CS557: Cryptography

Elementary Number Theory

S. Tripathy
IIT Patna

An appeal

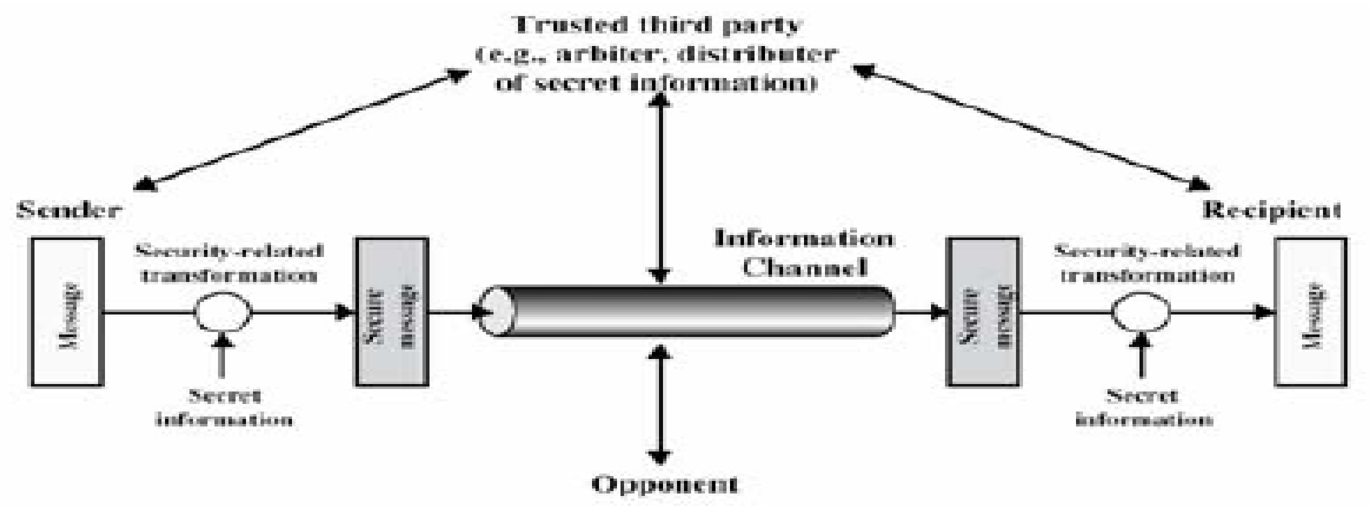
- Please keep your mobile in silent/ switch off mode

