密码算法

笔记本：	白皮书		
创建时间：	2019/10/8 16:20	**更新时间：**	2019/10/14 13:56
作者：	jyyhermance@163.com		
URL：	file:///C:/Users/Hermance/Desktop/说明书--故障诊断与预警.docx		

哈希算法

- 输入 任意长的字符串
- 输出 固定长度
- 计算过程有效率

特点：

1. 抗冲突，不同的输入输出不能相同（不代表不可能出现冲突，只是代价很大）
2. 信息隐藏，不可逆向还原
3. 可隐匿性，不能在合理的时间内，得到一个特定的输出值

MD5：输出4*32，已被破解
SHA1：已被google破解
SHA2：包括224，256，384，512
SHA3：即Keccak算法
RIPEMD-160

应用：
区块哈希
梅克文树

公开密钥算法

公钥加密 私钥解密 但不适用于大段数据

RSA：
基于大质数分解难度
产生密钥很麻烦；分组长度太大，运算代价高，速度慢
例子：
选择两个质数 p q
p * q = n
φ(n) = (p-1) * (q-1)
随机选择整数e，1<e<φ(n) 且 与φ(n)互质
计算d -> e * d ≡ 1 (mod φ(n)) 即 e*d + φ(n)*y = 1
产生公钥（n, e）和私钥（n, d）

椭圆曲线密码算法：
ECDSA
安全性高，生成方便，处理速度快，存储空间小
SECP256k1
比特币

编码/解码算法

Base64：
64个字符 大小写字母 十个数字 + /
例子：
    3个字节   10101101,10111010,01110110
    转换为4个字节   00101011, 00011011 ,00101001 ,00110110
    对应的十进制 43 27 41 54
    码表中的值 r b p 2

Base58：
少了 0 O I l + /
Base58 Check：
加了校验码 防止传输错误