# HTB Mysterybox Report

## Introduction

Encryption puzzles may be stated as a meaningful tool for examining more difficult encryption techniques and protocols. This article is all about solving the talk of rsa signatures on the acclaimed social network platform and because of that we gave our best effort for it. At this point, the challenge pushes players to do the exercises of understanding and exploring the RSA signature scheme that is implemented as a part of Python script. Interacting with a server brought us error and failure. However, we figured out the flag step-by-step and touched upon different aspects of cryptography. In this report, we will be doing a problem breakdown, an exercise of code assessing and a game play to solve the problem. While we were in distant world we were able to manage the dispency by applying our cryptography kniww-how and smart thinking.

**Tools used**

Netcat

Kali linux

Challenge Overview

Comprehending the RSA signature method is very difficult, not to say that you may not manage to derive the advantage out of it and implement it to the purpose. The Python script illustrated below is built with functionality to generate RSA key pairs, signatures, and justification of signatures.

The key components of the box are:

* 1. 1. *RSA Key Generation:* RSA public and private keys have modulus n, public exponent e, and private exponent d, which are precisely created randomized prime numbers.
  2. 2. *Signing and Verification:* A script is created to do the following operations: signing messages with the private key and validating signatures with the public key. To complete their purpose, participants must be in a position to do so.

**Challenge Objective**  
  
The main goal for executing the challenge is to allow an attacker to sign our specific message, but without letting an attacker to sign the message by direct means. In place of that the learner must uncover the RSA signatures as a whole and get the valid signature of the target message.  
  
Participants will be working through a menu-driven interface provided by the server which allows them to affix their message and verify its authenticity. Mandatory accomplishment of the project stands on nailing a tactic to embed message signatures in a hope of reaching the set goal.  
  
  
**Problem Analysis**  
  
In the Mysterybox challenge it is going to command the participants to figure out and then use the RSA signature algorithm that is imbedded in the given Python script (server.py). As a group to solve the challenge all the participants first was to understand the following several key aspects:As a group to solve the challenge all the participants first was to understand the following several key aspects:

1. *RSA Signature Algorithm:* To provide such technicalities as key generation, use a private key to sign a message and a public key to verify it.

2. *Constraints and Objectives:* After realizing that they couldn't directly retrieve the target message's signature, they identified and researched machine learning algorithms. In contrast to them, they search for the answer to their goal rather than pursuing instant fulfillment.

3. *Server Interaction:* By allowing participants to interact with the study's virtual environment, the limitations of using the menu-driven command-line interface were assumed. Completing these tasks is a crucial component of mastering the communication tool for the future.

4. *Exploiting RSA Properties:* In order to achieve this, it is "a must" to demonstrate the mathematical nature of RSA using signatures. Furthermore, the ability to obtain the necessary signature in reverse is made possible by the fact that the RSA method has multiplicative operation capabilities.

5. *Error Handling and Edge Cases*: With the Python snippet supplied, handling exceptional circumstances like error conditions and edge cases was crucial. It was required of participants to understand the script's error-handling mechanism and provide input in a way that complies with the script's constraints.

6. *Security Implications:* It is important to be aware of the security implications of the RSA signature technique and how it is implemented. Cryptology is used by users to evaluate security strength, preserve secret key confidentiality, and uphold the integrity of blockchain processes.

