加密解密

描述：

该功能的目的是保护我们的http请求不能被伪造，防止非法应用请求数据。

实现：

所有请求的数据都放在请求的body里面，该body的格式为json。在每个请求发起之前会body里的，并对json的字段按字母排序。将排序后的json + secret + timestamp做MD5.

同时服务器端也对每个请求做同样的操作并与客户端的MD5进行比较。如果双方的MD5相同，则认为是有效请求，反之，这是无效请求。

其中timestamp是在应用启动时从服务器端获得的， secret是一个最重要的变量，起主要保护作用。该secret是由统一程序生成，服务器端和客户端各有一份，但两端都不保存原始内容，而是保存用blowfish加密后的密文。secret原始内容是由30个随机字符组成，该30个字符等分成三段，每一段10个字符，将这三段分别用blowfish加密成三段密文，然后将三段密文顺序连接起来再进行二次加密，将二次加密后的密文保存在客户端。当需要处理请求时先将该保存的密文进行一次解密，得到密文，然后在根据三段密文的长度分别对三段密文进行blowfish解密， 得到原始的secret，最后将json body + secret + timestamp进行MD5，将得到的MD5放入http请求头中传给server端，由server验证该请求的合法性。