Java 加密算法

java 加密 算法

Base64

严格地说，Base64 属于编码格式，而非加密算法。

Base64被定义为：Base64内容传送编码被设计用来把任意序列的8位字节描述为一种不易被人直接识别的形式。（The Base64 Content-Transfer-Encoding is designed to represent arbitrary sequences of octets in a form that need not be humanly readable.）

另，BASE加密后产生的字节位数是8的倍数，如果不够位数以=符号填充。

对称加密算法

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法

在这只讲解两个，其它的可百度

- DES

  DES-Data Encryption Standard,即数据加密算法。DES算法的入口参数有三个:Key、Data、Mode。其中Key为8个字节共64位,是DES算法的工作密钥;Data也为8个字节64位,是要被加密或被解密的数据;Mode为DES的工作方式,有两种:加密或解密。

- PBE

  PBE——Password-based encryption（基于密码加密）。其特点在于口令由用户自己掌管，不借助任何物理媒体；采用随机数（这里我们叫做盐）杂凑多重加密等方法保证数据的安全性。是一种简便的加密方式。

单向加密算法

- MD5(Message Digest algorithm 5，信息摘要算法)
- SHA(Secure Hash Algorithm，安全散列算法)
- HMAC(Hash Message Authentication Code，散列消息鉴别码)

MD5、SHA以及HMAC是单向加密，任何数据加密后只会产生唯一的一个加密串，通常用来校验数据在传输过程中是否被修改。其中HMAC算法有一个密钥，增强了数据传输过程中的安全性，强化了算法外的不可控因素。

非对称加密算法

与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥

- RSA
  算法的名字以发明者的名字命名：Ron Rivest, AdiShamir 和Leonard Adleman。
  这种加密算法的特点主要是密钥的变化，上文我们看到DES只有一个密钥。相当于只有一把钥匙，如果这把钥匙丢了，数据也就不安全了。RSA同时有两把钥匙，公钥与私钥。同时支持数字签名。数字签名的意义在

于，对传输过来的数据进行校验。确保数据在传输工程中不被修改。
流程分析：

1. 甲方构建密钥对儿，将公钥公布给乙方，将私钥保留。

2. 甲方使用私钥加密数据，然后用私钥对加密后的数据签名，发送给乙方签名以及加密后的数据；乙方使用公钥、签名来验证待解密数据是否有效，如果有效使用公钥对数据解密。

3. 乙方使用公钥加密数据，向甲方发送经过加密后的数据；甲方获得加密数据，通过私钥解密。

- DH

  Diffie-Hellman算法(D-H算法)，密钥一致协议。

  流程分析：

  1. 甲方构建密钥对儿，将公钥公布给乙方，将私钥保留；双方约定数据加密算法；乙方通过甲方公钥构建密钥对儿，将公钥公布给甲方，将私钥保留。

  2. 甲方使用私钥、乙方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥加密数据，发送给乙方加密后的数据；乙方使用私钥、甲方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥对数据解密。

  3. 乙方使用私钥、甲方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥加密数据，发送给甲方加密后的数据；甲方使用私钥、乙方公钥、约定数据加密算法构建本地密钥，然后通过本地密钥对数据解密。

- DSA

  DSA-Digital Signature Algorithm, 是一种更高级的验证方式，用作数字签名。不单单只有公钥、私钥，还有数字签名。私钥加密生成数字签名，公钥验证数据及签名。如果数据和签名不匹配则认为验证失败！数字签名的作用就是校验数据在传输过程中不被修改。数字签名，是单向加密的升级！

- ECC

  ECC-Elliptic Curves Cryptography，椭圆曲线密码编码学，是目前已知的公钥体制中，对每比特所提供加密强度最高的一种体制。在软件注册保护方面起到很大的作用，一般的序列号通常由该算法产生。