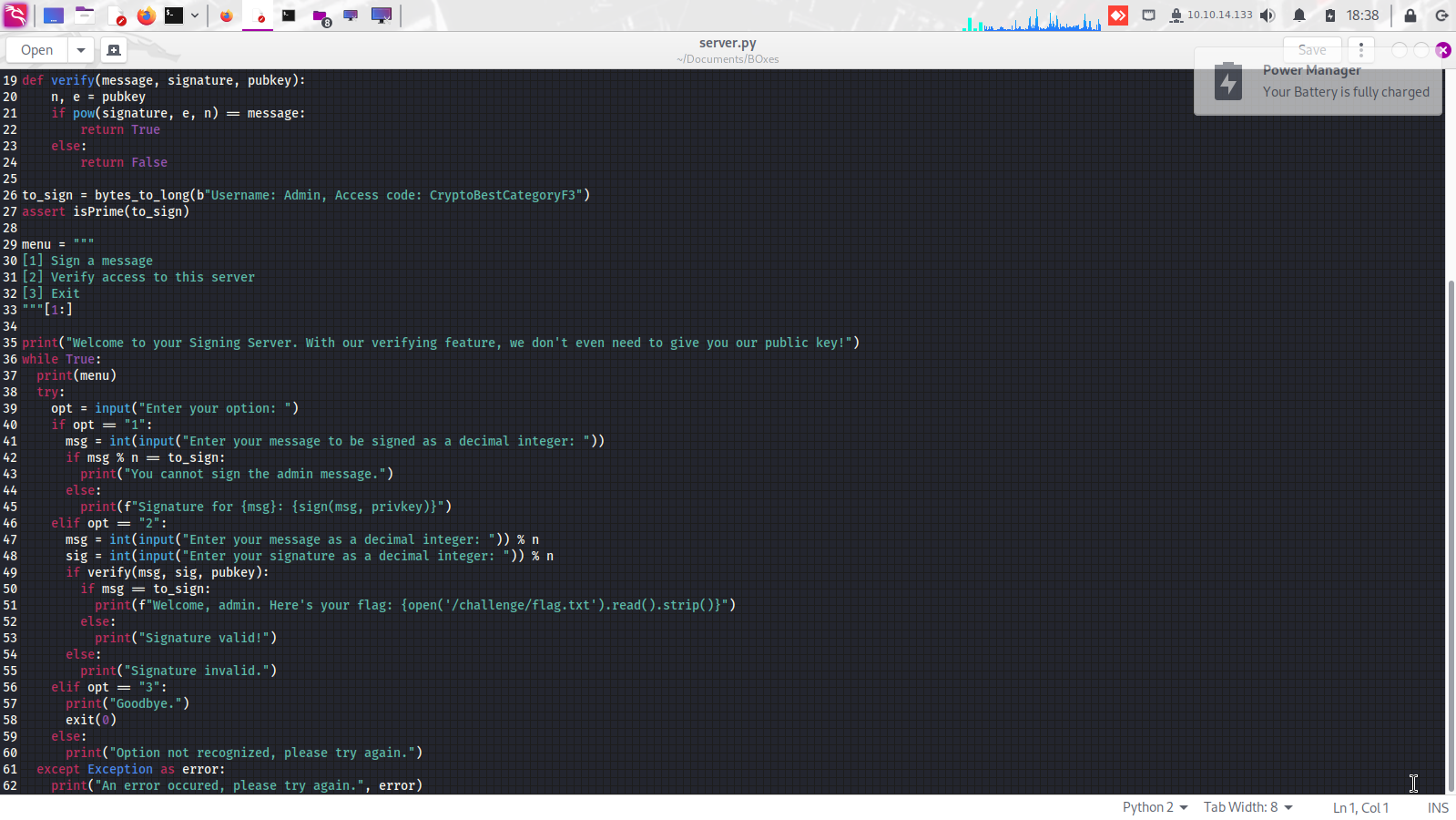


Fig 1: Part of the provided python code

Methodology

Among our efforts to running the Mysterybox challenge, we took many essential actions. The methods we employed involved exploiting the RSA signature algorithm representations and careful control of the message signatures to achieve our goal. The following describes our step-by-step approach:The following describes our step-by-step approach:

I. *Understanding the Challenge:* First, we carefully reviewed and comprehended the issue statement, which was provided along with the server.py Python script, as well as any constraints stated in the documentation. The next step was to confirm that the service was operational when running at the specified IP address and port.

