HackerFrogs Afterschool Cryptography Basics 6

Class:
Cryptography

Workshop Number:
AS-CRY-06

Document Version:
1.75

Special Requirements:
Registered account at
picoctf.org

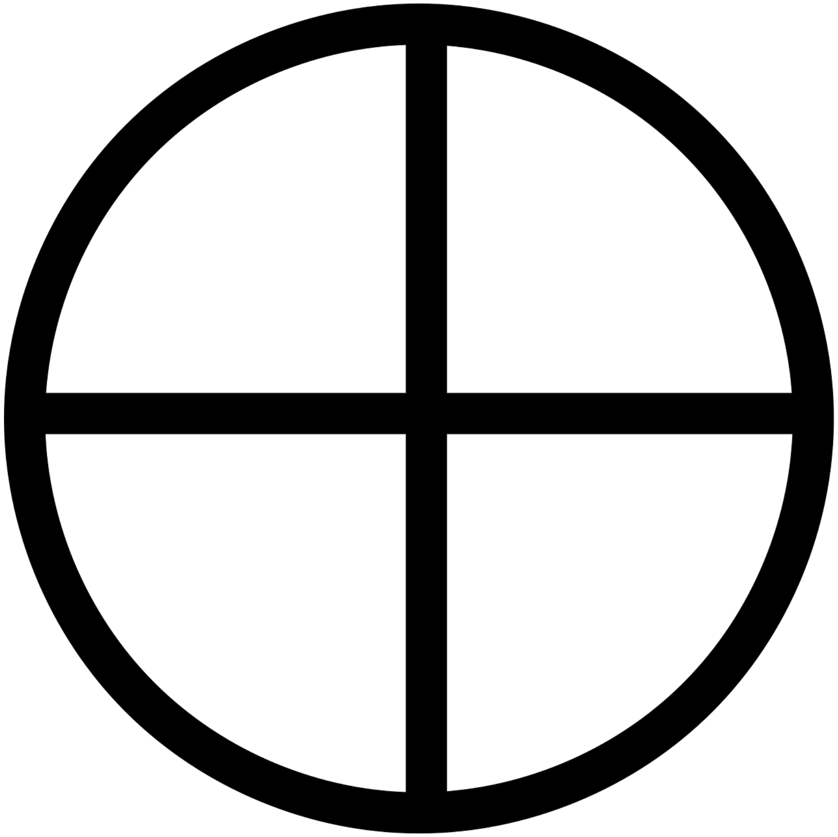
Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs! This workshop is the sixth and final session for cryptography basics

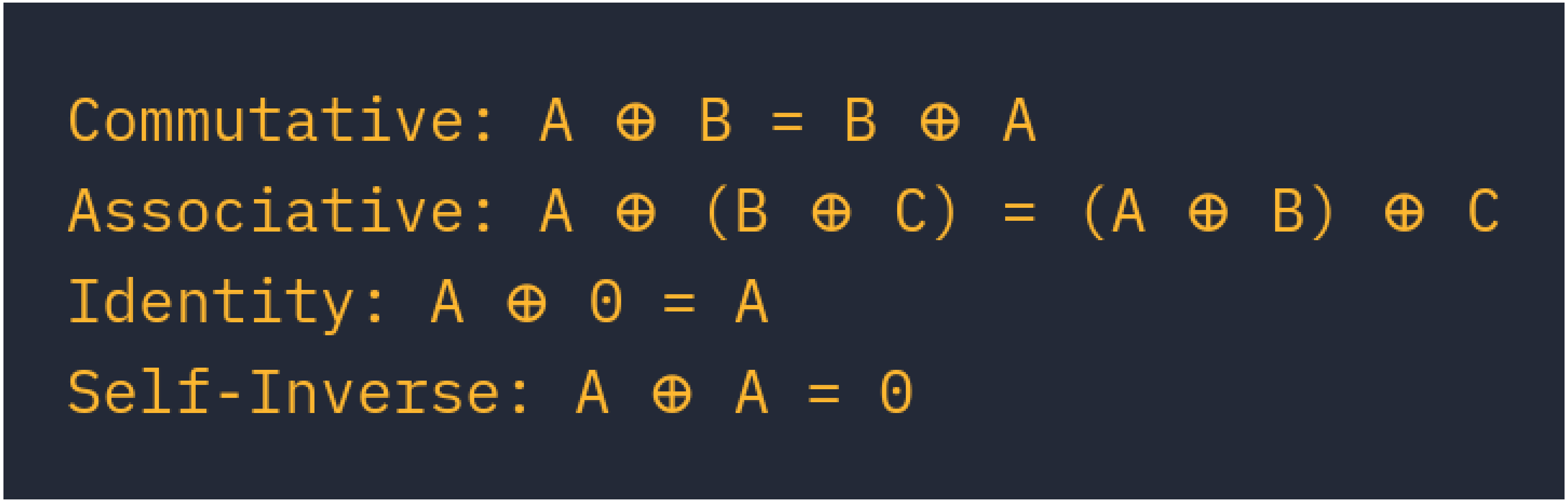
In the last session we learned about the following cryptography concepts

