CTF-Training Week3 Crypto

原创

Luminous_song 于 2020-10-25 14:43:19 发布 60 收藏

Crypto 密码学

数学、密码学、以及脑洞

Encrypt & Decrypt

- 古典密码
- 对称加密（流密码/块加密）
- 非对称加密
- 其他

古典密码

- 前置知识：
  - 几大类古典密码：
    - 单表代换密码：每个明文字母都有一个密文字母进行对应，攻击者可能通过观察某些密文字母出现的频率来猜测其对应的明文。
    - 栅栏密码：利用明文字母的排列组合进行加密
    - 维吉尼亚密码：用字符串作为密码，按照字符串中每个字符在字母表中的次序对明文进行循环加密
- 入门级：凯撒密码（cyberpeace）
  - 通过单纯的移位来完成加解密：
- 入门级：栅栏密码（cyberpeace）：
  - 通过特殊规则来完成加解密

对称加密：加解密同密钥

流加密

```
明文流与密钥流长度相同
```

密钥

```
一个分组密钥可以加密多块数据
```

成长级：

```
阅读伪代码，看出这是什么加密方式，并编程实现他的功能
```

非对称加密：加解密不同密钥

- 前置知识一：
  - 非对称加密相对于对称加密的一个最大的不同在于：它的加密和解密使用的密钥不同，RSA ECC
- 前置知识二：
  RSA加密原理

例题：

```
1. 已知五个数中的四个，利用gymp2算出私钥和明文

2. 得到两个n，求最大公约数，是p*q中的一个
```

其他类型

推理类型

编解码类型

练习题目

1. **MD5【易】**

   本题非常简单，题目大意为给定一个 md5 值，然后找出明文， md5 爆破即可。

2. **Caesar【易】**

   凯撒密码

3. **Railfence【易】**

   栅栏密码

4. **easy_RSA【易】**

5. **Normal_RSA【易】**

6. **幂数加密【易】**

7. **fanfie【难】**

   混合加密+仿射密码

8. **easy_ECC【难】**

   需要编码，考察对椭圆加密公钥算法的理解，需要对 ECC算法具有一定的了解，然后编程实现。