## 实验1：熟悉Python开发环境，Casear密码编程实现

### 实验目的

* 熟悉Pycharm/ Python Idle开发
* 完成Casear密码的编程。

### 实验内容

1、安装Python、Pycharm；了解Idle的应用；学会pip安装命令，将Cryptography gmpy2库安装到python中。

2、编写Casear密码程序，扩展到仿射密码、以及Casear密码的破译程序。

## 实验2：实现哈希编程

### 实验目的

* 学会使用hashlib模块实现对给定消息，利用不同的哈希算法生成消息摘要；
* 使用Cryptography和Crypto库实现不同的哈希算法生成消息摘要
* 体会哈希函数的抗碰撞性；
* 了解哈希函数在口令保护和区块链中的应用

### 实验内容

1. 编程实现生成空字符串、‘Alice’、‘Bob’的md5、sha256的哈希值；
2. 编程实现生成自己名字的哈希值，注意编码的转换；
3. 编写体现哈希雪崩的代码，哈希值用二进制表示； 参考Listing2-5 代码；
4. 利用scrypt密钥派生函数，实现口令加盐，生成更加安全的密钥（口令）；
5. 实现区块链中的工作量证明编程，通过设置不同的难度，体会生成符合要求哈希值需要时间长短的不同；