ctf xor题_2016 HCTF Crypto 出题总结

原创

weixin_39935257 于 2020-12-19 14:37:40 发布 332 收藏
文章标签： ctf xor题

Author：Hcamael

date： 2016-11-28 20:26:26

今年犯懒了所以只出了3题RSA的密码学题目, 出题思路来源于协会上一届的学长 @Mystery Of Panda 关于RSA后门的毕业设计.

Crypto So Interesting

出题时预测的分数在300分左右, 不过看完选手的wp后发现这题出现了重大失误, 现在来看, 这题只值150分左右, 但是实际情况只有23个队解出了该题.

本题思路来源: 基于隐藏指数的RSA-HSDβ算法, 全称为隐藏小私有指数δ的RSA后门密钥生成算法.

该算法依赖于wiener小指数攻击方法

后门生成流程:

其中β是在2^(k-1) ± 2^(k/2)范围内的素数, 转置函数的作用是在β非常大的情况下, 返回值可以认为是PRP(Pseudo-Random Permutation). 转置函数可以有好几种形式, 我选取的是一种比较简单的转置函数.

从上面的流程可以看出这题非常的简单, 要逆向也是很容易的, 所以该题为本届HCTF密码学的签到题

逆向思路:

从上图可以看出本题只涉及到了wiener算法, 难度差不多是150左右

原本设计着算出(ϵ, δ)后, 根据(ϵ, δ, n)分解出q和p, 但是出题失误, 导致只需要wiener算法就能getflag

PS2: 基于隐藏指数的RSA后门生成算法除了本题涉及的还有RSA-HSPEβ和RSA-HSEβ

Crypto So Cool

出题时预测的分数在400分左右, 实际情况只有7个队解出了该题. 和预测差不多, 最后放了一波hint, 要不然可能会更少.

本题思路来源: 基于隐藏素数因子的RSA-HPβ算法

该后门算法依赖于Coppersmith partial information attack算法, sage实现该算法

后门生成流程:

该算法的核心在于把p的前半部分比特隐写到n中

τ的长度为k/16比特

μ的长度为5k/16比特

λ的长度为5k/8比特

所以n的长度为k比特

p * (q xor random(k/8比特长度))的前3k/8比特的值是不变的

所以可以成功把τ, μ隐写到n中

逆向思路:

该题的难点主要在于Coppersmith partial information attack算法, 能在放hint前做出的队伍都是在github上找到了该算法的脚本 https://github.com/Gao-Chuan/RSA-and-LLL-attacks

Crypto So Amazing

payload:

出题时预测的分数在450分左右, 不过却没有能做出来, 我知道的几个队都是被上一题的脚本给坑了

本题思路来源: 基于有限域F(2^m)上椭圆曲线的RSA后门生成算法

流程图懒得画了, 上一题的后门算法看懂了, 这题去看代码也不难, 主要是通过Diffie–Hellman key exchange算法生成私钥作为种子生成伪随机数, 私钥很好求, 本题的难点跟上题一样同样在于Coppersmith partial information attack算法

但是这题已知p的前576bit, github上的那个脚本就跑不出来了

这部分是出题时无意间挖出的坑, 因为我并不知道github上的这个脚本, 在我预想中能做出rsa2的基本都是能做出rsa3的

这题还有一个坑点

sage和python 用相同的seed生成的随机数不一样, 所以在payload中我使用了python生成随机数

总结

本届HCTF的Crypto计划的考点是Coppersmith partial information attack算法和Riemann's hypothesis and tests for primality算法, 不过无奈由于出题失误第二个算法没考成

RSA后门相关的论文可参考:

Crépeau C, Slakmon A. Simple backdoors for RSA key generation[J]. Topics in Cryptology—CT-RSA 2003, 2003, 2612: 403-416.

Young, A., Yung, M. A Space Efficient Backdoor in RSA and its Applications[J]. Preneel, B., Tavares, S. (eds.) SAC 2005, 2005, 3897: 128-143.

Tzung-Her Chen, Tsung-Hao Hung. A Comprehensive Study of Backdoors f or RSA Key Generation[R]. Cryptology and Information Security Conference, 2010.

本文作者：清枫