遇到一个样本——怎么判断是AES算法

AES 带符号的实现样本——怎么处理?

AES OPENSSL 实现样本————怎么处理? （两种）

学员给的样本 rong360,还附带了分组的知识呢

AES Cyptopp 实现样本——怎么处理?

https://github.com/BruceWind/CryptoPPInNDK/blob/master/jni/main.cpp

AES 的另一种实现，怎么处理? （SPBOX融合）

小红书

AES 正式样本——怎么处理? （tiny aes C）

编译的tiny aes C

AES 复杂样本——怎么处理? （真实样本，我的样本）

趣多多。

AES 魔改S盒——怎么处理?

AES 魔改密钥扩展算法——怎么处理?

美团。

咪咕疑似就是。确认

AES 魔改mixcolumn

靠，这需要一定数学功底了

如果没有数学功底，就简单的看，是否有"1B"和"80"

某AES变种题分析 | Live to change world (killshadow.xyz)

安恒二月月赛部分WP | Ronpa的博客

RCTF 2019 baby_crypto & baby_aes Writeup - 先知社区 (aliyun.com)

AES 白盒算法——怎么处理?

https://bbs.pediy.com/thread-266447.htm

如何判断AES 的工作模式?

比如这篇博客里，轻描淡写一句"后面黑盒测试了一下就是AES ECB模式的加密"

关于AES 相关的内容，冰冰有三节课

第一节课，AES 的介绍，比较失望

1/2 的内容在JAVA层，1/4 从表面粗略介绍AES，1/8在逆向分析tiny aes，1/8在讲findcrypt以及逆向特征。

我总结一下对我有用的

最朴素的，最强烈的AES 特征是S盒

看一下Findcrypt如何实现检测AES

比较奇怪的是，冰冰在des一节中讲了查表法，aes一节中没有讲，不知道为啥。

Stalker aes一节中

介绍了stalker 逆向分析 ollvm 化的aes

我认为和aes关系不大，主要是介绍stalker

怎么说呢，多了一个trace和分析工具吧。

和ida trace ，unicorn trace 同级的stalker trace，在某些场景下和trace natives 同级。

除此之外，我并不认为print是个自动化的好主意，如果检验是个地址就hexdump，否则直接打印，这是禁不住结构体考研的，不好用。

分组模式这一节，对我是有用的，1h值得看。