

一 数据的机密性

实验目的

- 1、掌握程序设计中加密算法的使用方法；
- 2、理解弱与不安全加密算法攻击可能带来的风险；
- 3、掌握数据安全策略。

实验环境

- 1、连接互联网的计算机；
- 2、Python 等程序编译环境。

实验原理

1. RSA 加密算法

(1) RSA 加密算法的背景

1977 年，三位数学家 Rivest、Shamir 和 Adleman 设计了一种算法，可以实现非对称加密。这种算法用他们三个人的名字命名，叫做 RSA 算法。从那时直到现在，RSA 算法一直是最广为使用的“非对称加密算法”。非对称加密算法是指：

<1> A 生成密钥（公钥和私钥）。公钥是公开的，任何人都可以获得，私钥则是保密的；

<2> B 获取 A 的公钥，然后用它对信息加密；

<3> A 得到加密后的信息，用私钥解密。

即如果公钥加密的信息只有私钥解得开，那么只要私钥不泄漏，通信就是安全的。

(2) RSA 算法思想

RSA 的加密过程可以表示为(M:明文, C: 密文)：

$$C=M^e \bmod n$$

即 RSA 加密是对明文的 e 次方后模 n，其中关键的在于 e 和 n，所以(e, n)被称为公钥。

RSA 的解密过程可以表示为(M:明文, C: 密文)：

$$M = C^d \bmod n$$

即 RSA 解密是对密文的 d 次方后模 n ，其中关键的在于 d 和 n ，所以 (d, n) 被称为私钥。

算法流程：

<1> 选择 p 、 q ： p 和 q 都是素数，且 $p \neq q$ ；

<2> 计算 $n=pq$ ；

<3> 计算 $\varphi(n)=(p-1)(q-1)$ ；

<4> 选择整数 e ： $\gcd(\varphi(n), e) = 1$ ， $1 < e < \varphi(n)$ ；

<5> 计算 d ： $de \bmod \varphi(n) = 1$ ；

<6> 公钥： $KU = (e, n)$ ；

<7> 私钥： $KP = (d, n)$ ；

以下列较特殊的例子为例：设 $p=5, q=7$ ：

<1> $n=pq=5*7=35$ ， $\varphi(n) = (5-1)(7-1) = 24$ ；

<2> 由 $1 < E < \varphi(n)$ 且 E 与 24 互质，可取 $E=5$ ；

<3> $ed \bmod 24 = 1$ ，即 $5d \bmod 24 = 1$ ，可算出 $d = 5$ ；

<4> 即公钥 $(N, E) = (35, 5)$ ，私钥 $(N, D) = (35, 5)$ ；

假设需加密内容 $M=5$ ，则加密后 $C=Me \bmod N = 55 \bmod 35=10$ ，再对 C 进行解密，及 $M=C^d \bmod N = 10^5 \bmod 35 = 5$ 。

(3) Python 中 RSA 加密示例

代码清单 1.1 RSA 加密功能

```
#rsa公钥与私钥示例

import rsa

import base64

#生成公钥与私钥

(public_key, private_key) = rsa.newkeys(512)

# RSA加密

def rsaEncryption(public_key, cleartext):

    result = rsa.encrypt(cleartext.encode(), public_key)
```

```
        return base64.encodebytes(result)

# RSA解密

def rsaDecryption(private_key, ciphertext):

    result = rsa.decrypt(base64.decodebytes(ciphertext), private_key)

    return result.decode()

#输出公钥、私钥

print(public_key.save_pkcs1())

print(private_key.save_pkcs1())

cleartext = input("请输入明文:")

ciphertext = rsaEncryption(public_key, cleartext)

print("密文: ")

print(ciphertext)

decipher = rsaDecryption(private_key, ciphertext)

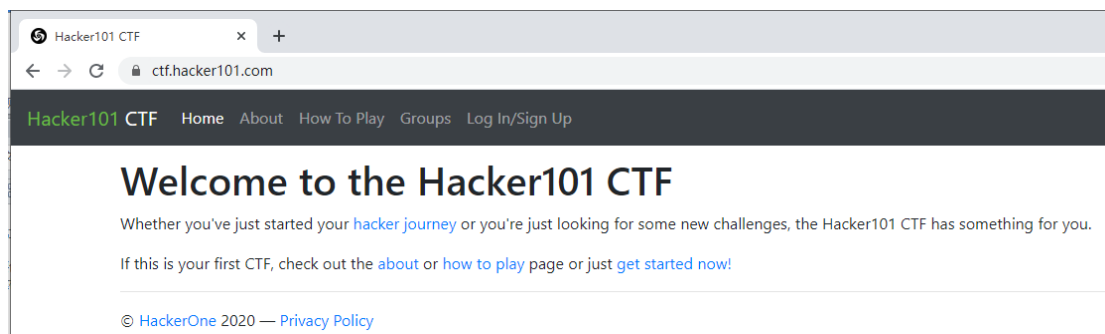
print("明文: ")

print(decipher)
```