The XOR Operation

XOR is a bitwise operator which can be performed between 2 or more numbers, and returns the number 0 if the bits are the same, and 1 if they are different



XOR Properties



```
Commutative: A ⊕ B = B ⊕ A
Associative: A ⊕ (B ⊕ C) = (A ⊕ B) ⊕ C
Identity: A ⊕ 0 = A
Self-Inverse: A ⊕ A = 0
```

There are several rules that apply to XOR operations, as illustrated above

This Session's Topics

- RSA Cryptosystem Overview

- Pico Mini RSA Challenge x2

Introduction to RSA

RSA, which is an acronym for its' creators Ron (R)ivest, Adi (S)hamnir, and Leonard (A)dleman, is a public-key cryptosystem

Public Key Cryptography

In a public-key cryptosystem, each party (the sender and the receiver) create both a public key and a private key for encryption / decryption purposes, then exchange their public keys

Public Key Cryptography

Alice and Bob exchange public keys

If Alice wants to send Bob an encrypted message with public-key cryptography, first the two would exchange public keys

Public Key Cryptography

Alice encrypts her message to Bob using Bob's private key, and sends it to Bob

Alice takes her message, then uses Bob's public key to encrypt the message and sends it to Bob. Even if the encrypted message is captured, it cannot be read, since its encrypted

Public Key Cryptography

Bob decrypts Alice's message using Bob's private key, and is then able to read Alice's message

Upon receiving the message, Bob can decrypt the message using his private key, and can then read the message. If Bob wanted to respond, he would encrypt a message using Alice's public key, etc...

Public Key Cryptography

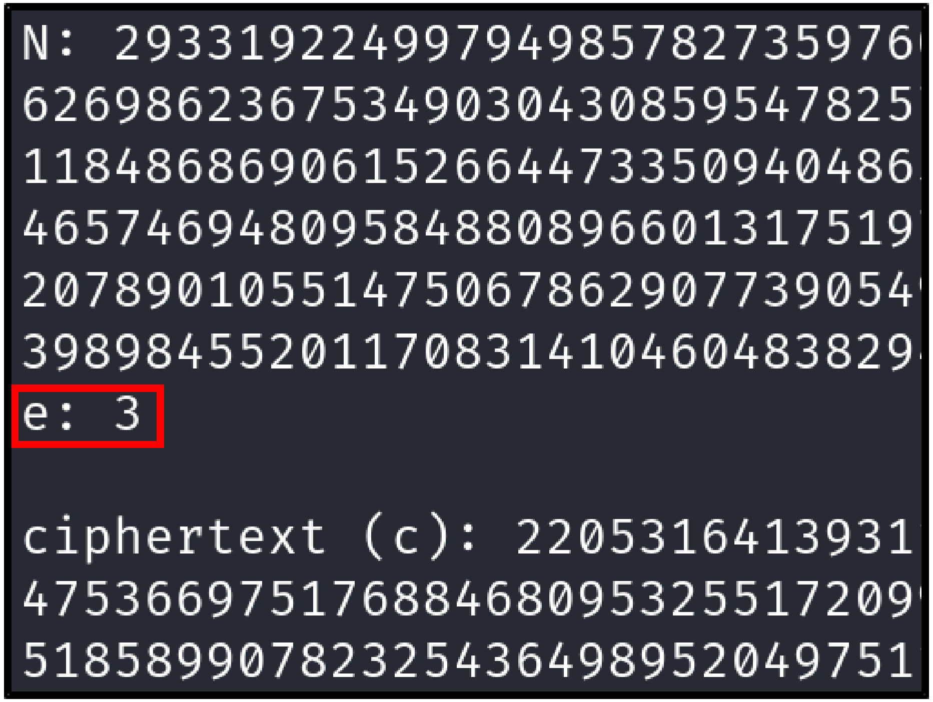
Public-key cryptography is widely used on the internet to secure systems such as HTTPS, SSH, and VPNs