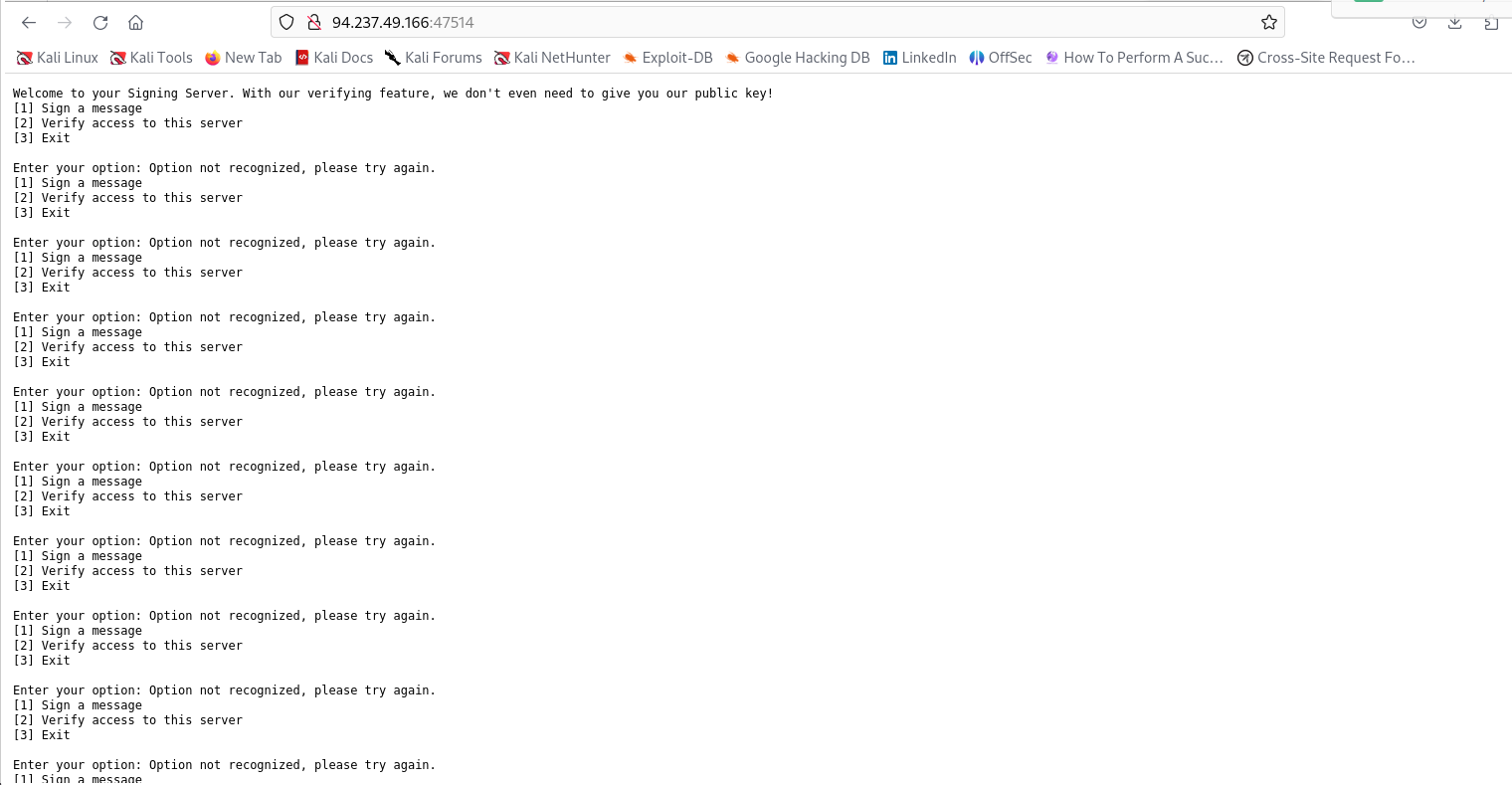


Fig 2: the output after accessing the service from web browser

*I. Analyzing the RSA Algorithm:* We've been learning about the RSA signature algorithm, which includes key creation to validate a signer's identity, message signing with a private key, and signature verification with a public key. Thus, we were able to build our solution on these fundamentals.

*II. Identifying the Target Message:* We went through and found a target message that causes it to be signed, as mentioned in the problem folder. Because we were unable to obtain a signature directly for this reason, we devised a strategy to obtain it indirectly, taking use of the weather on RSA site.

