l春秋—— Crypto Write up(一)

原创

Sn0w/ 于 2019-07-14 17:58:11 发布

分类专栏： CTF_Writeup 文章标签： Crypto

前言：密码学涉及一系列的加密算法，虽然自己数学贼烂，但觉得加密这些算法还是蛮好玩的，就通过题来了解一些算法，话不多说，开始做题。

Substituted

方法：百度翻译题目一下，Substituted（替换），**替换加密**中包含有**简单替换密码**，应该就是简单替换密码，在线网站求解一波。

替换密码解密

把头部改成iceCTF即可得出flag。

做题总结：通过这道题来了解一下简单替换密码

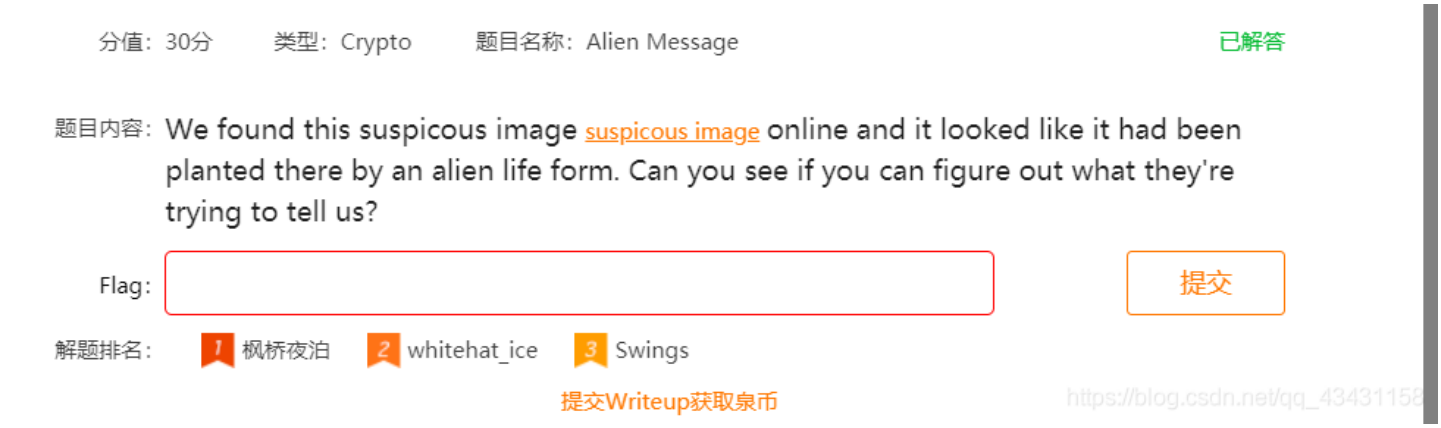
> 替换密码属于简单对称加密，即将字母表中一个字符替换成另一个字符，很好理解。

```
例如：
 明文 ABDDD
 替换规则：
A->C
B->T
D->F
密文 CTFFF
```

> 而攻击方式也有很多种
> 一、暴力破解
> 二、字母频率分析
> 因为替换密码只不过是从一个字符换成另一个字符，我们只要将出现在密文的所有字符出现的频率统计一下，看频率最高的。由此我们可以推断出，频率高的肯定是英文语言中最常用的一个字母的替换字母。密文中字母的频率分布与给定语言有着紧密的联系，即使在相对较短的密文中也成立。