RSA Hacking

Although RSA is a popular and considered to be a secure method of encryption, it is possible to decrypt RSA messages if the keys were created insecurely. We'll go over one of those now..

RSA Exploitation
Cube Root Attack

A Cube Root Attack is a cryptographic attack which takes advantage of a small public exponent (e) in RSA encryption. If successful, the encrypted message can be read without use of the private key

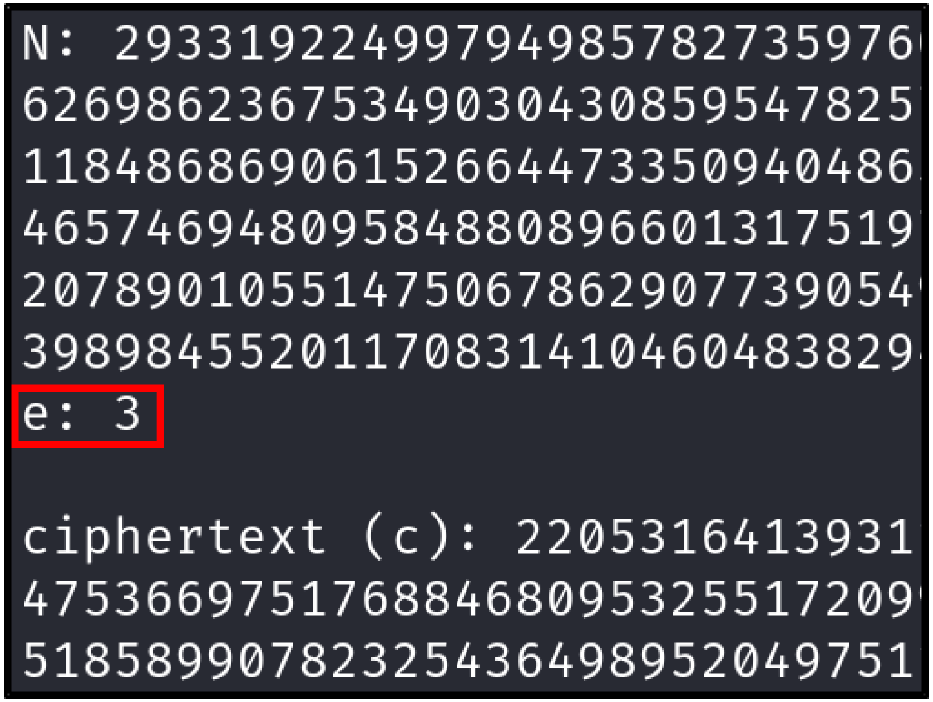


```
N: 29331922499794985782735976
62698623675349030430859547825
11848686906152664473350940486
46574694809584880896601317519
20789010551475067862907739054
39898455201170831410460483829
e: 3

ciphertext (c): 2205316413931
47536697517688468095325517209
51858990782325436498952049751
```

