密码学

Modified:: 2023-03-23 16:27

1. DES算法加密过程
    1. DES是由一个64位的明文和一个64位的密钥作为输入，然后输出一个64位的密文。
    2. 具体过程就是明文首先进行IP置换，然后进入一个Feistel网络，最后再经过一次IP逆置换。
    3. Feistel网络即将一个64位的数据作为输入，然后分成左右各32位的两部分，分别是L0和R0，然后进行若干次的迭代循环，DES算法是循环16次。每轮迭代中，Ri是Ri-1经过一次轮函数之后再和Li-1异或的结果，Li是Ri-1。这样不断迭代下去，得到L16和R16，然后再经过一次调换，之后组合成64位的输出。
    4. 至于轮函数的过程就是将32位的数据和48位的子密钥作为输入，得到32位的输出，这个48位的子密钥是通过64位的密钥经过密钥编排得到的，64位的密钥通过密钥编排得到16个48位的子密钥，分别对应16轮迭代。
    5. 轮函数的过程是首先将32位的输入进行E扩展，扩展为48位，然后和子密钥进行异或，得到的结果分为8组，每组6位。这8组分别进行一个S盒变换，得到8组4位的数据，合在一起即32位，最后再进行一个P置换，就得到了输出。
    6. 这就是DES算法的全部过程
2. S盒是什么
   S盒是一个4*16的矩阵，其中矩阵的行对应输入的第一位和最后一位，列对应输入的中间四位，所以当输入一个6位的比特串时，就可以知道对应这个矩阵的几行几列，然后就可以得到唯一一个对应的四位比特串
3. 密钥编排的过程
   将56位的密钥通过PC1变换分为了左右两个28位的部分，分别是C_0和D_0。然后根据移位次数表，按照上面轮函数迭代的次数分别进行左循环移位一位或者两位，然后再经过PC2置换得到最后要求的48位的子密钥
4. DES算法属于什么结构
5. DES中的轮函数主要采用了Feistel结构
6. AES算法加密过程
    1. AES算法是基于代换置换网络构建的，由一个16字节的明文和16字节的密钥作为输入，然后生成16字节的密文。
    2. 具体过程就是首先通过密钥扩展，将16字节的密钥扩展为11个16字节的子密钥K0到K10，分别对应每一轮循环。
    3. 首先是明文和k0进行一次异或，然后进入转换函数，然后得到输出，然后输出再和K1进行一次异或，然后再进入转换函数，如此循环10次，最后和k10进行一次异或得到最终的输出

4. 转换函数的过程主要分为3步，分别是字节代换，行移位，列混合，其中最后一次循环没有列混合这一个步骤。
5. 字节代换就是有一个S盒，然后对输入的每个字节都使用一次S盒，得到输出，然后行移位是对字节矩阵进行向右循环平移，第一行不动，第二行平移一个字节，第三行平移两个字节，第四行平移三个字节。列混合是将一个特定的矩阵和每一列的向量都进行相乘，得到新的列
6. 这就是AES算法的全部过程

