PennState
College of Information
Sciences and Technology

CyberChef - Lessons for Learning Encryption

CAE Forum

David M. Hozza, CISSP, MPS
Lecturer - Cybersecurity and IST
Penn State - College of Information Sciences & Technology

Bio – David Hozza

- Faculty – Penn State College of Information Science and Technology.
- Cybersecurity Instructor at Penn State since 2017.
- Prior to teaching, 30 years in Industry.
- Focus on Teaching Cyber Defense and Information Sciences and Technology courses.
- Developed several Cyber courses and 18 Cyber Labs.

Framing the Problem

Learning **Encryption can be overwhelming** for some students, for many this is their first Cybersecurity course.

- **Public and Private Key pairs** with Asymmetric Encryption lessons lack hands-on applications.
- Teaching **Digital Signatures lacked hands-on** applications.
- **Traditional hands-on** Labs are better suited for implementing encryption i.e.: SSL, PKI and SSH.
- Making it FUN.

What is CyberChef ?

Cyber Chef is a popular set of Crypto tools often referred to as the "**Cyber Swiss Army Knife**". It is maintained by the British Government Communications Headquarters (GCHQ). https://gchq.github.io/CyberChef

- Encoding/Encryption
- Malware Analysis
- Hashing
- Forensics and Much more…..

We used it in our **tool set for CTF's and Competitions** but didn't really think about it as a teaching tool.

Assignment Review

Introduction

The purpose of this assignment is to allow students to practice **Asymmetric encryption** while familiarizing themselves with Cyber Chef. These exercises will utilize **PGP encryption and digital signatures** so students can send and receive encrypted and signed data.

Noe: Instructor needs to provide students with the Instructor Public Key.

Deliverables

Submit **three text files** as outlined in the instructions.

Setup Work

Generate your Public-Private Keys and Save Them.

Generate the PGP Key pair in Cyber Chef by sliding the "**Generate PGP Key Pair**" from the left side of Cyber Chef to the Recipe. Make sure that the Recipe is green and do not enter any other info. Make sure your **Auto Bake** option is set at the bottom and it should generate output with a Private and Public Key.

SAVE your keys by clicking the **Disk icon** under input. Name your key file with a description and save it to a safe place on your system. Make sure you can open the file, it should open with notepad or some other editor so you can view your **Private and Public** Key Blocks.

Task 1 - Encrypt a Message and Submit

Learning Objective – How Asymmetric Key Pairs work.

In this task we want to ensure a message is **sent confidentially** to your instructor. So reviewing our lesson we know that you need to encrypt the message with the instructor's Public Key which was provided.

1. Click the **Garbage Can Icons** in Cyber Chef to remove any existing Recipes, or Input Output.
2. Slide the PGP Encrypt recipe over and copy the text of the Instructors Public Key which is made available in Canvas. Be sure that you **include** the ---- BEGIN at the beginning and ------ at the end, your recipe **should turn green.**

Task 1 - Continued

3. You still need to create a message so go to the Input Box and enter a message similar to the following with **YOUR name** in it. Ex: "This is a secret message for the Instructor from student David Hasselhoff".
4. If Auto Bake is enabled the **Output** should contain the PGP Cipher text. Click the disk by output and save it to a text file, name the **file with your name** and the task, for example "**David Hasselhoff task 1.txt**". IF you did everything right your instructor will use their Private Key to Decrypt your message.

Task 1 (File Submission) - Submit your first text file to Canvas and follow the naming instructions in Step D. If your work is correct only the Instructor can read the message.

Task 2 – Non Repudiation, Digitally Sign and Encrypt a Secret Message.

Learning Objective: Non Repudiation means that we can **verify the sender of a message.** We can do this with a **Digital Signature** that you put on your message with your Private Key. Remember that you never share the Private Key.

1. Delete any previous Recipes or Input Output and slide the **PGP Encrypt and Sign Recipe over.**
2. To prove you are the sender you will need to **copy the text of your Private Key into the Private Key and Signer Box** on the Recipe, not on the Input.
3. Since we are also **encrypting** the digitally signed message to your instructor you need to **provide the instructor's public key** so that only the instructor can open it. Just like the last Task you need to paste the instructor's Public key into the Public Key of the Recipient on the Recipe. Your Recipe **should turn Green**.

Task 2 – Part 2

4. Add input that can be signed and encrypted. In the Input box make a message that tells us you signed this and includes your name, for ex: "I signed this encrypted message, all the best David Hasselhoff".

5. Just like your last Task, If Auto Bake is enabled the **Output** should contain the PGP Cipher text. Click the disk by output and save it to a text file, name the **file with your name** and the task, for example "David Hasselhoff task 2.txt". If you did everything right your instructor will use their Private Key to Decrypt your message.

6. You need to **send the instructor a third file** so they can verify you actually sent the message. Figure out that that file should contain and send it as well. **Name the third file as task 3**, for ex: "David Hasselhoff pub key task 3.txt"

Results and Recap

Positive Feedback from Students.

- **This exercise was fun and gave me a better understanding of key pairs.**
- **It took me a few tries to get the digital signature part but it taught me how these algorithms work.**
- **I liked the change of pace from our regular labs, CyberChef is a great tool.**

Thank - You

Questions?