RSA Exploitation
Cube Root Attack

To determine if a specific message encrypted with an RSA public key can is vulnerable to the Cube Root Attack, there are two conditions that must be met:

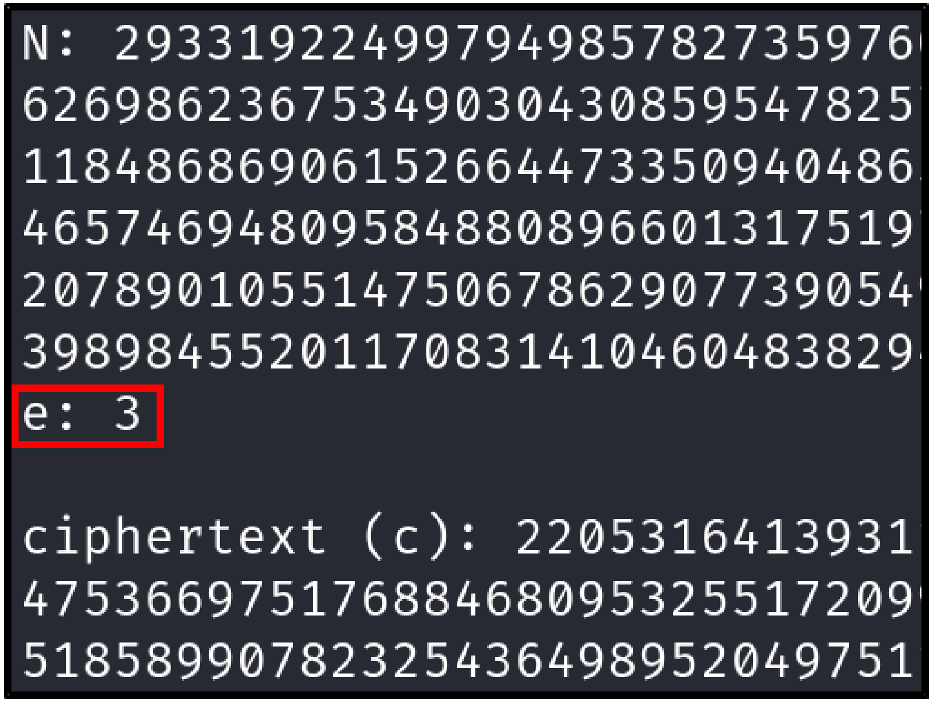


```
N: 29331922499794985782735976
62698623675349030430859547825
11848686906152664473350940486
46574694809584880896601317519
20789010551475067862907739054
39898455201170831410460483829
e: 3

ciphertext (c): 2205316413931
47536697517688468095325517209
51858990782325436498952049751
```

RSA Exploitation
Cube Root Attack

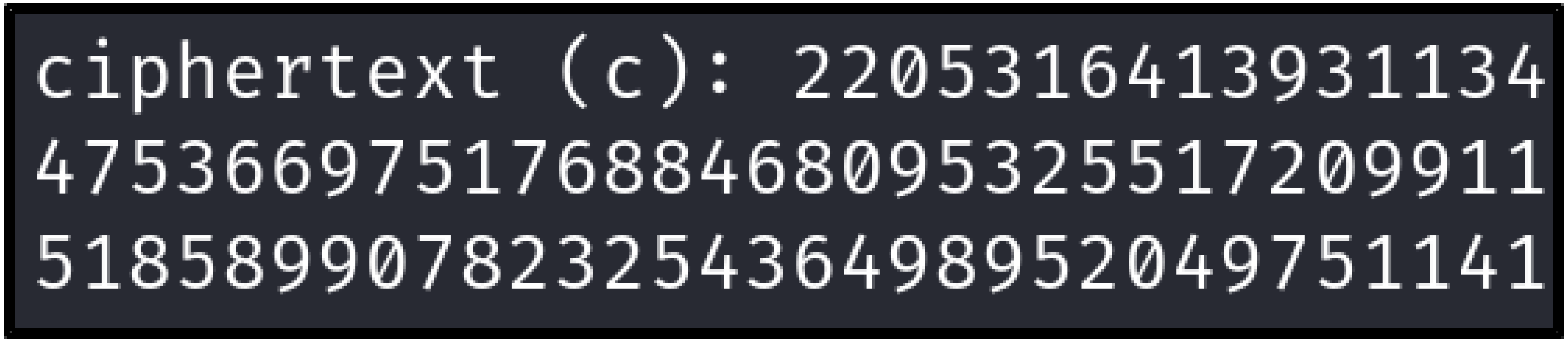
The first condition is that the exponent (e) used in the public key must be sufficiently small



```
N: 293319224997949857827359 76
626986236753490304308595478 25
1184868690615266447335094 0486
465746948095848808966013175 19
20789010551475067862907739054
398984552011708314104604838 29
e: 3

ciphertext (c): 2205316413931
47536697517688468095325517209
51858990782325436498952049751
```

