

# 任务分工

---

- 云数据加密：客户端+服务端的设计与实现
- 多类型文件的加密与解密的实现
- 数据库数据加密+索引加密的实现
- 两部分代码整合

- 使用对偶编码和布隆过滤器设计了模糊算法
- 利用距离可恢复加密生成安全索引
- 实现了多关键字可搜索加密

# 概述

- 客户端功能:

- ① 文件上传
- ② 文件下载
- ③ 多关键词搜索
- ④ 全部文件信息查询

- 支持的文件类型: 文本文档 (txt)、图片

- 多关键字说明:

用户手动给出文件的**关键字信息** (多关键字情况需要使用英文分号“;”对关键字进行隔开);  
在进行多关键字检索时, 同样使用英文分号对关键字进行分割。

- 文件名称加密、密文文档ID加密:

均采用AES加密算法, CBC模式 (需要密钥KEY和初始化向量IV): 采用CBC模式加密时, 明文首先与IV异或, 然后将结果进行块加密, 得到的输出就是密文, 同时本次的输出密文作为下一个块加密的IV。

# 图片加密



- 基本原理：逻辑异或运算

- 加密步骤：

- a) 随机生成KEY图像；

- b) 保存KEY图像；

- c) resize KEY图像为待加密图像尺寸；

- d) 对三个通道进行逻辑异或运算；

为了确保加密图像的隐私性，随机生成了5个KEY图像，加密过程为：

KEY1 xor Picture ---> Temp1

KEY2 xor Temp1 ---> Temp2

KEY3 xor Temp2 ---> Temp3

KEY4 xor Temp3 ---> Temp4

KEY5 xor Temp4 ---> EnPicture

(解密为加密逆过程)

# 文档加密

- 采用AES加密算法，CBC模式

- 加密步骤：

- a) 随机生成key和iv

- b) 保存key和iv;

- c) 使用AES-CBC对明文进行加密，生成密文;

- d) （如果加密文件名和密文文档ID时）使用base64对密文进行编码

- e) 存储最终密文

- base64编码：

base64编码除了数字与字母外，只有“+”“/”两个特殊字符，base64与加密解密无关，只是对数据进行编码，方便在网络间进行传输。