7. 分组密码算法的运行模式有哪些
   2. 有ECB(Electronic CodeBook mode)，CBC(Cipher Block Chainning mode)，CFB(Cipher Feedback mode)，OFB(output feedback mode)，CTR(CounTer mode)
   3. ECB：最简单的运行模式，将明文分成若干个64bit的明文块，每次用相同的密钥去加密。密文块可以分别独立解密，无顺序要求。
   4. CBC模式：使用初始向量和第一个分组异或，然后加密，之后的分组在加密之前都要和前一个分组的密文异或。
   5. CFB模式：将明文分成若干个64比特的分组。取一个64比特的移位寄存器，初值为一个随机的初始向量。首先对一个64比特的初始向量进行加密，得到64比特的密钥流，和明文的第一组进行异或，产生密文的第一组，然后将再次对刚刚得到的密文进行加密，再和下一组明文异或，这样不断进行下去，得到的每个单元的密文进行组合就得到了最终的密文。CFB模式对传输错误非常敏感，所以应该有完整性保护。
   6. CTR模式：将明文分组，每组64bit。有一个随机向量和计数器，分别为32bit，两个合在一起得到64bit的随机向量。首先将随机向量通过密钥进行加密，然后和第一组明文异或得到第一组密文。之后随机向量通过计数器加1，再通过密钥加密，然后和第二个分组得到第二组密文，依次得到所有密文。
8. 什么是OTP
   OTP是一次性密码，是一种只能使用一次的密码，随机密钥长度大于或等于明文长度具有完善保密性
9. 什么是流密码
   流密码是一种重要的密码体制，不同于分组密码将明文分成若干组去分别加密，流密码将明文消息按照字符或者比特逐位的进行加密，主要是使用高随机的密钥流去进行加密，大多是通过硬件实现的。
10. 密码学中，随机数有什么应用场景
    1. 生成密钥，用于对称密码和消息认证码
    2. 生成密钥对：用于公钥密码和数字签名
    3. 生成初始化向量，用于CBC，CFB，OFB模式
    4. 生成随机数，用于CTR模式
    5. 生成盐，用于基于口令的密码
11. 同步流密码和自同步流密码是什么

1. 同步流密码是一种每个比特都依赖于相应密钥比特的密码系统，需要在加密和解密时使用完全相同的密钥流
2. 自同步流密码是密钥流不需要完全同步的密码系统，在自同步流密码中，密钥流的生成不仅依赖于密钥本身，还依赖于先前的密文比特。
3. 一般在可靠信道传输时使用同步流密码，不可靠信道传输时使用自同步流密码
4. CFB属于自同步流密码，CTR属于同步流密码

12. 什么是LFSR
    LFSR是线性反馈移位寄存器，由n位的移位寄存器和反馈函数组成的，其中反馈函数是线性函数。当移位寄存器右移时，最后一个存储单元的值输出，第一个存储单元由反馈函数的输出值填充，其中反馈函数通常是若干存储单元的异或得到
13. LFSR中，什么是m序列呢
    m序列是一种特殊的由LFSR生成的伪随机比特序列，他的周期是2的n次减1，也就是一个n级的LFSR的最大周期。他的反馈函数是一个特定的多项式函数，也即本源多项式
14. 知道n级LFSR的密钥序列，如何计算反馈函数
    取前2n个密钥序列，然后建立矩阵方程，即前n个密钥序列矩阵和反馈函数矩阵的矩阵乘的成绩应该为后n个密钥序列矩阵
15. RC4算法的基本原理
    RC4是属于对称密码中的流密码加密算法，密钥长度可变，面向字节操作。以一个足够大的S表为基础，对表进行非线性变化，产生密钥流。其主要步骤分为，初始化S表，密钥流的生成
    初始化S表首先对S表进行线性填充，一般是256个字节，然后用种子密钥填充另一个256字节的K表，之后用K表对S表进行初始置换，就得到了S表。
    密钥流的生成就是通过密钥调度算法对S表进行各种变换，最后得到了一个伪随机数序列，就是作为密钥流。
    最后用这个密钥流和明文进行异或就得到了密文
16. 哈希函数的性质
    1. 确定性：它可以根据任意长度的消息计算出固定长度的散列值
    2. 抗修改性：输入的轻微的改变也会导致输出的哈希值发生巨大的变化
    3. 抗碰撞性，对于两个不同的输出，发生哈希值相等的情况的概率很小
    4. 唯一性，消息不同，散列值也不同
    5. 单向性，只能从消息计算得到散列值，而不能从散列值反推得到消息
17. 哈希函数可以用来干什么
    1. 用于基于口令的加密
    2. 用于构造消息认证码
    3. 用于进行数字签名
    4. 用于构造伪随机数生成器
    5. 用于构造一次性口令