RSA Exploitation
Cube Root Attack



```
ciphertext (c): 2205316413931134
47536697517688468095325517209911
51858990782325436498952049751141
```

The second condition is that the ciphertext (c), and in turn, the plaintext (m) is sufficiently short

PicoCTF – Mini RSA

Let's learn more about the RSA cipher by working through a challenge on PicoCTF. Navigate to the following URL

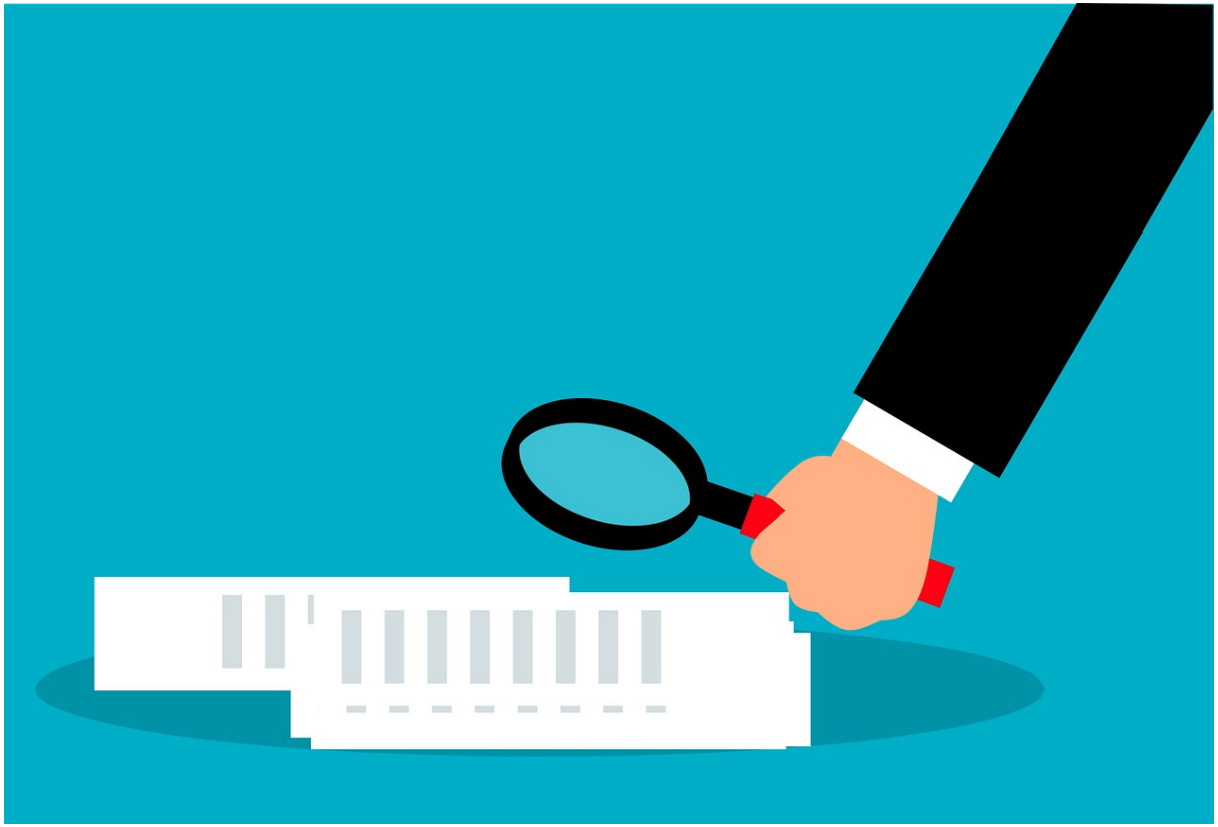
https://play.picoctf.org/practice/challenge/188?page=1&search=mini

