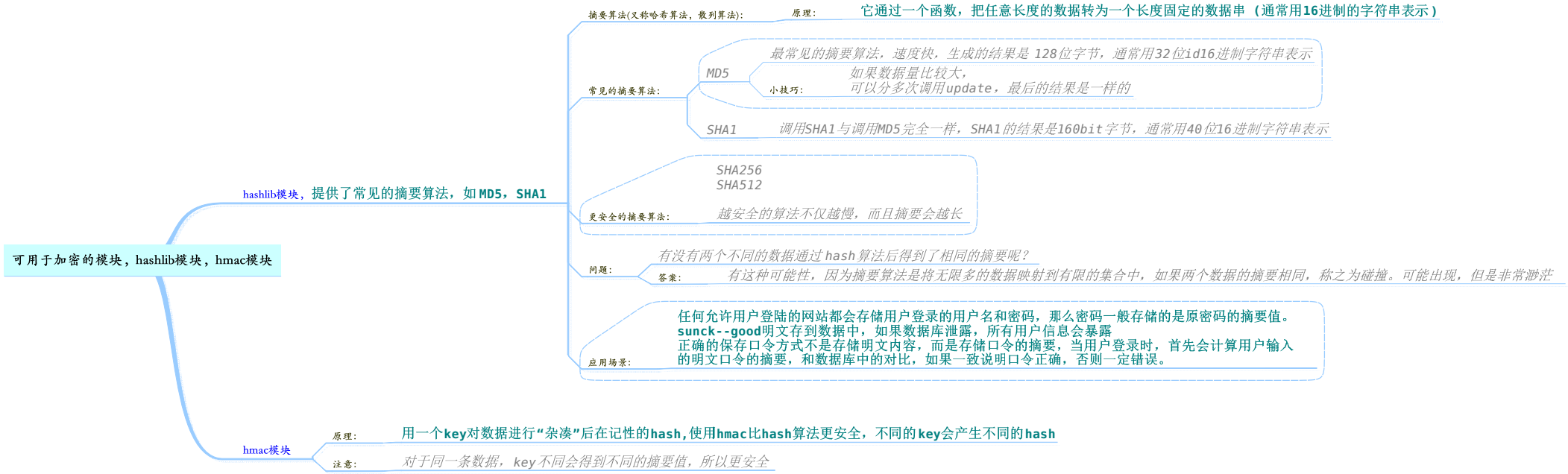
可用于加密的模块，hashlib模块，hmac模块
hashlib模块，提供了常见的摘要算法，如MD5，SHA1
摘要算法(又称哈希算法，散列算法):
原理:
它通过一个函数，把任意长度的数据转为一个长度固定的数据串（通常用16进制的字符串表示）
常见的摘要算法:
MD5
最常见的摘要算法，速度快，生成的结果是128位字节，通常用32位id16进制字符串表示
小技巧:
如果数据量比较大，
可以分多次调用update，最后的结果是一样的
SHA1
调用SHA1与调用MD5完全一样，SHA1的结果是160bit字节，通常用40位16进制字符串表示
更安全的摘要算法:
SHA256
SHA512
越安全的算法不仅越慢，而且摘要会越长
问题:
有没有两个不同的数据通过hash算法后得到了相同的摘要呢？
答案:
有这种可能性，因为摘要算法是将无限多的数据映射到有限的集合中，如果两个数据的摘要相同，称之为碰撞。可能出现，但是非常渺茫
应用场景:
任何允许用户登陆的网站都会存储用户登录的用户名和密码，那么密码一般存储的是原密码的摘要值。
sunck--good明文存到数据中，如果数据库泄露，所有用户信息会暴露
正确的保存口令方式不是存储明文内容，而是存储口令的摘要，当用户登录时，首先会计算用户输入的明文口令的摘要，和数据库中的对比，如果一致说明口令正确，否则一定错误。
hmac模块
原理:
用一个key对数据进行“杂凑”后在记性的hash,使用hmac比hash算法更安全，不同的key会产生不同的hash
注意:
对于同一条数据，key不同会得到不同的摘要值，所以更安全