

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

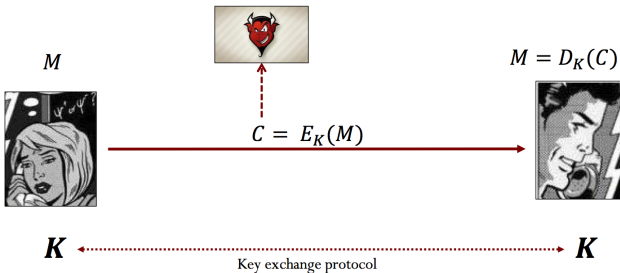
Read the chapter on the applications of congruences.

Number Theory and Cryptography

Number Theory and Cryptography

Cryptography

- One of the main tasks in Cryptography is *secure communication*.

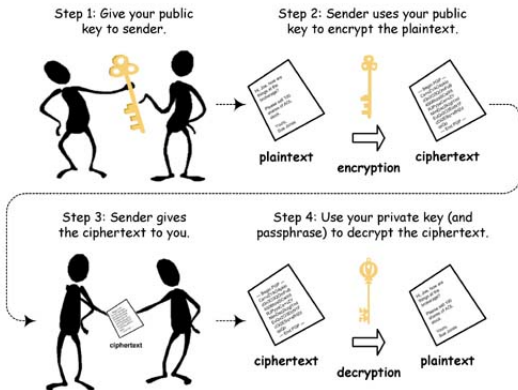


- The above picture shows a *symmetric* scheme.
- How do you construct such a scheme?

Number Theory and Cryptography

Cryptography

- The main issue with symmetric schemes is *key distribution*.
- The picture below shows an alternate mechanism known as *Public key encryption*.



Number Theory and Cryptography

Cryptography

- How do we construct a public key encryption scheme?
- The description of a public key encryption scheme involves defining three procedures.
 - Gen : This generates the public-key, secret-key pair (pk, sk) .
 - $Encrypt_{pk}(M)$: This takes as input a message and then uses just the public key to generate a cipher text.
 - $Decrypt_{sk}(C)$: This takes as input a cipher text and uses the secret key to generate the message.
- The correctness property that should hold for the above procedures is:

$$Decrypt_{sk}(Encrypt_{pk}(M)) = M.$$

Number Theory and Cryptography

Cryptography

- Consider the following scheme:
 - *Gen*: Find large n -bit primes p, q (n is usually 1024). Let $N = pq$ and $\phi(N) = (p-1)(q-1)$. Find integers e, d such that $ed \equiv 1 \pmod{\phi(N)}$. Output (pk, sk) , where

$$pk = (N, e) \quad \text{and} \quad sk = (N, d)$$

- $Encrypt_{pk}(M)$: Output $M^e \pmod{N}$.
 - $Decrypt_{sk}(C)$: Output $C^d \pmod{N}$.
- This is popularly called the RSA scheme. This is named after its inventors Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman.
- Does the correctness property hold for the above scheme?

Number Theory and Cryptography

Group Theory

Definition (Group)

A group is a set G along with a binary operator $\cdot$ for which the following conditions hold:

- ① Closure: For all $g, h \in G$, $g \cdot h \in G$.
- ② Identity: There exists an identity $e \in G$ such that for all $g \in G$,
 $e \cdot g = g \cdot e = g$.
- ③ Inverse: For all $g \in G$, there exists an $h \in G$ such that
 $g \cdot h = e = h \cdot g$. Such h is called an *inverse* of g .
- ④ Associativity: For all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.

Definition (Finite Group)

When a group G has finite number of elements, then we say that it is a finite group of *order* $|G|$.

Definition (Abelian Group)

G is called an *abelian* group if it is a group and also satisfies the following condition:

- Commutativity: For all $g, h \in G$, $g \cdot h = h \cdot g$.

Number Theory and Cryptography

Group Theory

- Exercise 1: Identity element in any group is unique.
- Exercise 2: Every element in any group has a unique inverse.
- Exercise 3: Let G be a group and $a, b, c \in G$. If $a \cdot c = b \cdot c$, then $a = b$. In particular, if $a \cdot c = c$, then a is the identity element.

End