实验一 加密、解密与隐写术

实验目的

1. 熟悉常见的加密解密算法，掌握其原理，能编程实现如 RSA 算法；
2. 理解 ASCII 码的编码方式及其在加解密中的作用，熟悉 ASCII 对照表的使用；
3. 掌握 Base64 编码和解码原理，能够使用 Python 第三方库实现其功能；
4. 初步了解信息安全中的隐写术原理，并通过实验识别隐藏信息，提高信息提取能力。

实验要求

1. 独立完成 RSA 算法的编程实现，要求包括密钥生成、加密、解密过程，可选择任意一种熟悉的编程语言（推荐 Python 或 Java）；
2. 使用 Python 的 `base64` 库编写一个 Base64 编码和解码函数，观察原始字符串、编码后字符串和解码后字符串的对比；
3. 使用隐写术工具或编程方式分析给定的图片，提取并还原其中的密文（提示：可能经过 Base64 或 RSA 等加密、进制转换等）；
4. 实验报告需包含：
   - 实验目的、实验原理、实验过程、
   - 运行结果截图、实验总结等，
   - **严禁抄袭。**

实验内容

1. 编程实现 RSA 算法

RSA加密算法是一种非对称加密算法，在公开密钥加密和电子商业中被广泛使用。RSA是由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）在1977年一起提出的。当时他们三人都在麻省理工学院工作。RSA 就是他们三人姓氏开头字母拼在一起组成的。(来源： 维基百科-RSA 算法)

- 实现密钥生成（p、q、n、e、d）
- 编写加密函数和解密函数
- 输入明文字符串，输出密文，再解密为原文

实验要求：编程实现 RSA 加密，解密算法

算法介绍：RSA 算法由两个密钥，即公钥和私钥组成。

1）准备两个非常大的素数p和q（转换成二进制后位数越多越难破解）

2）利用字符串模拟计算大素数p和q的乘积$n = pq$；

3）同样方法计算$m = (p-1)(q-1)$，这里m为n的欧拉函数；

4）找到一个数$e(1 < e < m)$，满足$\gcd(m, e) = 1$；

5）计算e在模m域上的逆元d（即满足$ed \bmod m = 1$）；

6）公钥私钥生成完毕：(n, e)为公钥，(n, d)为私钥。

RSA 加密：

对于明文x，用公钥(n, e)对x加密的过程，就是将x转换成数字（字符串的话取其 ASCII 码或者 Unicode 值），然后通过幂取模计算出y，其中y就是密文：

