IS 3513-001 Information Assurance and Security

Lab #02
Using Encryption

Student:
Dillen Dela Cruz, odv464

Prepared for Information Assurance and Security
10/1/2023
Professor: Cody Cunov

Contents

Introduction:

This lab aims to equip students with the tools and knowledge to encrypt/decrypt emails and files. Students will experiment using Gpg4win for Windows and a few of its several Free Software components such as Kleopatra and GnuPG. The end goal is to provide firsthand experience into asymmetric encryption.

Encryption:

Encryption is the process of converting information into a secret code that hides its true meaning. Although this process may sound like some present-day innovation, this process can be traced back as early as 1900 BC with Egyptian hieroglyphics. They used a method called simple substitution to create disordered hieroglyphics but in reality each letter (picture in this case) was replaced by another letter in their alphabet (Cryptography). A great example of this would be a Caeser Cipher or a shift cipher in which Julius Caesar would shift the alphabet a certain number of times creating a cipher alphabet. In the picture below you can see that the alphabet (first line) is shifted three spaces to the left (second line). Now you can see that the new Position of 'A' would be the position where 'X' would be in the original alphabet. The second line would represent your newly created cipher alphabet. If you wanted to translate the word 'hello' you would need to write down its corresponding letter in the cipher alphabet (blue dots). The encoded message would read 'khoor'. To Caesars' enemies, this would look like a bunch of gibberish but to his generals who possessed the cipher alphabet or knew the shift value, the message would be easily decipherable and reveal the next plan of operation.

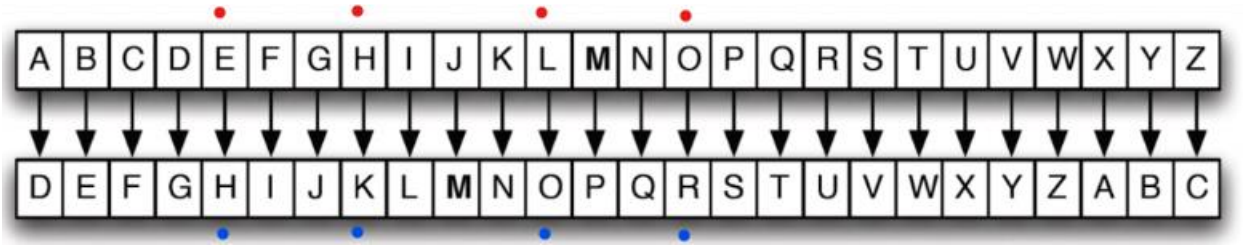


Figure 1: Caeser Cipher

Some other substitutions methods can also involve splitting the alphabet in half and using the corresponding letters given.

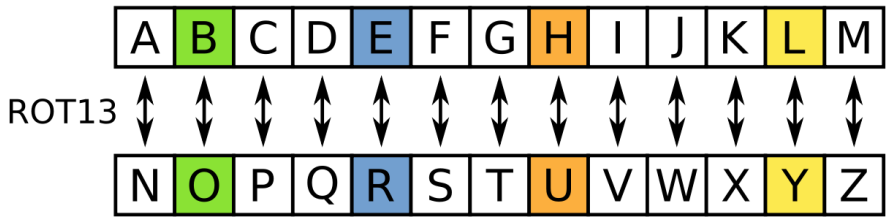
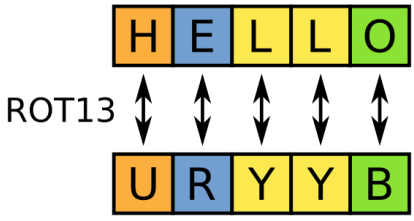


Figure 2: Substitution Method



Nowadays encryption involves mathematical techniques which have ultimately changed and improved the way we encrypt messages or files. If you think Caesars' enemies were confused when looking at his encrypted messages, just imagine what they would think if they saw this encrypted text below. Mathematic concepts such as number theory, modular arithmetic, and probability theory play a crucial role in the development of secure cryptographic algorithms (Saini). This is also one of the basic principles needed to become a cryptography professional as well as an understanding of programming languages such as Python and Java, and a strong ability to communicate within a team, both verbally and in writing (Tulane).

