设计引言：不能陷入只造轮子不开车的情况，需要结合实战、新技术、新思路，增加这些内容的篇幅，同时不属于这部分的内容应该为其服务。

比如原理讲解，目的不是让你去搞数学，而是当你在遇到算法的时候，能分辨特征，识别是否被魔改，以及如果魔改了如何修复。所以讲解时应该重“手算”轻“原理”。

能不能从逆向的角度重新编排？？

0.AES 背景

主要知识点如下

需要注意的是，并非所以我会的东西，受众都是需要的，所以尽量讲他们需要的。

- AES 是 DES和3DES 的 后继者。

  AES 、DES的全称，DES和AES并非算法本身的名字，而是一种荣誉和标准。
- AES 是对称加密算法的典范和主流。
- AES 的基本特征，输入、输出。

1.AES 算法原理

主要知识点如下

- 密钥编排
  - 循环左移
  - S表替换
  - Rcon 异或

  手算AES 128以及256的密钥扩展表。

  种子密钥：用户输入的密钥

  轮密钥：各轮中使用的密钥

  密钥编排：由种子密钥计算出每轮的轮密钥的算法就叫密钥编排

  扩展密钥：所有轮密钥拼在一起

  这些概念有助于我们后续的交流和逆向中的理解。

- 明文运算
    - S表替换
    - 循环左移
    - 列混淆
    - 密钥xor

2.AES 与 DES 的区分

主要知识点

- 原理层面上两者的异同

  这篇讲的还不错 http://bristolcrypto.blogspot.com/2015/01/52-things-number-17-describe-and.html

  首先说联系，从某些方面上，你可以说aes和des很相近

  1.DES和AES都是对称加密算法，加解密都使用同一个密钥

  2.DES和AES都是分组加密算法

  3.DES和AES的运算整体上都可以分成密钥的编排和明文的运算

  4.DES和AES在密钥的编排中，都通过对密钥的处理生成一系列的“subkey”，即子密钥，且每轮运算使用一个。DES有16轮运算，在密钥编排中生成了16个子密钥。AES有10，12，14轮运算，也生成10，12，14个子密钥。都是一轮用一个。

  5.AES的10轮运算中，每轮经过四个步骤，第一步叫根据S盒查表替换，在一个16*16的S盒中查找。而DES中也存在S盒，但它是4*16的小S盒，共8个，而AES是一个大的S盒。第二步是循环左移，DES又或者哈希算法中都有它的痕迹。第三步不去说它，第四步和密钥异或，DES中同样有这一步。

  那么不同的地方有哪些呢?

  1.DES的分组长度是64比特，AES的分组长度是128比特.

  2.DES的密钥长64比特，AES的密钥有三种规格，128比特，192比特，以及256比特。

  3.在运算中，DES的运算的基本单元是比特，而AES运算的基本单元是字节（8比特），且组织成了矩阵的形式。

  4.AES充满了数论的知识，相比DES，AES是纯数学的产物。

  5.AES和DES的运算结构不同，DES基于Fesital网络，AES基于SPN。

  6.DES中有非常多的置换，AES没有。

- 如何确认加密方式为AES加密或者DES

  https://bbs.pediy.com/thread-170860.htm

  这个答案有两重

  第一重的内容是寻常意义上的，来自于冰冰老师的思路

  通过重放工具来确认是否是aes算法

  如果不管明文多少，密文始终是16个字节的倍数，那就是aes。通过重放攻击验证这一点。

  如果两个相同分组的输入，输出相同，那就是ecb，否则就不是ecb模式。

  第二重是反转

一个像序列密码的情况，结果竟是aes？这是怎么回事？？

AES 算法按字节加密

- FIndcrypt，S表。

  DES 和 AES 的S表显然不同嘛

算法的工作模式

ECB——将每个分组单独做处理，相同的明文输出相同的密文，有安全隐患

CBC——将前一个分组的密文与当前分组的明文进行异或，问题在于，第一个分组的明文哪来的"前一个分组的密文"，这就是IV的由来了。

CBC是最常见最常用的模式。

OFB等模式可以使之成为流密码，也不用填充。

3.AES工程实现

这部分反而是真的重点，因为look up table 的程度不同。

或者可以分为标准实现和查表实现两种

- tiny-AES-c
- Openssl
- Libtomcrypt
- 标准实现

4.AES 的逆向识别特征分析

https://tinyniko.github.io/2021/02/20/aes-enhance/

Findcrypt

我要提防自己的一种糟糕的倾向，忽略或者对较简单的部分不屑一顾的倾向。

原因有二

1是我会了，学员不一定会，我认为简单的部分可能对他很有帮助。

2是可以耗费一些时间。

5.实战分析

以KCTF 那道里面的AES为例（标准）

6.魔改AES

如何判断AES是否被魔改

如何修复魔改AES

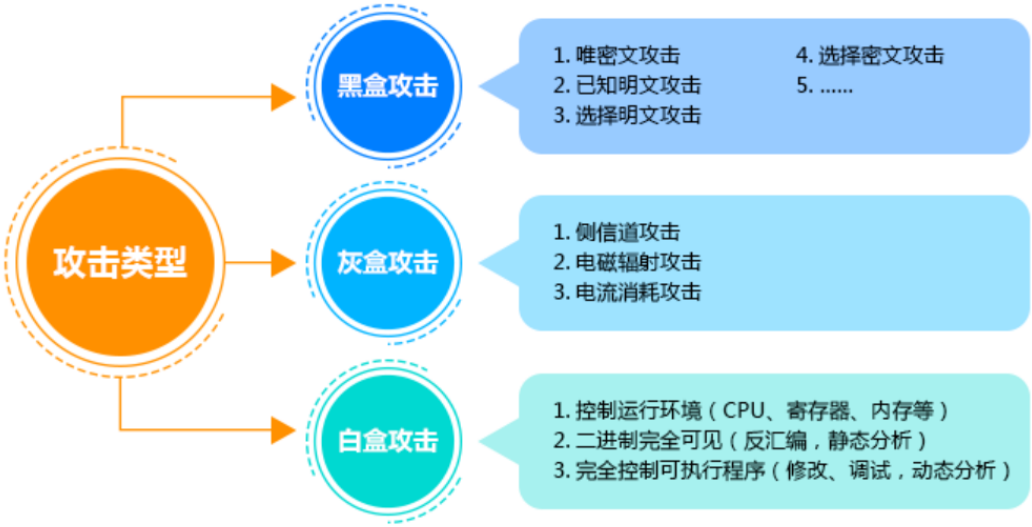
- 魔改S盒
- 魔改密钥扩展流程

7.AES 灰盒攻击

梆梆安全密钥白盒加密技术:

为解决在不直接暴露任何密钥或数据的前提下实现对数据加解密，梆梆安全推出密钥白盒加密保护技术，从根本上防护针对密钥的白盒攻击行为。

Lookup table转换 将密钥转换为大量的Lookup table，构造复杂庞大的结构化查找表系统。
随机双射编码 应用随机化、非线性化操作，对查找表进行随机双射编码，隐藏相关内容。
算法边界扩展 将加密算法边界由算法本身扩展到整个程序，实现对密钥的隐藏。
内外混编 采用外部编码加内部编码混合方式，对查找表进行隐藏、混淆和扩散。
多层防护措施 采用多种安全技术集成，增强对密钥白盒环境下非法调用、注入、内存修改的防护。



8.白盒AES

9.对白盒AES的攻击和分析