**0.AES背景**

**1.AES 算法原理**

《Rijndael 的设计》 设计者出的书

最原汁原味，最标准

《Fips 197》中英文对照版

AES 标准文档的英文版以及主体的中文翻译

比较好和详尽的中文介绍

AES加密算法的详细介绍与实现*TimeShatter的博客-CSDN博客*aes加密

《图解密码学》

其上关于工作模式的内容，图比较好看。

《对称密码学》

很好的书，数学原理比较深

S盒的设计原理

AES加密算法中的S盒及其C语言实现 - 道客巴巴 (doc88.com)

另两篇AES 的详解

https://zhuanlan.zhihu.com/p/78913397

https://zhuanlan.zhihu.com/p/41716899

AES列混淆 wiki

Rijndael MixColumns - Wikipedia

AES 看雪图解

https://bbs.pediy.com/thread-90722.htm

AES 算法细节 题目

https://blog.csdn.net/Akatsuki__Itachi/article/details/94396771

AES 详解：原理+实践

https://github.com/matt-wu/AES

flash aes 非常好

http://flashplayer.fullstacks.net/ （播放flash）

Python版本的AES 密钥扩展流程，很清晰好懂，用于看256位密钥如何处理

https://github.com/arsenalahm/AES-Encryption/blob/41df3d7e1731d0a73424f9271cbc677983147ff4/AES.py#L47

AES 理论结合实践，文档出乎意料的好，讲了不少工程化实现中的look up table

https://bbs.pediy.com/thread-188428.htm

AES 的数学基础——感兴趣的可以去研究一下

主要是线性代数以及抽象代数

2.AES 与 DES 的区分

http://bristolcrypto.blogspot.com/2015/01/52-things-number-17-describe-and.html

3.AES 工程实现

课堂演示——Python版本的标准AES实现

追踪与匹配，得益于好用的memory view——tiny aes C

除此之外还有tiny aes ndk https://github.com/anonym24/Android-Tiny-AES-NDK/tree/master/app

OpenSSL aes 实现 ，非常难得，从openssl中抠出了aes

https://github.com/bozhu/AES-C

https://crypto.stackexchange.com/questions/34341/aes-size-of-t-boxes-and-obtaining-t-box-values

https://www.sciencedirect.com/science/article/abs/pii/S0141933115001945

根据算法描述的实现版本VS查表法

利用T表讲原先轮变换过程中列混淆中的较复杂的矩阵运算转变成简单的查表和异或运算。这种实现需要2-8KB的存储空间，但效率提高数倍。

朴素的说，查表法就是除了addroundkeys以外的三个运算整合到一起：

对于查表法实现，就是要将每一轮中的前三层操作(字节代换层、ShiftRows层和MixColumn层)合并为查找表。

白盒AES就是四合一。

**4.AES 特征识别**

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

勒索病毒aes实战

https://www.freebuf.com/articles/database/111756.html

**6.魔改AES**

- 魔改S盒，自己写
- 魔改S盒和密钥扩展，怎么办?
  https://bbs.pediy.com/thread-254678.htm
- 伪白盒，只对流程做了小的整合、

实战 咪咕SO

它的mixcolumn部分为什么是一张表？？？是魔改还是一种实现？？

**7.白盒AES**

必看的文章

A Tutorial on White-box AES

Python版本的白盒实现以及破解，必看

https://github.com/DavidBuchanan314/aes-playground

https://f5.pm/52409 必看的总结

白盒AES实例

[分享]分享个逆X梆vmp遇到变种aes源码-Android安全-看雪论坛-安全社区|安全招聘|bbs.pediy.com

https://github.com/Gr1zz/WhiteBoxAES C实现了论文中的白盒aes

https://www.bangcle.com/products/productindex?product_id=3 梆梆介绍白盒

一些论文在文件夹里

**8.对白盒aes的分析和攻击**

DFA 攻击白盒AES获取密钥

Differential Fault Analysis on White-box AES Implementations (quarkslab.com)

Unicorn模拟执行攻击获取密钥

https://www.anquanke.com/post/id/187028

https://www.anquanke.com/post/id/188340

AES白盒破解

https://tinyniko.github.io/2021/03/14/%E7%99%BD%E7%9B%92AES%E7%A0%B4%E8%A7%A3/

一种还原白盒AES秘钥的方法

https://bbs.pediy.com/thread-254042.htm

当发现一个SO可能是白盒SO时，权衡成本后，如果逆向分析无妄，可以采用主动调用

https://blog.csdn.net/tangsilian/article/details/106178660，这里面还总结了攻击白盒，破解密钥的几种手段。

黑盒调用

- Frida rpc
- Xposed + server
- unicorn

除了黑盒调用外，魔改算法或者白盒算法的最常规手段是扣算法，比如https://github.com/smallsun107/xhsShield/，小红书这个就是一个很好的例子。

在学习中，我们遇到了很多挺有用的小tips，但千万不要把小tips当真理。

AES 分组长度是 16个字节：

所以Frida重放攻击时，密文表现出了相关特征，就一定是AES 算法。

-------并不

TwoFish或者RC6以及其他参与到AES终赛评选的分组加密算法都符合AES的分组要求以及安全性，只是在各方面属性上比不过Rijni算法。

AES 分组长度是 16个字节：

所以Frida重放攻击时，发现不是16字节分组，就一定不是AES算法。

——并不

在AES算法设计和评选阶段，官方声称如果支持多种分组大小是一个加分项，所以Rij也设计并支持了192位或者256位分组大小。

因此你可能遇到一个32字节分组的Rij算法，它不在AES标准里，但确实是Rij算法，而非魔改。

Frida重放攻击时，密文表现的像一个序列密码，并不向某个分组靠齐，看来是一个序列密码或者叫流密码吧？

RC4 - CyberChef (gchq.github.io)

——并不

也可能是AES算法，只不过采用了CFB或者xxx模式，这两个模式可以将分组密码转成流密码。

AES中最标志性的特征是S盒，SO中找不到S盒，一定不是AES算法吧？

——并不

S盒既可以魔改，也可以通过程序生成。

魔改eg

生成eg

FIndcrypt没说有AES，应该没有吧？

——并不

理由同上。

S盒里的256个数，我一个个对了，是标准的，S盒既然没动，应该没魔改吧？

——并不

比如美团。

我真的得懂那么多密码学知识才能逆向SO吗？

——并不

你也可以C和C++很6，拼着经验把F5代码直接全部抠出来，不用懂太多算法

，但相比起来，学好密码学更简单呢。比如AES，我带着你，你几天就能掌握的七七八八，我不带你，一两周也能搞定，但绝对不会这么有体系化，这么细。

我工作中并未遇到这么难的，符号名都很清晰，Hook一下就全部出来了，你说的这些各种实现，魔改，对我有帮助吗？或者说在真实样本中多吗？

多，实在太多了。

美团样本就是很好的例子。

遇到一个涉及魔改aes的样本，我该怎么去分析它呢？

Clion + Frida/AndroidNativeemu

我在SO中既没有找到S盒也没找到T表，这一定不是一个AES。

——并不

正如S盒可以动态生成，不管是否是标准S盒，T表也可以动态生成。

除此之外也可以只有T表无S盒，因为T表由S盒生成以及其余几个步骤生成，每个T表中都可以算出S盒，以T0为例。

然后就是开始搞样本呢！

最简单的例子——rong360，带符号。

属性：openssl，EVP