2. 利用不安全加密算法删除帖子

(1) 系统登录

登录某 CTF 夺旗赛网站: <https://ctf.hacker101.com>, 网站首次使用需注册, **注意注册时用户名、密码勿包含个人隐私信息, 勿使用通用用户名和密码。**

图 1.1 <https://ctf.hacker101.com> 网站首页

(2) 项目选择

登录账户后在项目列表中选择“Postbook”项目，如图 1.2 所示为 Postbook 项目首页。

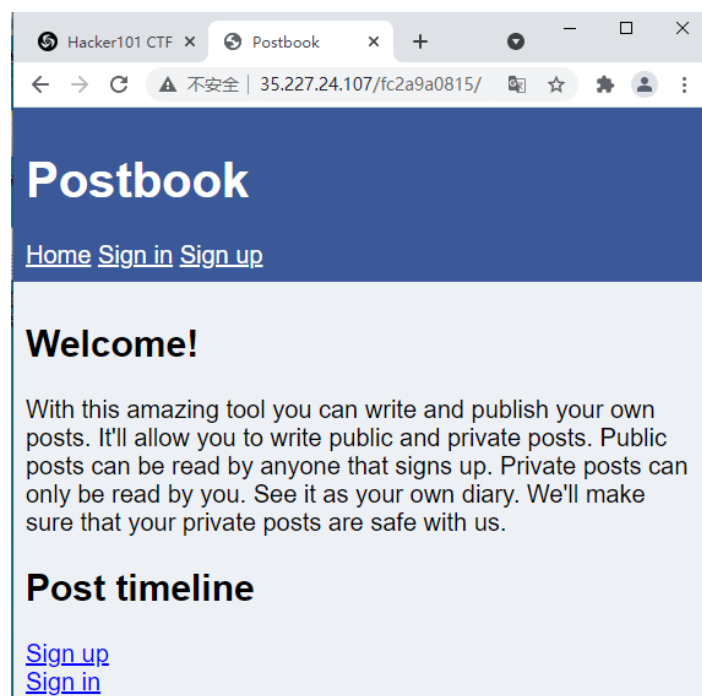


图 1.2 Postbook 项目首页

(3) 账户注册

单击“Sign up”注册两个账户，如本示例中注册 aaa/aaa, bbb/bbb.

(4) 帖子发布

登录 aaa/aaa 用户，并创建两个帖子，如图 1.3 所示为创建帖子结果.

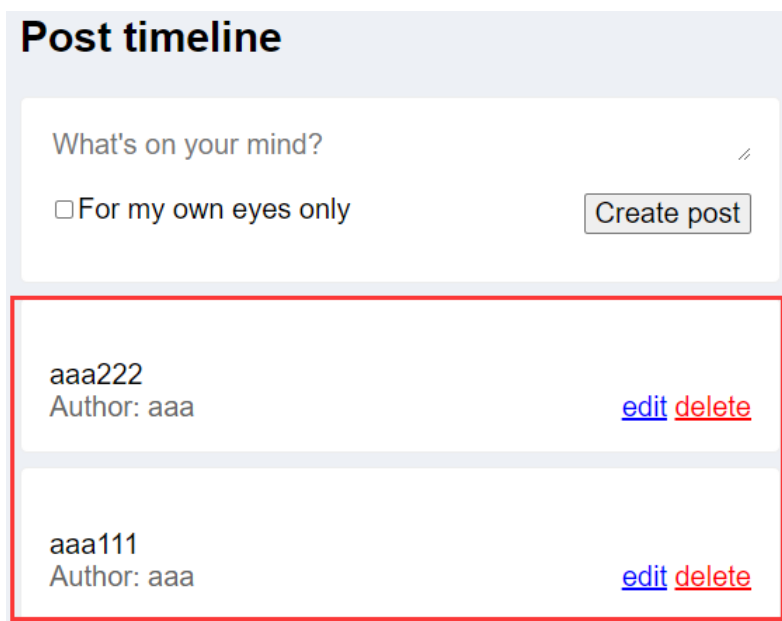


图 1.3 创建帖子

观察图 1.3 中新建帖子链接地址，可以查看新建帖子地址分别为“http://***/index.php?page=delete.php&id=a87ff679a2f3e71d9181a67b7542122c”与“http://***/index.php?page=delete.php&id=e4da3b7fbbce2345d7772b0674a318d5”；

