Introduction to (mathematical) cryptography

Introduction + Basic Abstract algebra

Alexander Buchnev

May 2023

Outline

Course structure

1. Introduction + Basic Abstract algebra with SageMath
2. Basic abstract algebra with SageMath (cnt.)
3. Public key cryptography + concept of secure messaging
4. Message integrity: secure hash functions and random numbers
5. Asymmetric cryptography: RSA and Rabin cryptosystems
6. Asymmetric cryptography: DHKE with DLP some other key-exhange protocols
7. Asymmetric cryptography: ECDHKE and TLS/SSL
8. Asymmetric cryptography: digital signatures, GOST and Bitcoin curves
9. Inroduction to symmetric cryptography: block ciphers
10. Inroduction to symmetric cryptography: stream ciphers

History of cryptography

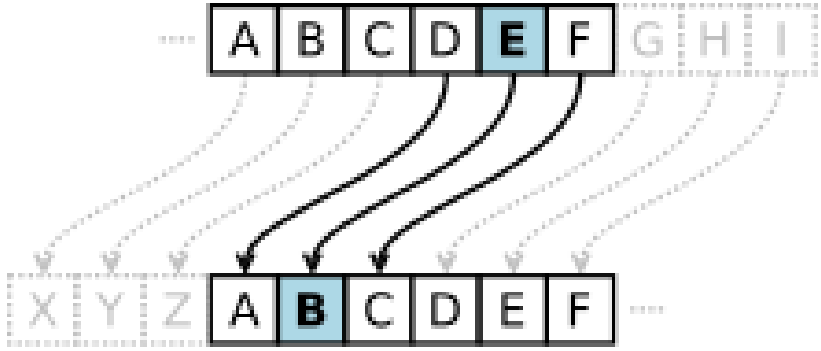


Figure: Ceasar cipher

Figure: Skytale

Figure: Examples of ancient cryptographic machinery

First cryptographers

Figure: The first page of al-Kindi's manuscript "On Deciphering Cryptographic Messages", containing the oldest known description of cryptanalysis by frequency analysis.

Figure: Auguste Kerckhoffs

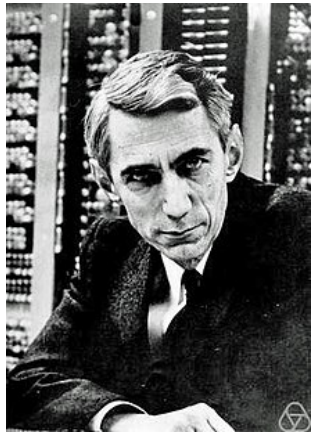


Figure: Claude Shannon

Modern cryptography

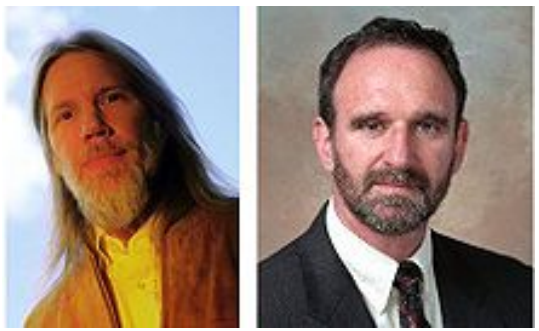


Figure: Whitfield Diffie and Martin Hellman, authors of the first published paper on public-key cryptography.

Figure: Ron Rivest, Adi Shamir and Leonard Adleman — reinventors of RSA cryptosystem.

Applications of cryptography

- Blockchains
- Secure messaging
- SSL\TLS
- Secure data storage
- You name it!

Why mathematical cryptography?

Selected topics in mathematics

- Abstract algebra (must have!)
- Number theory (must have!) — although we will only scratch the surface
- Probability theory
- Category theory

Basic Abstract Algebra

Sets (later we will define more rigorous terms) we are going to extensively use:

- $\mathbb{N}$, $\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z}$ — the set of integers modulo n
- $\mathbb{Z}/n\mathbb{Z}^*$ — important set that we will define later in this lecture

Functions (mappings)

Definition

A function from set X (domain) to set Y (co-domain) is an assignment of an element of Y to each element of X. A function is called to be 'well-defined' if and only if for each element from domain there exists exactly one element from co-domain.