III. *Exploiting Multiplicative Property*: To identify which features of RSA Rule and signature signs. We negated the target message's (-to\_sign) value and determined that the produced figure was a valid signature. Our solution strategy was built on the experience we gained in the course of this work.

IV. *Interacting with the Server:* After obtaining the server settings, we used the menu-driven interface's (MDI) instructions to sign messages and verify signatures. To advance in the task, we needed to send messages and interpret what they stated.

To achieve the desired output, this technique required proper input formatting and the use of the module approach.

VI. *Verifying the Obtained Signature:* Following the act of acquiring a signature for message denial, we used the verify signature option to compare the signature of the message (to\_sign) with the signed message. Following that, a flag appeared on the screen as proof of signature verification.

V. *Signing the Negated Message:* Our team found that creating a string (-to\_sign) with the negation of the message we wanted to sign was the most effective way to finish this assignment. The resulting signatures are

multiplicative.

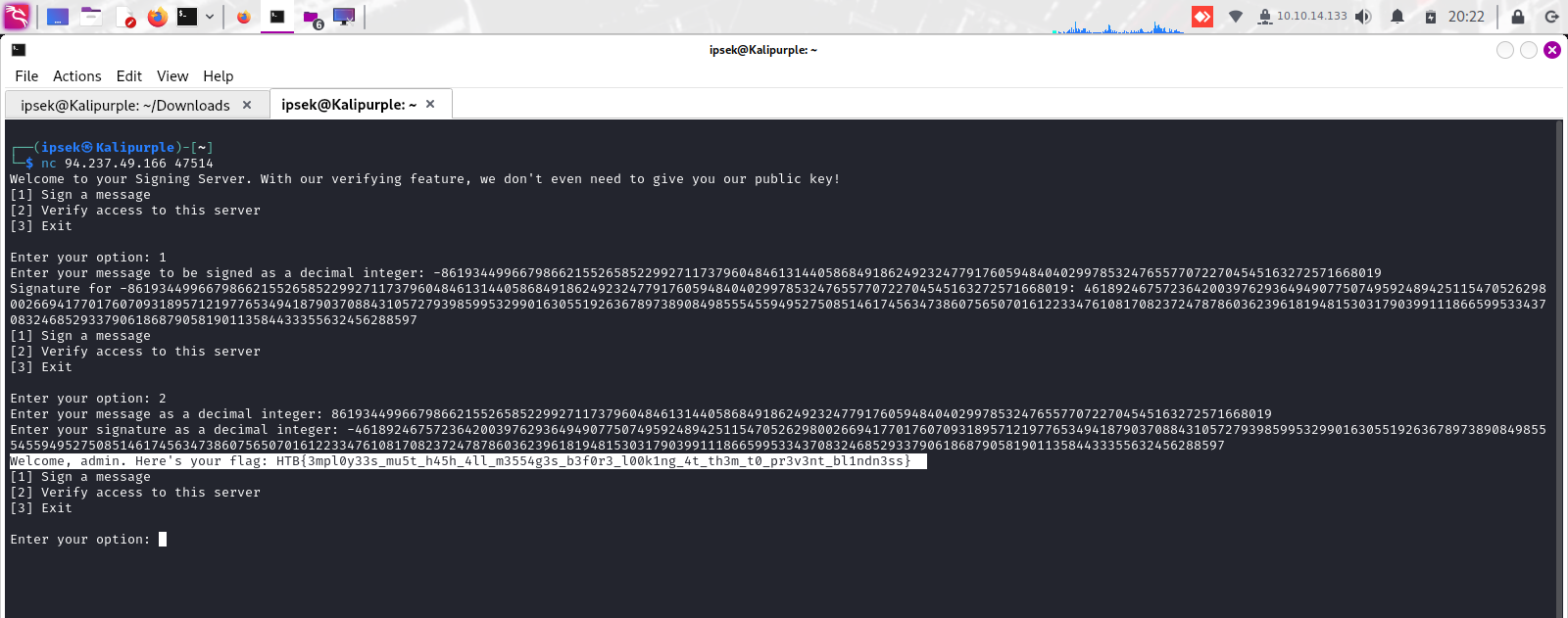


Fig 3: game over! Successful verification of the signature

Throughout the process, we continuously improved our methodology, verified our findings, and adjusted our strategy as needed based on server replies and observed results. We successfully addressed the difficulty and achieved our goal (flag) using this methodical approach and our understanding of the RSA signature technique.