参考大佬的博客进行学习关于替换密码详解

Alien Message

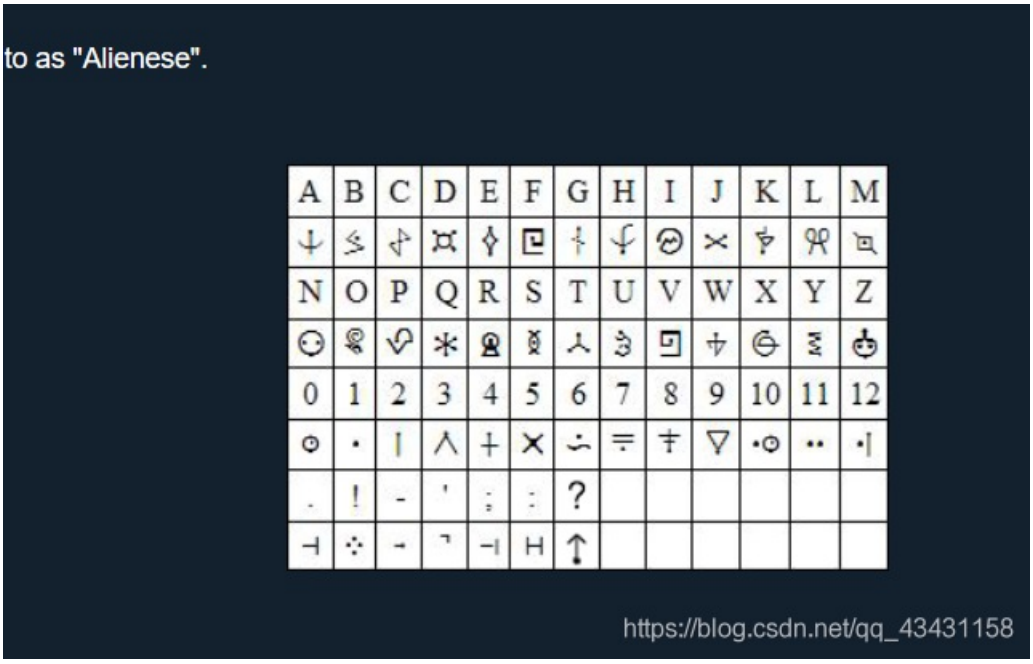


一张外星语言图片

方法：谷歌识图，查到对应的表，手动对照即可，但是flag格式有毒，大小写格式问题

查找该图片的其他尺寸：
全部尺寸 - 中尺寸

可能相关的搜索查询： ***futurama alienese messages***



做题总结： 一开始拿到这个题，以为是图片会隐藏信息，用做杂项的方法尝试了但都没用，最后又学到了一招，**百度识图或谷歌识图**，有时也可以解决问题，也算了解了一种新的做题方法。

回旋13踢

分值：50分　　类型：Crypto Basic　　题目名称：回旋13踢　　已解答

题目内容：看我回旋13踢
synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

Flag:　　提交

解题排名：1 截爱的海盗　2 dolo　3 z离人梦

方法：根据题目和提供的格式推断出是ROT13(回旋13)，在线解密即可得出flag
在线解密

做题总结：一开始真的是一脸懵，完全没有思路，只能查百度谷歌，查到了ROT13编码，所以就通过这个题来了解一下ROT13加密。

> ROT13（回转13位）编码是凯撒加密的一种变体，只对字母进行编码（对数字、空格等无影响），用当前字母往前数的第13个字母替换当前字母即可
> 例如：A->N,B->O,C->P等

a	b	c	d	e	f	g	h	i	g	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	g	k	l	m

除此之外，还有ROT5,ROT47

> ROT5 只对数字有效，用当前数字往前数的第5个数字替换当前数字即可。

> ROT47：对数字、字母、常用符号进行编码，按照它们的ASCII值进行位置替换，用当前字符ASCII值往前数的第47位对应字符替换当前字符，例如：当前为小写字母z，编码后变成大写字母K，当前为数字0，编码后变成符号_，用于ROT47编码的字符其ASCII值范围是33－126。

接下来了解一下非对称加密和对称加密

①：**非对称加密**，即加密和解密不是使用**同一套规则**，之前的对称加密解密中，使用的都是**同一个密匙**，如果在传输中被拦截，破解的几率会很高。
②：**非对称加密**，加密和解密使用的**不是同一个密匙**，明文A通过公钥B加密，加密后的明文和公钥一起传输，接收方接收密文后用私钥C(只有接收者才有)解密，这样的加密解密的方式非常安全，即使公钥和密文在传输过程中被拦截了，拦截者没有私钥，就算拿着公钥和密文也无法破解出明文。因此相较于对称加密，非对称加密会更加安全。

了解完对称加密和非对称加密后，就来学习一下**RSA算法**

在了解RSA算法之前，要先了解一下质数和互质数等数学概念，方便更好的理解RSA算法。

> 质数：一个大于1的自然数，除了1和它本身外，不能被其他自然数整除（除0以外）的数称之为质数(素数)。
> 互质数：公约数只有1的两个数。
> 判断互质数：
> ①任意两个质数一定构成互质数
> ②大数是质数的两个数一定是互质数（如97与88）