$$y = x^e \bmod n$$

RSA 解密：

对于密文y，用私钥(n, d)对y解密的过程和加密类似，同样是计算幂取模：

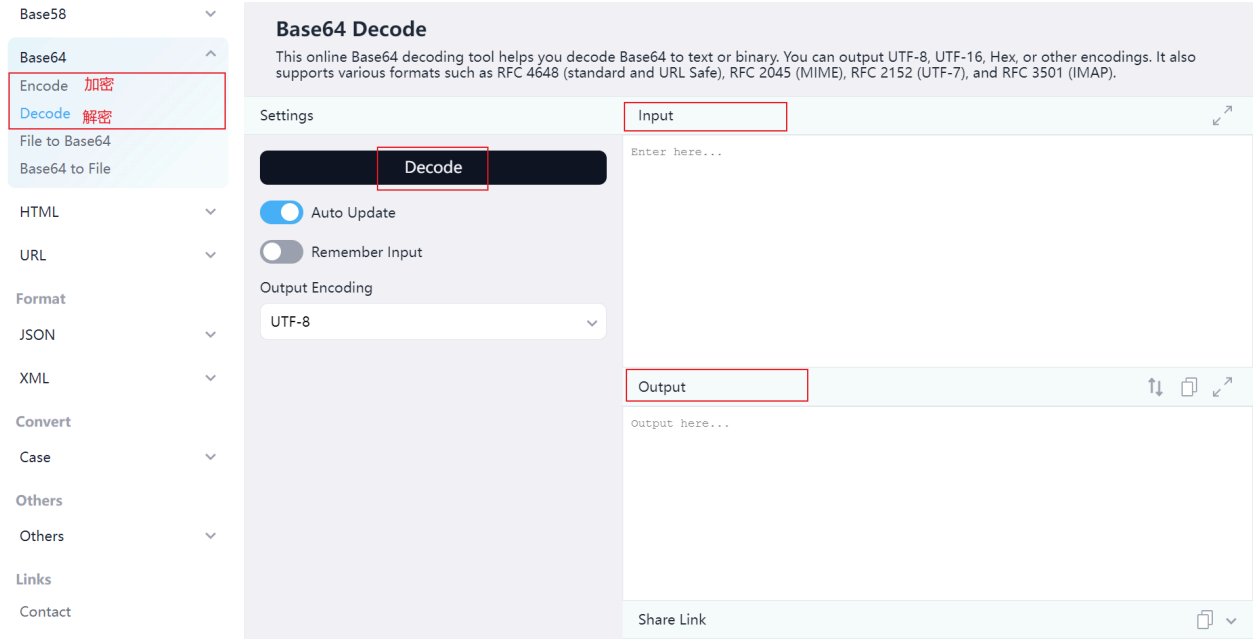
$$x = y^d \bmod n$$

2. 编写 Base64 加解密函数

- 使用 Python 的 `base64` 模块实现 encode 和 decode
- 展示原始字符串、加密后的字符串、解密后的字符串

Base64（基底64）是一种基于64个可打印字符来表示二进制数据的表示方法。由于log264=6 $\log_2 64 = 6$，所以每6个比特为一个单元，对应某个可打印字符。3个字节相当于24个比特，对应于4个Base64单元，即3个字节可由4个可打印字符来表示。在Base64中的可打印字符包括字母 `A-Z`、`a-z`、数字 `0-9`，这样共有62个字符。

- Base64 在线加解密工具
  - 在线地址

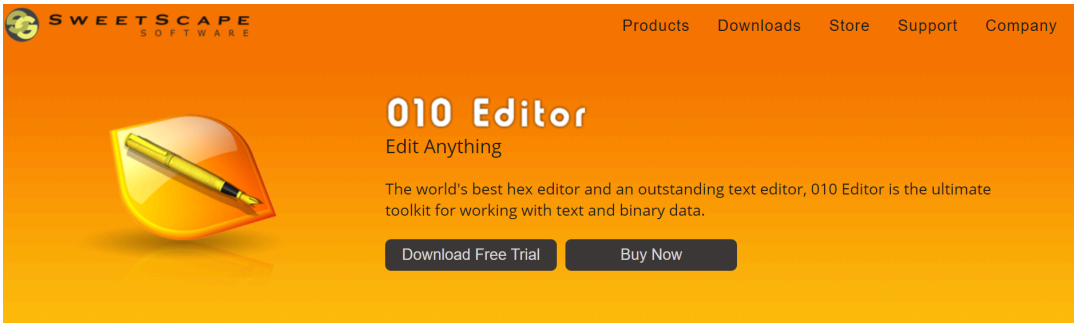


3. 提取图片中隐写的密文

- 前往文件快递柜获取实验所需图片

- 获取图片地址
- 取件码：**ODk0NTY=** （After Base64 encode）
- 下图为示例图片，非本次实验所用图片

- 使用 **010 Edito** 工具查看图片。
  010 Editor 是一款专业文本编辑器，拥有强大的文件分析和编辑功能，可以处理文本文件，二进制文件，十六进制文件，数据库文件，等等。它可以用来轻松编辑任何非结构化数据，它还支持功能强大的脚本语言，可以用来自动化数据处理，对于整理、调试、修复或其他操作有很大帮助。
  - 下载地址



- 分析图片文件结构、像素数据或十六进制数据
- 找出隐写在 Logo 图片中的密文文本。

提示：

- ASCII 码：ASCII
- 密文格式：`flag{XXXXXXXXXXXXXXX}`
- 目标文本：`Tea**********************ing!`