关于加密/解密、编码/解密的一些你应该知道的基础知识

作为 PB 程序员，许多人只是忙于增删改查，过去课堂上学的东西早就忘光了（或者是当时就谈恋爱打网游根本没学？）。现在需要做一些加密/解密、编码/解密业务时，就抓瞎，总希望找部“点读机”，别人能点石成金，却忘记了：如果你没有一些基础知识，“点读机”告诉你的内容，你也听不懂。现就一些基础概念做一些归纳，尽量又白话方式表述，方便理解。更详细的一些内容，自己去百度查找学习。

1、何为加密解密？

通常使用**密钥**，对明文按照一定算法进行处理，得到密文，这是加密。反之为解密。

加密、解密通常是必须有密钥。又分为对称加密和不对称加密。

(1)对称加密: des, aes, sm4 … 需钥通常是一个字符串或 blob 串，长度 8 或 16 或 32 之类，有些还需要提供向量表，也是一个固定字符串，或者 blob 串。

(2)不对称加密: RSA, sm2，密钥分**公钥**和**私钥**

注意：加密解密的数据源都是二进制数据，即 PB 里的 blob 类型。Pbidea 里用 blob 或 toUtf8 都可以得到源数据的 blob 类型。

2、何为编码解码？

将数据进行码制转换，方便将二进制数据以文本方式传输。例如，一个回车，PB 里记作 “~r”，这是 PB 的编码方式，PBVM 会自动把它转成回车。作为与其他语言接口，咱们传”~r”人家也不认识啊，就得有个编码方式，把它转成肉眼可见的字符串。它的 asc 码 10 进制是 13,写成 16 进制 HEX 是 d，进行 base64 转换就是 DQ==。这就是编码了。

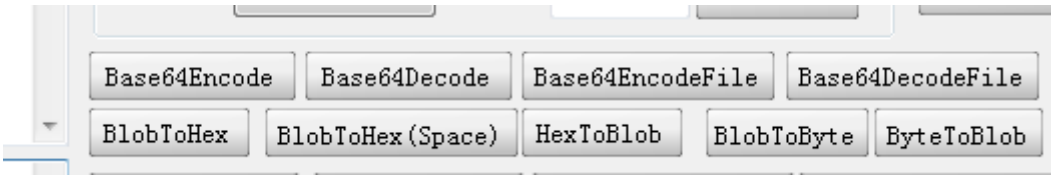
编码通常有 HEX 和 base64 两种方式。HEX 就是将二进制串，每一个字节用个字符的十六进制表示，比如回车它就是 0D 或 0d。base64 概念稍微复杂点，请自行百度。

E698A5E99BA8E6838AE698A5E6B885E8B0B7E5A4A9E, 这是一个 HEX 串

5pil6Zuo5oOK5pil5riF6LC35a==， 这是一个 base64 串

仔细比较上面的串有什么不一样，至少肉眼可以分辨出，它是 hex 还是 base64，根据需要使用，而不是强行将 hex 当作 base64 使用，或将 bse64 当作 hex 使用。必要时，需要转成 blob 二进制方式使用。通常你的接口文档上对这些使用规范有规定。

不管以何种编码展示数据，其根本还是 blob 二进制数据，本质上不变。



具体可以到 pbidea demo 里去熟悉这些个编码转换。

3、何为哈希(hash)？

这些最容易为人误以为是加密解密。

Hash 是一种摘要信息。例如你有 10 万字的一篇文章，你写个简述，体现文章主题，可能就几十个字，这就是摘要，也就是哈希(hash)。根据这个摘要，是不可能还原出你那 10 万个字的文章的。所以，**哈希(hash)是不可逆的**。它也不是加密，更谈不上解密。

常用的哈希(hash)算法有： md5, sm3, sha1, sha128,sha256 ……

4、签名

那什么是签名呢？结合上面已述内容：

签名就是先进行哈希，得到一个摘要，再对这个摘要进行非对称加密。

验签就是对使用密钥对签名数据解密，再对数据进行哈希得到摘要，比较摘要与解密结果是否一致，一致就是验签通过，不一致就是验签不通过。

常用签名是 sm2withsm3，即 sm3 哈希后 sm2 加密。 RSAwithXXX,使用 md5 sha1 ….哈希后用 rsa 加密。

5、国密系统

国密概念自行百度，常用的包含 3 个算法：sm2 sm3 sm4

对照前文概念：

sm2： 是非对称加密解密算法，它需要公钥和私钥。也可以用它进行签名。注意：公钥和私钥通常是交换使用，例如 用户 A 和用户 B：用户 A 拥有 A 的私钥和 B 的公钥，而用户 B 拥有 A 的公钥和 B 的私钥，这样他们才能互相发数据进行加密解密，或者签名验签。

注意：私钥要妥善保管好，因为有了私钥可以推导出公钥。

sm3： 是哈希算法，就是提取一个摘要。

sm4： 是对称加密解密算法，它通常需要一个 16 字节长度的密钥(这里指 blob 长度)，至于 hex 长度那当然是 32（因为 16*2，一个字节是 2 个字符长度的 16 进制字符串），base64 长度通常是 24 个左右，因为长度超出 1/3。

6、敬请读熟你的接口文档

以上相关知识，在你的接口文档里都有具体说明，例如说 UTF8，那你就不能用 blob 对字符串直接转，你得用 toUtf8 进行转换。密钥提供 HEX 还是 base64 方式，结果使用哪种方式编码，这些文档接口里基本上都有，不清楚的，找对方技术支持问清楚。

弄清楚以上基本概念，在加密解密这些业务上就不会再有牵绊，这些概念本身不限语言，即使在其他语言中，原理同样适用。

大自在

2024 年 7 月 19 日