**JAVA密码技术**

1.什么是JAVA加密？

对JAVA源代码加密，使其不被窃取、反编译等的一种保护技术。JAVA的源代码很容易被偷看只要有一个反编译器，任何任都可以分析JAVA源代码，JAVA的灵活性使得源代码不被窃取，

2.JAVA加密的方式、适用场景？

基本的单向加密算法：

* BASE64 严格地说，属于编码格式，而非加密算法
* 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)

复杂的对称加密（DES、PBE）、非对称加密算法：

* DES(Data Encryption Standard，数据加密算法)
* PBE(Password-based encryption，基于密码验证)
* RSA(算法的名字以发明者的名字命名：Ron Rivest, AdiShamir 和Leonard Adleman)
* DH(Diffie-Hellman算法，密钥一致协议)
* DSA(Digital Signature Algorithm，数字签名)
* ECC(Elliptic Curves Cryptography，椭圆曲线密码编码学)

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。

常见于邮件、http加密，截取http信息，登录操作的用户名、密码字段一般采用BASE64加密。

解密：public static byte[] decryptBASE64(String key) throws Exception {

return (new BASE64Decoder()).decodeBuffer(key);

}

加密：public static String encryptBASE64(byte[] key) throws Exception {

return (new BASE64Encoder()).encodeBuffer(key);

}

BASE64加密后产生的字节位数是8位数，如果不够位数用“=”填充。主要的是BASE64Decoder和BASE64Encoder这两个类以及方法。

MD5 -- message-digest algorithm 5 （信息-摘要算法）缩写，广泛用于加密和解密技术，常用于文件校验。不论文件有多大都能生成唯一的MD5值， 通常不直接使用MD5加密，而是将MD5产生的字节数组交给BASE64再一次加密。

SHA(Secure Hash Algorithm，安全散列算法），数字签名等密码学应用中重要的工具，被广泛地应用于电子商务等信息安全领域，SHA和MD5都通过碰撞法已经破解，但SHA仍然是公认的安全加密算法，较之MD5更加安全。

HMAC：(Hash Message Authentication Code，散列消息鉴别码)基于密钥的Hash算法的认证协议，原理：用公开函数和密钥产生一个固定的值作为认证标识，用来鉴别消息的完整性，使用一个密钥生成一个固定大小的数据块即MAC，并将其加入到消息中用于传输，接收方利用与发送方共享的密钥进行鉴别认证。

DES(Data Encryption Standard，数据加密算法)DES算法是一种用56位密钥来加密64位数据的对称密钥算法。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。对称算法，数据加密标准，速度较快，适用于加密大量数据的场合

PBE(Password-based encryption，基于密码验证) 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。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：由 RSA 公司发明，是一个支持变长密钥的公共密钥算法，需要加密的文件块的长度也是可变的，非对称算法。

DH(Diffie-Hellman算法，密钥一致协议) 是安全性基于在有限域中计算离散对数的难度的一种加密算法。可用于密钥分发，但不能用于加/解密报文。

DSA(Digital Signature Algorithm，数字签名) 它是另一种公开密钥算法，它不能用作加密，只用作数字签名。DSA使用公开密钥，为接受者验证数据的完整性和数据发送者的身份。它也可用于由第三方去确定签名和所签数据的真实性。DSA算法的安全性基于解离散对数的困难性，这类签字标准具有较大的兼容性和适用性，成为网络安全体系的基本构件之一。

ECC(Elliptic Curves Cryptography，椭圆曲线密码编码学) 属于公开密钥算法，单位安全强度相对较高，它的破译或求解难度基本上是指数级的，黑客很难用通常使用的暴力破解的方法来破解。数学原理相对简单，在工程应用中比较易于实现，但它的单位安全强度相对较低。因此，ECC算法的可以用较少的计算能力提供比RSA加密算法更高的安全强度，有效地解决了“提高安全强度必须增加密钥长度”的工程实现问题。