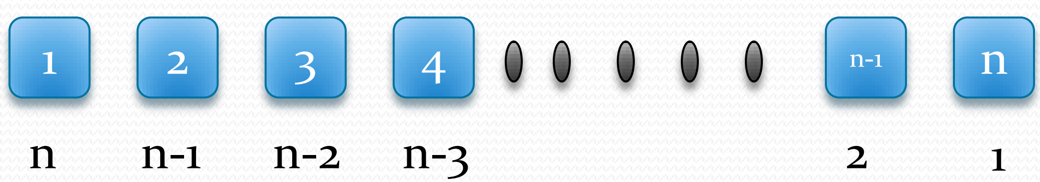
- Number of positive integers less than m that are co-prime to m
- E.g.: $\phi(5) = 4$
- For a prime number: $\phi(p) = p - 1$
- Product of prime numbers:

$$\phi(pq) = (p-1)(q-1)$$

Permutations

- ***Permutation*** (arrangement) of a given set **S** is an ordered list of all the elements in **S** in which each element appears exactly once
- E.g.: $S = \{0,1,2,3,4,5,6\} \Rightarrow S = \{4,3,0,5,6,2,1\}$
- Number of Permutations:

$$S = \{0,1,2,3,\ldots\ldots.,n-1,n\} \Rightarrow n!$$



- Symmetric-Key Cryptography

Substitution Box (S-Box)

- Deployed in DES
- Designed to cause ***Confusion***

Input bits 1 and 6 ↓	Input bits 2 thru 5															
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101