章节安排

Outline

实验环境配置

RSA算法实践

实 验 环 境 配 置

- 软件安装包
- 实验环境配置
- 开发板介绍

章节安排

Outline

实验环境配置

RSA算法实践

实 验 目 的

- **实验1：RSA算法实践（4学时）**

  实验目的：了解常见的素数筛选和测试算法并能够编程实现

  能够采用现有工具产生大素数和对大整数进行分解

实 验 内 容

- **实验1：RSA算法实践（4学时）**
- **实验要求：**
- 1 素数筛选和测试算法

  在1-100000整数中，编程实现打印所有素数，并输出素数个数，编程语言不限
- 2 RSA Calculator实践

  https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- 3 OpenSSL实践
- 4 yafu的大整数分解

实 验 内 容

- **素数筛选算法**
  - 1 ~ $\sqrt{p}$即可
  - 如何快速筛选出1到整数n之间的所有素数?

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	…
✓		✗		✗		✗		✗		✗		✗		✗		✗		✗		…

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	…
✓	✓	✗		✗		✗	✗	✗		✗		✗	✗	✗		✗		✗	✗	…

2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	…
✓	✓	✗	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	…

实 验 内 容

- **RSA Calculator实践**
- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

实 验 内 容

- **Openssl实践**
- https://www.openssl.org
- 产生私钥
  - openssl genrsa -out rsa_2048_priv.pem 2048
- 产生公钥
  - openssl rsa -pubout -in rsa_2048_priv.pem -out rsa_2048_pub.pem
- RSA加密
  - openssl rsautl -encrypt -inkey rsa_2048_pub.pem -pubin -in plaintext.txt -out ciphertext.txt
- RSA解密
  - openssl rsautl -decrypt -inkey rsa_2048_priv.pem -in ciphertext.txt -out plaintext2.txt

实 验 内 容

- **利用yafu的大整数分解**
- https://sourceforge.net/projects/yafu/

- **在线大素数分解网站**
- http://www.factordb.com/