> 欧拉函数：任意给定正整数n，计算在小于等于n的正整数之中，有多少个与n构成互质关系？计算这个值的方法就叫做欧拉函数，以φ(n)表示.（计算互为质数的个数）

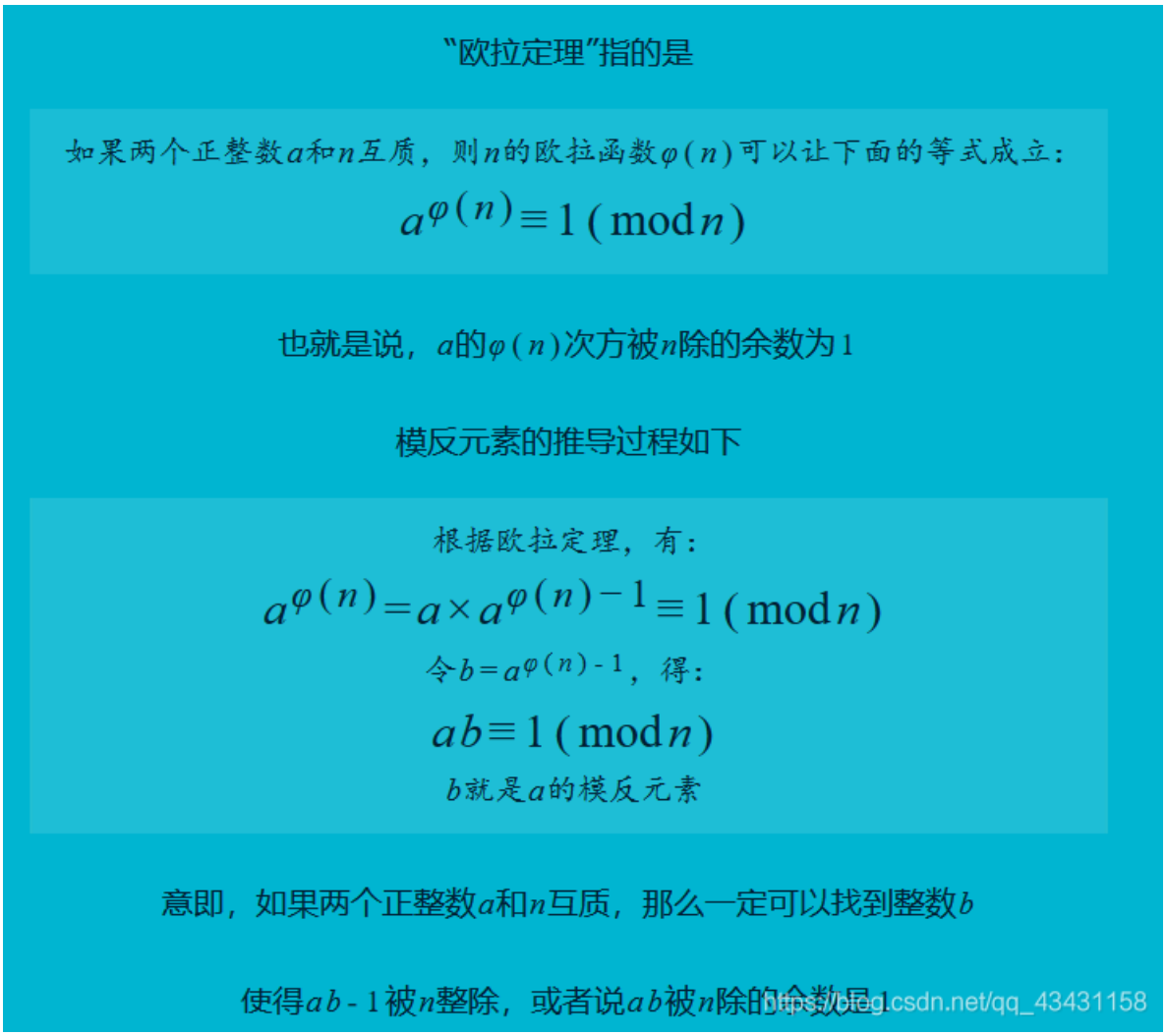
```
例如：
n为10，则与1、3、5、7、9互质，所以ϕ(n)=5
注意这里10不是质数，只算与其互质的。
```

在RSA算法中，欧拉函数对以下定理成立

1. 如果n可以分解成**两个互质的整数之积**，即n=p×q,则有`ϕ(n)=ϕ(pq)=ϕ(p)ϕ(q)`；
2. 根据“**大数是质数的两个数一定是互质数**”可以知道：一个数如果是质数，则小于它的所有正整数与它都是互质数；所以如果一个数p是质数，则有：`ϕ(p)=p-1`
3. **φ(n)=(p-1)(q-1)**

```
例如：
定理二：
n=33,q=3,p=11,n=p*q
p、q均为质数，所以只要是小于自己本身的都是互质数，因此才有如下公式
ϕ(p)=(p-1)//(-1)是为了去除本身，得出与其互质的个数
ϕ(q)=(q-1)
所以：
ϕ(33)=（3-1）*（11-1）=30
```

除此之外，还需了解一下**欧拉定理与模反元素**



概念清楚过后，就来梳理一下**生成密钥对的流程**

1. **随机选择两个不相等的质数p和q，p与q越大则越安全** 选取p和q
2. **计算p和q的乘积n** 计算出n的值
3. **计算n的欧拉函数值，即φ(n)=(p-1)(q-1)** 计算出ϕ(n)的值
4. **随机选择一个整数e，条件是1<e<φ(n)，且e与φ(n)互质** 得出e的值
5. **计算e对φ(n)的模反元素d** 计算出d的值
6. **将(n,e)封装为公钥，(n,d)封装为私钥** n的长度就是密钥长度

公钥	n：质数p和质数q的乘积，e：与φ(n)互质
私钥	n：同公钥n，d

m为明文，c为密文

加密	$c = m^e \bmod n$
解密	$m = c^d \bmod n$

参考大佬博客学习了一波，真的是学到知识了。
黄映焜的博客园
一文搞懂 RSA 算法
RSA算法使用介绍
RSA算法流程
RSA练习

这次就先学习到这里，下次就开始练习RSA题目。