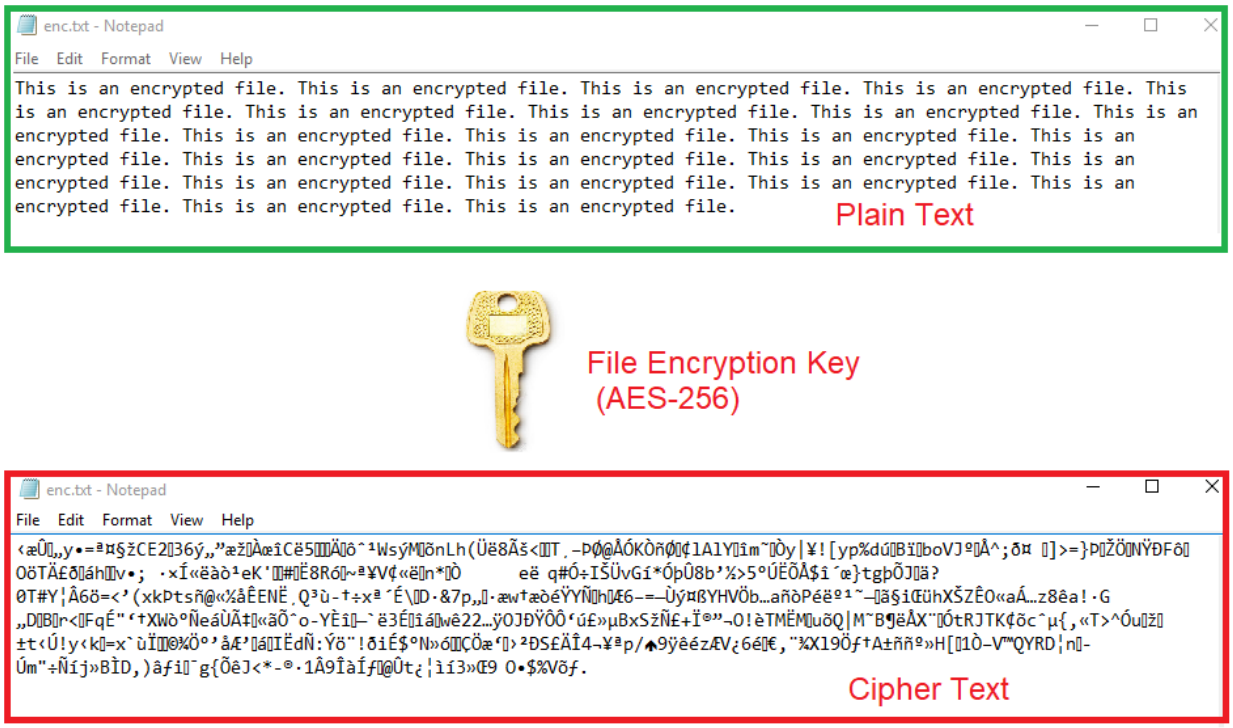


Figure 3: Current Encryptions

There are two types of encryptions Asymmetric and Symmetric:

Symmetric – Symmetric is considered an older and simpler method of encrypting information. This encryption involves only one key to encrypt (lock) and decrypt (unlock) data. This means that parties communicating between each other must use the same key to encrypt and decrypt messages being sent. You can find symmetric encryption all around you such as online banking and shopping, cloud storage (Google Drive) and even when you connect to a secure WI-FI network.

- *Advantage:*
    - Faster and more efficient than asymmetric encryption. Is widely used for bulk encrypting and decrypting of large amounts of data (Smirnoff et al.)
    - Cheaper to use for businesses who do not plan on exchanging data between different parties. Consequently, because symmetric encryption relies on a single encryption key, it is most suitable for securing data at rest.
- *Disadvantage:*
    - Key exhaustion may occur. This is where every time the key is used some information can potentially leak out which could be used by an attacker to reconstruct the key (Smirnoff et al.).
    - Since there is only one key that does both encrypting and decrypting, a plan must be devised to safely ensure the distribution and the management of the key. Nevertheless, on a broader scale, this approach can swiftly become impractical when it comes to the need for key tracking and rotation.