- Please Keep your mobile(s)
  - inside your bag/ pocket

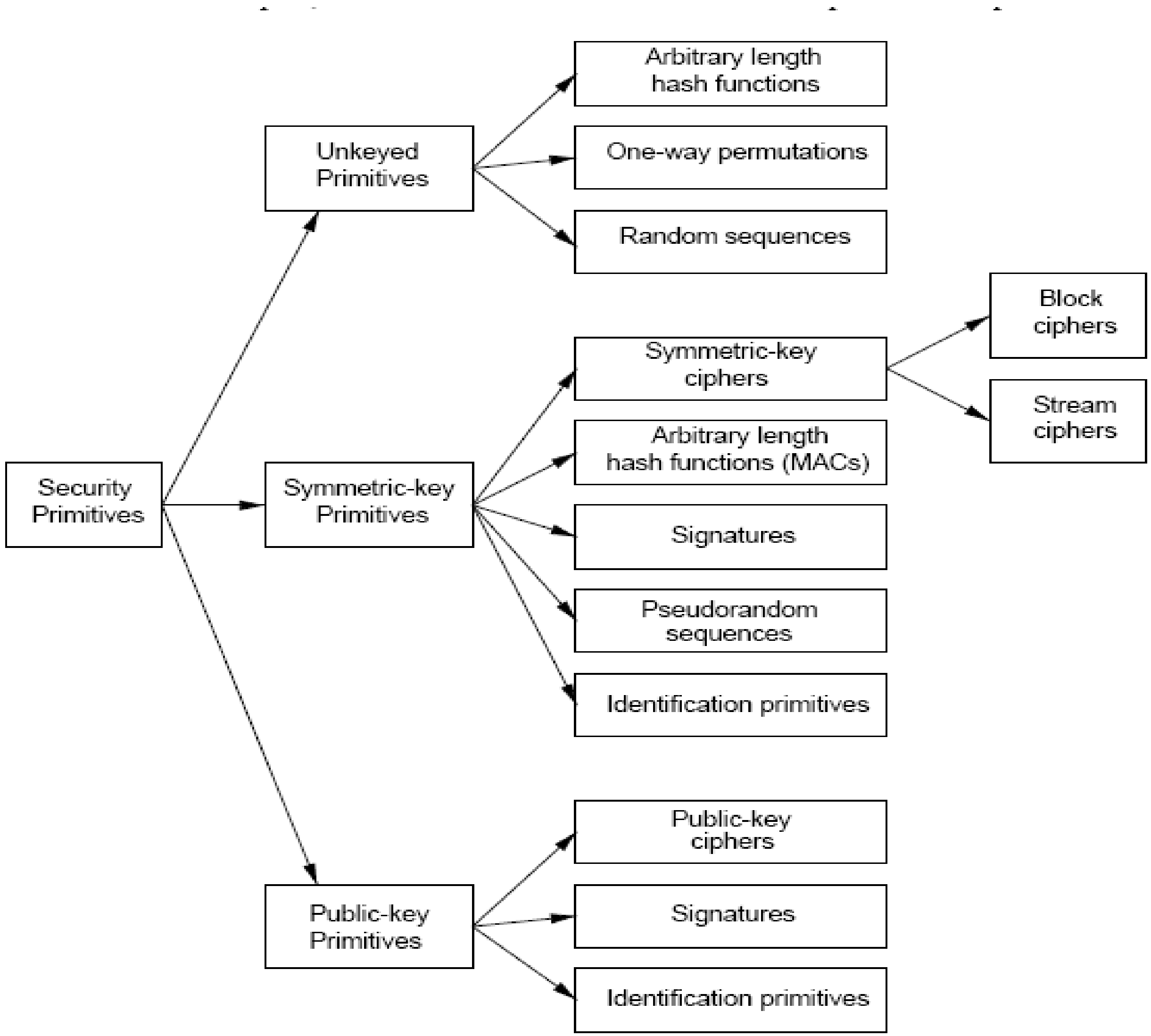
Previous Class

- Introduction to Cryptography
  - What is Cryptography?
  - Why Cryptography?
  - How it works?

- Communication in the presence of adversary
- Secure communication in an insecure channel



A Taxonomy of Cryptographic Primitives



Present Class

- Elementary Number Theory
  - Integer Operation
  - Euclidean Algorithm

Elementary Number Theory

- Motivation :
  - Increasing importance in cryptography AES, IDEA, RSA, ECC, DH etc. like cryptographic primitives design based on number theory
  - **Modular Arithmetic**

Arithmetic

- Number in different bases
  - An integer n satisfies the relation $b^{k-1} \leq n < b^k$

$$\text{number of digits} = \lfloor \log_b n \rfloor + 1 = \left\lfloor \frac{\log n}{\log b} \right\rfloor + 1.$$

  - Time estimates for Bit operations:
    - A k-bit integer operated with an n-bit integer
    - Addition
    - Multiplication

Divides

- If $a, b \in Z$ we say a divides b written as
  $a|b$
  if $ac = b$ for some $c \in Z$

- If there is no $c \in Z$ such that $ac = b$, we say that a does not divide b, written as
  $a \nmid b$

- If p is prime and $p|ab$, then $p|a$ or $p|b$

The Greatest Common Divisor (GCD)

- $gcd(a,b) = \max \{d \in z : d \mid a \text{ and } d \mid b\}$

  if $a = b = 0$, Then $gcd(0,0) = 0$
- For any a

  $gcd(0,b) = gcd(b,0) = b$
  - If $a \neq 0$, the gcd exist because

    if $d \mid a$ then $d < |a|$

- EX:
- Let $a = 2261$ and $b = 1275$
  - Also can be represented as

    $a = 7 \cdot 17 \cdot 19$ and $b = 3 \cdot 5^2 \cdot 17$,
- So $gcd(a, b) = 17$.

The Greatest Common Divisor

- For any integer a and b, we have,

$$\gcd(a,b) = \gcd(b,a) = \gcd(\pm a, \pm b)$$
$$= \gcd(a, b-a) = \gcd(a, b+a)$$

- Thus, $a, b, n \in Z$. Then $\gcd(a, b) = \gcd(a, b - an)$.

The Greatest Common Divisor [Algorithm]

1. *Assume* $a > b > 0$, We have

   $$gcd(a, b) = gcd(|a|, |b|) = gcd(|b|, |a|)$$

   If $a = b$, output a

   If $a > 0$ and $b = 0$ output a

2. [*Quotient and Remainder*] write $a = bq + r$,

   with $0 \leq r < b$ and $q \in Z$

3. [*Finished ?*] If $r = 0$,

   then $b \mid a$, so we output b and terminate.

   [*Shift and Repeat*] Set $a \leftarrow b$ and $b \leftarrow r$,

   then compute $(gcd(a,b))$ *go* to Step 2

Euclidean Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - `GCD(a,b) = a if b=0`
  - `GCD(b, a mod b)` if b ≠ 0
- Euclidean Algorithm to compute GCD(a,b) is:

```
EUCLID(a,b)
1. A = a; B = b
2. if B = 0 return  A = gcd(a, b)
3. R = A mod B
4. A = B
5. B = R
6. goto 2
```

Example GCD(68,26)

`68 = 2 x 26 + 16`	`gcd(26, 16)`
`26 = 1 x 16 + 10`	`gcd(16, 10)`
`16 = 1 x 10 + 6`	`gcd(10, 6)`
`10 = 1 x 6 + 4`	`gcd(6, 4)`
`6 = 1 x 4 + 2`	`gcd(4, 2)`
`4 = 2 x 2 + 0`	`gcd(2, 0)`

- Thanks