PicoCTF – miniRSA

Let's reinforce our RSA hacking skills by working through another challenge on PicoCTF. Navigate to the following URL

https://play.picoctf.org/practice/challenge/73?page=1&search=mini

Summary



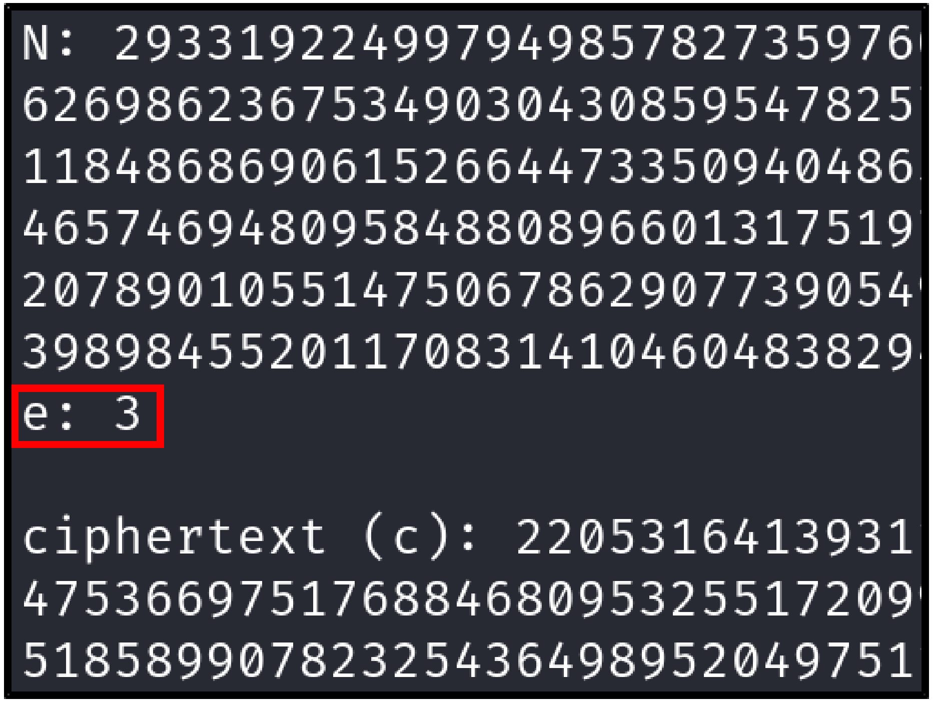
Let's review the cryptography concepts we learned in this workshop:

Introduction to RSA

RSA, which is an acronym for its' creators Ron (R)ivest, Adi (S)hamnir, and Leonard (A)dleman, is a public-key cryptosystem

RSA Exploitation
Cube Root Attack

Although RSA is considered secure, it can be hacked if it is used with insecure settings, and one such attack that could be leveraged against it is the Cube Root Attack



```
N: 2933192249979498578273597 6
6269862367534903043085954782 5
1184868690615266447335094048 6
4657469480958488089660131751 9
2078901055147506786290773905 4
3989845520117083141046048382 9
e: 3

ciphertext (c): 220531641393 1
4753669751768846809532551720 9
5185899078232543649895204975 1
```

What's Next?

This is the end of our HackerFrogs AfterSchool cryptography course, but tune in next time when we'll be starting a new course on network hacking!

Until Next Time, HackerFrogs!