18. 举出几种哈希函数算法
    MD4, MD5, SHA系列算法
19. 举出对哈希函数的攻击方式
    暴力破解，生日攻击
20. 什么是生日攻击
    生日攻击是利用生日悖论进行的攻击，攻击者可以生成多个输入，然后用哈希函数进行处理，然后查看是否具有相同的输出，也就是是否发生了哈希碰撞。这样就可以在不改变哈希值的基础上对信息进行修改
21. 介绍一下SHA-256算法的具体步骤
    1. 对消息进行补位处理，使得最终的长度是512位的倍数
    2. 以512位为单位将消息分成若干块，拆成16个32比特的消息，然后通过循环右移和异或扩充为64个32比特的消息
    3. 用初始的8个哈希值对每一个512位的消息块进行加密，得到新的8个哈希值，这样循环下去，当每一块都通过加密之后，得到的就是最终的哈希值
22. 散列函数和消息认证码之间的区别
    1. 哈希函数是通过对输入的数据进行加密，转化为固定长度的输出数据，用来验证消息的完整性，一致性
    2. 消息认证码通过输入数据和共享密钥的加密来对消息的完整性和真实性进行验证。
    3. 哈希函数主要用于数据完整性验证方面
    4. 消息认证码主要用于身份验证
23. 可以通过什么方法来实现消息认证码
    1. 使用SHA-2之类的哈希函数实现消息认证码
    2. 使用AES之类的对称加密算法来实现消息认证码，使用CBC模式，将前面生成的密文全部抛弃，只留下最后一部分的密文作为MAC值
24. 消息认证码的攻击目的是什么
    1. 密钥恢复攻击，用来找到用户的密钥
    2. 伪造攻击，用来在未知密钥的情况下伪造未经认证的消息和认证码
25. HMAC计算MAC值的步骤
    1. 首先将密钥填充为一个哈希函数的分组的长度
    2. 然后将填充后的密钥和ipad的比特序列进行异或运算，ipad是一个特定的比特序列
    3. 然后将运算后的值和消息进行组合，放在消息的开头
    4. 将组合后的值输入到哈希函数，计算出哈希值
    5. 将上面填充后的密钥和opad的比特序列进行异或运算，然后后面拼上上一步得到的哈希值
    6. 将最后得到的这个哈希值再次输入到哈希函数中，计算得到最终的哈希值，也就是MAC值

26. 请介绍一下RSA加密算法的基本加密步骤
    1. 首先取两个不相等且足够大的质数p和q
    2. 然后计算p和q的乘积n
    3. 之后计算n的欧拉函数ϕn。
    4. 取一个和ϕn互质的整数e
    5. 求出e对于ϕn的模反元素d
    6. 然后公钥就是e和n的组合
    7. 私钥就是d和n的组合
    8. 加密时明文的e次方 mod n便是密文
    9. 解密时密文的d次方 mod n便是明文
27. 请说几种公钥加密的攻击方式
    1. 中间人攻击
    2. 选择密文攻击
28. 介绍几种公钥密码
    1. RSA
    2. Rabin
    3. 椭圆曲线密码
29. 相比于公钥密码，对称加密密码有什么缺陷呢
    1. 当用对称加密算法加密后，必须要将密钥告知接收方，而在传输密钥的过程中，可能会有风险
    2. 当在一个多人网络中需要两两用户安全通信时，如果采用对称加密，那么密钥的数量将会很多
    3. A收到B的文档时，无法证明这个文档确实来自B
30. 说明用公钥加密传输数据的过程
    比如Bob想要给Alice发送一个消息，然后他让Alice生成一段公钥和私钥，私钥由Alice自己保存，公钥发送给Bob，Bob用公钥加密他要准备发送的消息，然后将密文发给Alice，Alice收到密文之后用私钥就可以解锁密文得到明文
31. 数字签名的算法有哪些
    1. RSA算法
    2. DSA算法
    3. 椭圆曲线数字签名
32. 介绍一下秘钥分发的步骤
    这里介绍一下NS密钥分发协议的步骤
    1. 首先，A向KDC发送请求，要求和B通信，同时发送一个随机数
    2. KDC向A发送会话密钥，B的ID，之前A向KDC发送的随机数和一个证书的加密信息，用A和KDC的共享密钥加密。那个证书是用B和C的共享密钥加密后的会话密钥和A的ID
    3. A解密信息，然后向B转交证书