Lessons Learned

The cryptographic puchase of the Mysterybox not only helps but also shed a light on different angles of cryptography and problem solving. The following are key lessons we gleaned from the experience:The following are key lessons we gleaned from the experience:

1*. Understanding RSA Signature Algorithm*: In the mastery of the challenge, I mainly learned the significance of getting knowledge of the fundamentals of the cryptography algorithms, for instance, the RSA signature method. RSA which was the source of most problems, to some extent, was inevitably the one governing the right manner of problem-solving.

*2. Exploiting Cryptographic Properties:* In cryptography, discovering the creative uses of cryptographic cypher and algorithms was very critical so that the constraints could be overcome and the specific objectives could be achieved. Taking advantage of the RSA signatures that follow the rule of multiplication illustrated the significance of the art of encouraging problem-solving in cryptography.

3. *Practical Application of Cryptography:* A potential obstacle encountered along the way was the defense of real-world applications of cryptography, including digital signatures and secure communication protocols. Putting fundamentals of cryptography in the practice rewrote possibilities we do understand and appreciate subtlety of cryptographic techniques.

4*. Error Handling and Input Validation:* Error handling and input validation, which were the demonstrations in the given environment, showed us the value of the robust error handling. A foothold in integrity concerns and, finally, resilience to edge cases is a must in real-life cryptograph algorithms.

5. *Iterative Problem-Solving Approach:* Show the adaptive problem-solving method yielded positive and favorable outcomes, though it was applied in the face of great challenges. On an iterative basis, we checked the efficiency of out strategy, validated the results found, and making adjustments of our approach based on the visible outcome were the things that helped us to realize the goal.

6. *Critical Thinking and Analysis:* The task explained indirectly that a good deal of learning took place during the task and that the skills of critical thinking and analysis were the most important in cybersecurity jobs. Investigative analysis about problem statements, locating patterns and producing procedural solutions are some of the most crucial traits required to be a successful participant in cryptographic challenges and cybersecurity areas.

7. *Documentation and Reporting:* Recording our methodology, results and insights in a structured report form was the most useful to help us achieve the objectives of recording and communicating the problem solution approach effectively. Clear and concise documentations is the key for the knowledge sharing and aids collaboration in cybersecurity and other enterprises.

**Conclusion**

The RSA signature Mysterybox challenge acts as a cryptography learning environment, providing me with the opportunity to thoroughly explore the RSA algorithm and apply cryptographic concepts in a real-world context. By using a logical approach to problem solving, thinking strategically, and being willing to experiment, we were able to overcome the obstacle and attain the intended goal.

We established a method for the major issue by understanding the fundamentals of the RSA signature technique and taking advantage of its features. As a result, we were able to obtain the signature for the target message indirectly. Using the multiplicative properties of RSA was only one example of how figuring things out, solving problems, and comprehending concepts is the primary concern here.

This task allowed us to elaborate. The following classes will focus on cryptography theory: mastering the various cryptographic methods, using cryptographic properties to break secrets, and applying theoretical principles in real life. Furthermore, it emphasized the necessity of well-developed error handling, iterative strategies for solving specific challenges, and good documentation in this field.

In the future, we plan to focus on cybersecurity and cryptography as primary themes, as well as take our failed experience to the next level and work on the MysteryBox challenge. With polishing our abilities further, cooperating and team building with colleagues, and working on the various cybercrime concerns, we want to contribute significantly to the cybersecurity community and be more skilled and effective in cybersecurity by increasing the community's reliability.

Furthermore, we can conclude that the Mysterybox work was a beneficial experience, as it provided us with significant gains in knowledge, training, and development in the field of cryptography and cybersecurity. We are delighted about this learning experience and plan to utilize it not just in our future undertakings, but also in future problems, with a fresh attitude and drive.