MATH2068/2988

Lecturer: Dmitry Badziahin

Email: MATH2068@sydney.edu.au

§0 Introduction.

0.1. Cryptography.

Cryptography

Before 1970's — After 1970's.

Before most of cryptography dealt with encryption (encipher) the messages

$$M \xrightarrow{\text{encryption}} EM$$

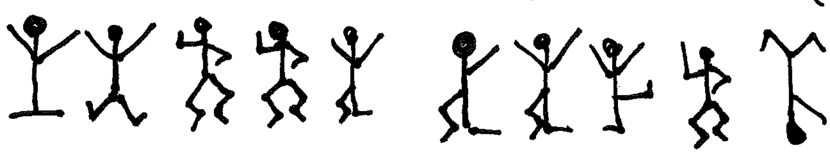
M - message

EM - encrypted message, something unreadable.

Examples:

1) In "Adventure of Dancing Men" of Arthur Conan Doyle.
Every latin symbol is replaced by a figure of dancing men.

Hello world



Substitution cipher.

2) Novel "Eight Hundred Leagues on the Amazon". By Jule Verne
The letter was enciphered by trickier method which uses a code (latin letters or digits)

Consider Code = BCD or 123

M	H	E	L	L	O	W	O	R	L	D
Code	1	2	3	1	2	3	1	2	3	1
EM	I	G	O	M	Q	Z	P	T	O	E

Vigenére cipher.

3) One of the most complicated methods of this type was implemented in "Enigma" machine.

General propert: as soon as you can encipher the message you can easily decipher it.

In 1970's "Open key" cryptography was invented.

In "Open key" cryptography encryption method is made public but no one can decrypt messages without additional information (<u>private key</u>).

Diffie-Helmann key exchange algorithm (1976)

RSA - 1977.

Remark: Theoretically there exist decryption methods in open key cryptosystems. But they take unreasonably long time to proceed.

The main concept of open key cryptography is so-called "one-way" or "trapdoor" function. It is invertible function

$$f : X \longrightarrow X$$

such that

1) $f(m)$ can be computed quickly
2) $f^{-1}(M)$ can be computed quickly if some additional info. is known
3) $f^{-1}(M)$ is extremely hard to compute without that information.

NT is a good source of trapdoor functions.

1 Peano postulates (axioms) of $\mathbb{N}$

P1) There is a natural number denoted by 0.

P2) For every natural number a there is another natural number, $S(a)$, called the "successor of a". The successor of a is unique: no a has more than one successor.

P3) There is no a such that $S(a) = 0$.

P4) Is a, b are natural numbers with $a \neq b$ then $S(a) \neq S(b)$.

P5) Suppose that A is a subset of natural numbers having the property that $0 \in A$ and the property that $S(a) \in A$ whenever $a \in A$. Then $A = \mathbb{N}$.

The we define $1 = S(0), 2 = S(1), \ldots$.
Addition is defined as follows: $a + 0 = a$, $a + 1 = s(a)$, ..., $a + S(b) = S(a + b)$.
It is easy to define the multiplication $a \cdot b$ and the order relation $a < b$. (Enthusiastic reader may do that themselves as an exercise).

§0.2. Number Theory.

General notation:

$\mathbb{Z}$ - integer numbers

$\mathbb{Q}$ - rational numbers

$\mathbb{Z}^+$ - positive integers

$\mathbb{N}$ - natural numbers.
(non-negative integers).

Property p5 is equivalent to principle of Math. induction.

Let $P(n)$ is some statement about natural numbers. We want to check $P(n)$ is true for all $n \in \mathbb{N}$.

$$A = \{n \in \mathbb{N} : P(n) \text{ is true}\}.$$

P5: If

$0 \in A$ ($P(0)$ is true)

$S(a) \in A$ as soon as $a \in A$ ($P(n+1)$ is true as soon as $P(n)$ is true)

Then A is $\mathbb{N}$.

Another reformulation of P5 is "Least integer principle": any non-empty set of natural numbers contains its minimal element.