Lecture One

Mathematical Basic Concepts

1. Introduction

This lecture introduces the basic concepts in different fields in mathematics, which the cryptography and cryptanalysis are needed, specially, in stream cipher systems, which will be discussed in details in chapter two.

This lecture is a collection of basic material on probability theory, number theory, abstract algebra, and finite fields that will be used throughout this book. The following standard notation will be used throughout:

1. $\mathbb{Z}$ denotes the set of integers; that is, the set $\{...,-2,-1,0,1,2,...\}$.
2. $\mathbb{Q}$ denotes the set of rational numbers; that is, the set $\{\frac{a}{b}|a,b\in\mathbb{Z},b\neq 0\}$.
3. $\mathbb{R}$ denotes the set of real numbers.
4. [a, b] denotes the integers x satisfying $a \leq x \leq b$.
5. $a\in A$ means that element a is a member of the set A.
6. $A\subseteq B$ means that A is a subset of B.
7. $A\subset B$ means that A is a proper subset of B; that is $A\subseteq B$ and $A\neq B$.
8. The intersection of sets A and B is the set $A\cap B=\{x|x\in A \text{ and } x\in B\}$.
9. The union of sets A and B is the set $A\cap B = \{x|x\in A \text{ or } x\in B\}$.
10. The difference of sets A and B is the set $A-B = \{x|x\in A \text{ and } x\notin B\}$.
11. The Cartesian product of sets A and B is the set $A\times B=\{(a,b)|a\in A \text{ and } b\in B\}$. For example, $\{a_1,a_2\}\times\{b_1,b_2,b_3\}=\{(a_1,b_1),(a_1,b_2),(a_1,b_3),(a_2,b_1),(a_2,b_2),(a_2,b_3)\}$.

12. $\sum_{i=1}^{n} a_i$ denotes the sum $a_1+a_2+\ldots+a_n$.

13. $\prod_{i=1}^{n} a_i$ denotes the product $a_1.a_2.\ldots.a_n$.

14. For a positive integer n, the factorial function is $n!=n(n-1)(n-2)\ldots1$. By convention, $0! = 1$.