Java 基础回顾

Java加密解密

Base64加密方法

密码体制:

对称密码 与 非对称密码

分组密码：

流密码：

散列函数用来验证数据的完整性

特点 长度不收限制 哈希值容易计算 三列运算过程不可逆

消息摘要算法MD5

数字签名 主要是针对以数字的形式存储的消息进行的处理

OSI 安全体系

Java安全组成

Jca:提供基本的加密

Jce：DES、AES、RSA算法通过jce提供

Jsse：提供基于ssl的加密功能，大多数用于网络传输

Jaas：提供了在java这个平台上，用于安全和加密的api

包：

Java.security -消息摘要算法的实现

Javax.crypto -安全消息摘要，消息认证（鉴别）码

Java.net.ssl --安全套接字

第三方java 扩展

Bouncy Castle –两种支持方案：1）配置；2）调用

Commons Codec

-Apache

-Base64、二进制、十六进制、字符集编码

-Url编码/解码

Java Base64应用

算法的实现

-jdk

-cc

-bc

BASE64Encoder

Es:Apaceh旗下的搜索引擎

Es安装

集群和节点 一个集群由多个节点组成

索引：含有相同属性的文档集合

类型：所以可以定义一个活多个类型，文档必须属于一个类型

文档：文档是可以被索引的基本数据单位

分片：每个索引都有多个分片，每个分片是一个lucene索引

备份：拷贝一份分片就完成了分片的备份

基本用法：

RESTFul API