4. B解密证书，并且向A发送一个用会话密钥加密后的随机数
5. A相应B的请求，并且将随机数减一，用会话密钥加密后再发送回B

33. 什么是数字证书
    数字证书是一种工具，用来证明自己的身份和数据的真实性。数字证书中包含了一个人或组织的公钥及其相关信息，包括证书名称，过期日期等，由可信任的第三方机构签名为凭证，通常用于网站认证，电子邮件加密和安全连接等。
34. 什么是PKI
    PKI是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员策略和规程的总和
35. 密码分析主要有哪几类，他们的含义是什么
    1. 唯密文分析：密码分析者取得一个或多个用同一密钥加密的密文
    2. 已知明文分析，除要破译的密文外，密码分析者有用同一密钥加密的明密文对
    3. 选择明文分析，密码分析者可取得他所选择的任何明文所对应的密文，这些明密文对和要破译的密文是用同一密钥加密的
    4. 选择密文分析，密码分析者可取得他所选择的任何密文所对应的明文，这些密文和明文是用同一密钥解密的
36. 什么是PRG，介绍几个你知道的PRG算法
    PRG是伪随机数生成器，通常就是给他一段短的种子密钥，然后可以按照一定的算法生成一段很长的随机序列。常用的PRG有
    2. 线性同余法，用线性方程来产生数字序列，已经被淘汰了
    3. Salsa20
37. 流密码加密有什么优势和劣势
    1. 优势
        1. 加密速度快
        2. 适用于大量或少量的数据，不用进行分组
    2. 劣势
        1. 同一个密钥不能重复加密
        2. 需要高质量的PRG，否则密钥会被预测
        3. 当对特定位置经过修改之后可能会被探测到
38. 什么是循环冗余校验
    循环冗余校验是一种检测数据传输过程中是否出现错误的技术，主要是利用除法还有余数的原理来实现校验的。产生一个固定的校验码，跟在数据的后面，用来判断数据是否出错
39. 什么是MAC消息认证码
    MAC消息认证码是通过特定的算法来让一段数据产生一段特定的信息，然后用这段信息来检测数据的完整性，同时也可以进行身份的验证。MAC消息认证码包含两个算法，分别是签名算法和认证算法。具体的方法有CBC-MAC和HMAC等
40. CBC-MAC的基本步骤是什么呢
    主要是利用分组密码和CBC模式去构建消息认证码。具体来说就是选择一种分组密

码算法，然后将消息分成若干组m0, m1, m2到mn，然后首先m0进行加密，之后的密文和m1进行异或之后加密，以此类推，最后mn的密文再加密的密文再进行截断就是消息认证码，之前所有的密文都可以丢弃。