(5) MD5 反查

搜索引擎中搜索“MD5 加解密”，并将上一步中“a87ff679a2f3e71d9181a67b7542122c”和“e4da3b7fbbce2345d7772b0674a318d5”放入 MD5 解密，解开原始值分别为 4、5。



图 1.4(a) MD5 反查



图 1.4(b) MD5 反查

(6) 越权删帖

尝试使用其他用户删除 aaa 用户删除的帖子。登录 bbb 用户，如图 1.5 所示，bbb 用户能看到 aaa 用户建立的帖子，但无“delete”删帖按钮。

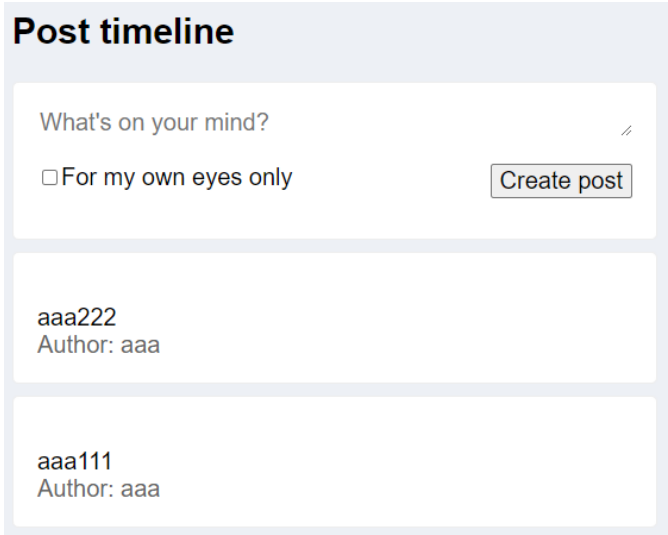


图 1.5 查看帖子

若 bbb 用户尝试删除 id=1 的帖子，可将“1”进行 MD5 计算，得到其 MD5 值为 c4ca4238a0b923820dcc509a6f75849b，用户可组合域名为“http://***/index.php?page=delete.php&id= c4ca4238a0b923820dcc509a6f75849b”（星号部分请自行替换），删除成功后，页面可获得 FLAG（代表删帖成功），同时，可看到页面中标题为“Hello world”的帖子已消失。

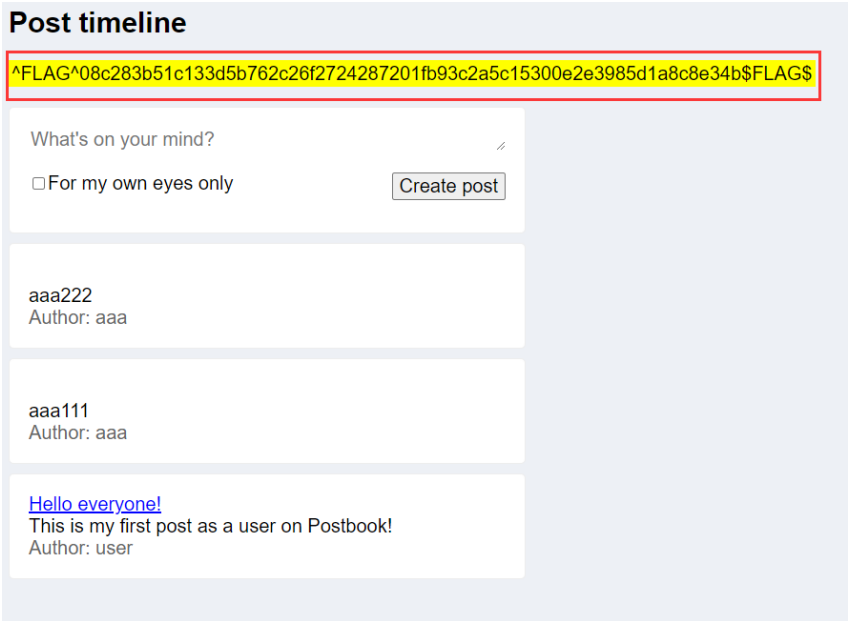


图 1.6 删帖成功

实验内容

- 1、运行实验指导书中的 RSA 加密程序，并对以上程序进行改进以提升其安全性，总结 RSA 加密算法优缺点（编程语言不限）。
- 2、在实验 1 的基础上，查询相关资料，利用国密算法（SM2）替换 RSA 加密。
- 3、在 PostBook 中新建两个用户，用其中一个用户新建帖子，并通过另一个用户利用帖子号采用不安全的加密算法漏洞删除系统中的所有帖子，并获得系统 FLAG。
- 4、查询相关资料对实验内容 3 中的安全问题提出改进方案。