对称密码作业

1. 分组密码主要采用哪两个原则来抵抗攻击者对密码体制的统计分析？评价密码算法抵抗统计分析能力的准则是什么？
2. 扩散、混乱
3. 雪崩、完全性

2、DES算法已经不再安全的主要原因是什么？当前的主要替代方法是什么？

（1）通过穷举法可破解；存在互补对称性；随机选择密钥，有可能会选中弱密钥或半弱密钥，使得很容易破解；差分攻击，线性攻击

（2）AES

3、DES算法在使用过程中需要注意什么？从算法本身的要求、算法安全性角度分析。

算法本身：分组长度为64bits，密文长度也是64bits，有效密钥长度为56bits。加密过程分为初始置换、16轮迭代、末置换

算法安全性：可以实现暴力破解，因此可以尝试多重DES；尽量不要使用弱密钥

4、简要描述Feistal网络和SP网络在设计分组密码时各自是如何体现扩散、混淆的？各有什么优缺点？

（1）Feistal：该网络中每轮结构相同，右半数据进行F运算后与左半数据进行异或，体现扩散；每轮采取不同的k值，完成后左右两边数字互换，体现混淆。

SP：S变换：混乱；P变换：扩散。

（2）Feistal优点：加解密过程相似；对轮函数没有可逆要求。

缺点：要更多的轮数。

SP优点：符合香农要求；轮数少、扩散快。

缺点：要经过多次数据变换操作。

5 、DES密钥的所有弱密钥、半弱密钥、四分之一弱密钥、八分之一弱密钥全部加起来，一共有多少个安全性差的密钥？

256个

6、为什么要使用加密模式（分组密码的工作模式）？说出两个理由

多次使用相同的密钥对多个分组加密，会引发许多安全问题。为了应对不同场合，因而需要开发出不同的工作模式来增强密码算法的安全性。

7、分别分析说明电视直播、网络点播适合采用的加密模式是什么。

电视直播要求加密速度快，所以使用CTR。

网络点播对速度要求没那么大，所以使用OFB。

8、找一下国密算法中哪些分组密码、哪些是序列密码？序列密码在使用中需要注意什么？

分组：SM1，SM2，SM3，SM4，SM7

序列：ZUC

密钥序列产生器生成的密钥序列要有尽可能高的不确定性。

9、假设你能够使用的计算能力如下：

* 每台计算机每秒可尝试10^20个密钥
* 一共有10^100台计算机
* 所有的计算机可运转10^20年

如果依然要保证暴力破解遍历整个密钥空间失效，那么密钥长度需要多少比特？

1）只要512比特就够了

2）至少1024比特

3）至少2048比特

4）4096比特

512比特

10、设密文空间共含有5个信息mi（1≤i≤5），并且p(m1)=p(m2)=1/4，p(m3)=1/8，p(m4)=p(m5)=3/16，求H(M)。

H（M）=-（2\*（1/4log1/4）+1/8log1/8+2\*(3/16log3/16)）=23/8-3/8log3

11、设明文分组序列xi…xn产生的密文分组序列为y1…yn。假设一个密文分组yi在传输时出现了错误（即某些1变成了0，或者相反），不能正确解密的明文分组数目在应用（ ）模式时为1。

A．电子密码本模式和输出反馈模式

B．电子密码本模式和密码分组链接模式

C．密码反馈模式和密码分组链接模式

D．密码分组链接模式和输出反馈模式

A

1. 下面假设一个密钥长度为192位的AES和一个每秒可以检查3-107个密钥的ASIC。

（1）如果并行使用100000个这样的IC，一次密钥搜索平均需要多长时间？请将这个时间长度与宇宙年龄（大致为1010年）进行比较。

（2）假设摩尔定理在未来数年内始终有效，我们需要等多少年才能构建一个可在24小时内执行一次一般AES-192密钥搜索的密钥搜索机器？同时假设能并行使用100000个IC。

（1）2^192/(3\*10^12)>10^10\*60\*60\*24\*356

(2)83