41. 什么是哈希函数
    哈希函数就是把一个任意长度的数据映射为固定长度数据的函数，可以用来检测数据的完整性，判断两个数据是否相等等，常用的哈希函数有MD5，SHA-256等
42. 单向陷门函数和单向函数的区别
    单向函数不能用来加密，因为无人可以解开它
    单向陷门函数不是单向函数，只是对于不知道陷门的人表现出了单向函数的特性
43. 密码学的目标是什么
    密码学的目标主要有五个，即
    1. 保密性
    2. 认证性
    3. 完整性
    4. 不可否认性
    5. 可用性
44. 哈希函数需要满足的安全目标是什么
    1. 单向性：对于任意给定的消息，计算它的哈希值很容易，但是从哈希值反推消息不可行
    2. 弱抗碰撞：对于给定消息，要找到另一个和这个消息的哈希值一样的消息是不可行的
    3. 强碰撞性：找到两个任意哈希值相同的消息是不可行的
45. 说明混淆和扩散的定义，还有他们的作用
    混淆和扩散是设计密码体制的两种基本方法，目的是为了抵抗对于密码体制的统计分析。混淆主要是为了让密文和密钥的关系更加复杂，扩散是为了让明文和密文的关系更加复杂
46. 什么是SPN结构
    SPN结构也就是代换置换网络，是一种分组密码的结构，在AES中用的就是SPN结构。
47. 什么是Feistel结构
    Feistel结构是一种对称密码结构，是最广泛的分组密码结构之一，在DES算法中运用的就是Feistel结构，具体结构是明文分成两个部分L0和R0，一次循环中L1等于R0，R1等于R0经过加密函数然后和L0的异或，依次进行。
48. 保密系统满足的安全性假设是什么
    这些假设包括：密钥是随机的，攻击者无法获得密钥，攻击者无法获得明文，攻击者无法获得密文，攻击者无法获得加密算法细节等
49. 为什么分组密码和流密码都要保证(IV, K)不重复使用
    因为如果重复使用的话，攻击者可以通过分析加密结果，推算出密钥，从而破解加密。

50. 密码系统安全性的定义有几种，分别是什么
    密码系统安全性的定义主要有两种，分别是基于信息论的方法和基于计算复杂性理论的方法
    1. 基于信息论的方法关注点在密文中是否含有任何明文的信息，如果密文中不含有明文的任何信息就是安全的
    2. 基于计算复杂性理论的方法考虑是否在有效时间内能够将密文中蕴含的明文中的信息提取出来。
51. 介绍一下Diffie-Hellman交换协议的过程
    Diffie-Hellman交换协议是一个安全协议，可以让双方在完全没有任何预先信息的条件下通过不安全信道建立一个密钥，具体过程是这样的：
    1. 选取一个大质数p，再选取一个本原元a，这两个数是公开的
    2. U和V各有一个私有密钥xu和xv
    3. U向V发送信息a的xu次mod p
    4. V向U发送信息a的xv次 mod p
    5. 然后双方在对方发送的消息的基础上再加上自己的密钥的次方，再mod p，就得到了相同的密钥。
52. Diffie-Hellman交换协议有什么优缺点
    优点：
    1. 双方可以在事先没有协商的情况下在不安全的信道交换对称密钥信息
    2. 在通信结束之后可以丢弃密钥信息，没有保密的负担
       缺点：
       容易受到中间人进攻，所以需要可信服务中心的存在
53. 如何用哈希函数对长消息进行签名
    首先用哈希函数将一段长消息转换为一段短消息，然后再用数字签名算法对短消息进行签名。在认证时，首先将长消息转换成短消息，然后用公钥对上述的签名进行解密，看看两个短消息是否相同。
54. DES算法中S盒的作用是什么
    1. S盒主要是将48位比特的输入压缩为32位，当两个输入相差1比特时，输出相差2比特
    2. S盒是DES算法的核心，也是DES算法中唯一的非线性结构
55. DES算法和AES算法之间有哪些相似之处
    1. 两者的轮函数都是由三层构成的，分别是非线性层，线性混合层和子密钥异或层
    2. 他们都是分组密码，都对固定长度的块加密
    3. 都采用密钥扩展算法，都根据密钥生成若干个子密钥
56. 信息安全中常用的攻击有什么
    有中断，截取，篡改，伪造和重放
57. 什么是单表代换密码
    单表代换密码是一种替代密码，就是将明文中的每个字母按照一个固定的映射关系

表格进行替换。

58. 什么是多表代换密码

    多表代换密码是一种替代密码，就是有多个代换表，表中标识者每一个明文和密文的字母的一一对应关系，循环的利用这些表，就得到了密文。

59. 什么是数字信封

    数字信封是一种加密技术，用加密技术来保证只有特定的人才能阅读信息的内容。数字信封中，发送方首先用对称加密来加密信息，然后用收件人的公钥来加密密钥。加密后的密钥和信息被传输给收件人，只有通过收件人的私钥才能解密密钥，进而解密信息。