Example

An example of not well-defined function:

$$\varphi : \mathbb{Q} \to \mathbb{Z}$$
$$\varphi : \frac{p}{q} \mapsto p \cdot q$$
$$\varphi\left(\frac{2}{4}\right) = 8 \neq \varphi\left(\frac{1}{2}\right) = 2$$

Image and preimage of a function

Definition

Image of a function is a set of all output values it can produce. Formally

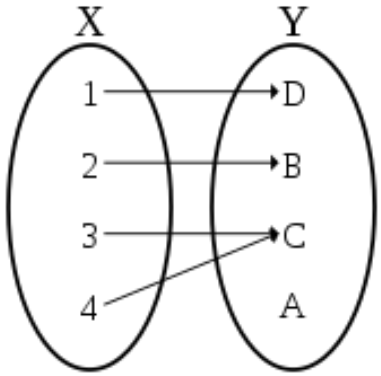
$$\psi : X \to Y, A \subseteq X$$
$$\psi[A] = \{\psi(a) : a \in A\} = B, B \subseteq Y$$

Definition

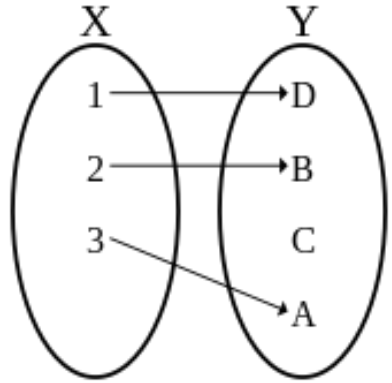
Preimage of a function is a set of all values that produce the given outputs. Formally

$$\psi^{-1}[B] = \{x \in X : \psi(x) \in B\} = A$$

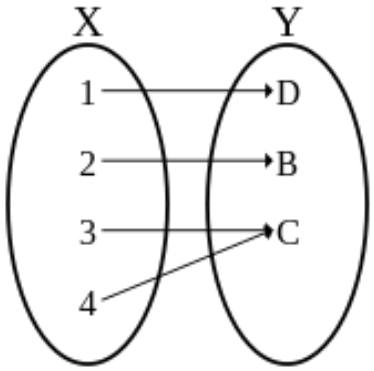
Surjection, injection and bijection



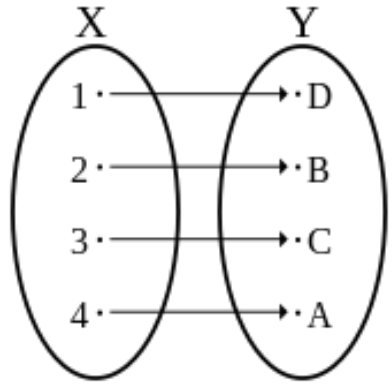
neither injection nor surjection



injection



surjection



bijection

Basic properties of integers

Definition

$a \mid b$ - a divides b

$$a, b \in \mathbb{Z}$$

$$a \mid b \iff \exists(!)c \in \mathbb{Z} : b = c \cdot c$$

(!) Only in $\mathbb{Z}$ and other PIDs (PIDs are not covered in this course)

Definition

An integer is called prime, iff it has only 2 divisors: 1 and itself

Definition

An integer is called composite if it has more than 2 distinct divisors

GCD and LCM

Definition

GCD — Greatest Common Divisor

$\gcd(a, b)$(or just (a, b)) $= \max\{c \in \mathbb{Z} : c \mid a \text{ and } c \mid b\}$

Example

$\gcd(12, 4) = 4, \quad \gcd(64, 12) = 4$

Definition

LCM — Least Common Multiple

$\text{lcm}(a, b) = \min\{c \in \mathbb{Z}_{>0} : a \mid c \text{ and } b \mid c\}$

Example

$\text{lcm}(12, 4) = 12, \quad \text{lcm}(64, 12) = 192$

Fermat's little theorem

Theorem (Fermat's little theorem)

p — *prime*, $a \in \mathbb{Z}$

$a^p \equiv a \pmod{p}$

Example

$2^7 \equiv 2 \pmod{2}, \quad -1^{13} \equiv 12 \pmod{13}$

Proof: on the next lecture

Euler's totient function and Euler's theorem

Definition

$\varphi(n)$ — The number of positive integers less than n s.t. they are coprime. Formally:

$$\varphi(n) = \#\{x : (x, n) = 1\}$$

Theorem (Euler's theorem)

$$a \in \mathbb{Z}, n \in \mathbb{Z}_{>0}$$
$$a^{\varphi(n)} \equiv a \pmod{n}$$

In other words: it is more general version of Fermat's little theorem. Both Euler's phi function and Euler's theorem are essential for understanding the RSA cryptosystem.

Introduction to SageMath

- Download and install SageMath from `https://doc.sagemath.org/html/en/installation/index.html`
- Or, alternatively, use `https://sagecell.sagemath.org/` for online access.

Homework

Build an bijection $\varphi : \mathbb{Z} \to \mathbb{N}$ and show that φ is indeed a bijection, i.e. φ is the surjection and injection simultaneously.

Next lecture

On the next lecture we are going to dig deep into Abstract Algebra, and learn new mathematical objects, such as semigroups, monoids and groups, as well as prove the Fermat's ~~last~~ little theorem and Euler's theorem.