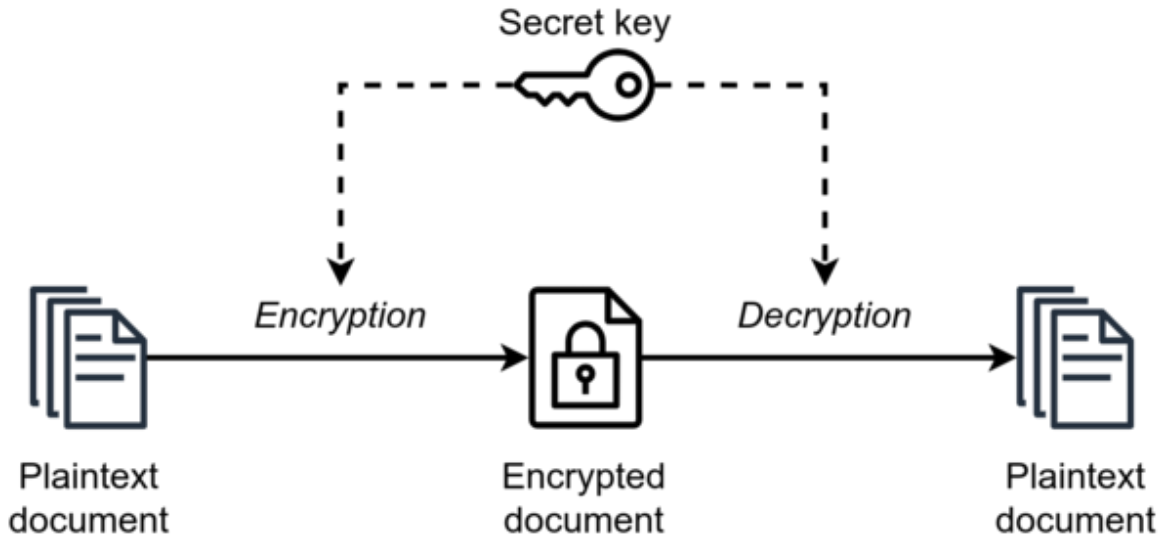


Figure 4: Symmetric Encryption

Asymmetric – Was invented by Whitefield and Martin Hellman in 1975 (UTSA). Known also as public-key encryption uses two types of keys: one public key which is shared by everyone and one private key which can be shared by individual parties. In the process, the sender will use the recipient's public key to encrypt. Once the information is sent to the recipient the individual/party will use their private key to decrypt the message. Examples of asymmetric encryption would be digital signatures, secure shell (SSH), and blockchain.

- *Advantage:*
  - Eliminates key distribution for decryption. This overcomes the biggest problem that symmetric encryption has (2nd bullet under disadvantage of symmetric encryption)
  - Provides non-repudiation meaning that the sender cannot deny sending or altering any of the data that is being send to the receiver. In asymmetric encryption, a sender can create a digital signature for a message or document using their private key. This signature is unique to the sender and the content of the message. This also provides authentication, enabling the receiver to verify the sender's identity (Jain).
- *Disadvantage:*
  - A slower encryption process compared to symmetric due to its high utilization of resources thus less efficient since it can only handle smaller amount of data compared to symmetric
  - If either party loses their private key, there is no way to decrypt messages being sent to them.

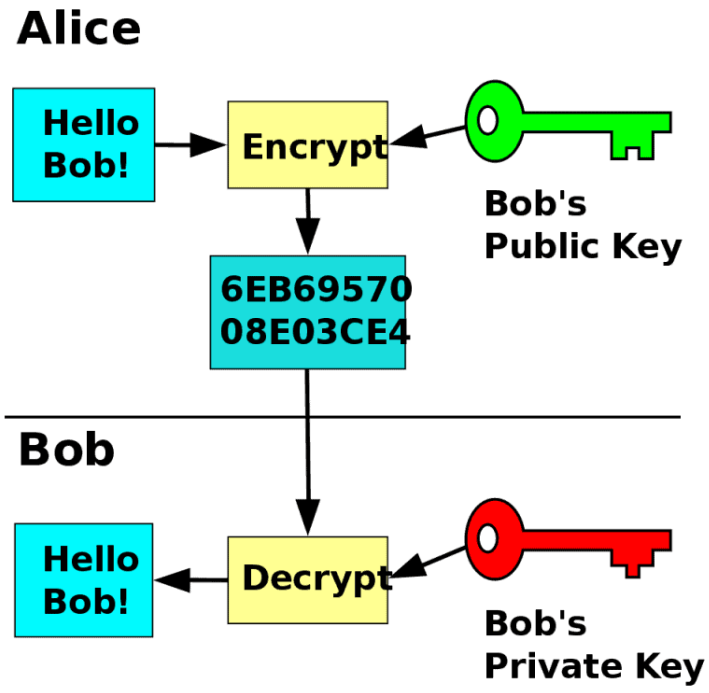


Figure 5: Asymmetric Encryption

Asymmetric and Symmetric together:

In cases involving data in motion or during transmission, encryption protocols like SSL/TLS use a combination of asymmetric and symmetric encryption (F5). Initially, asymmetric encryption is employed to establish a secure connection between a client and a server, creating a secure environment. Once this secure connection is established, data transfer occurs within this secure environment using symmetric encryption.

Why encryption is important to implement:

Encryption serves as a valuable defense for organizations against potential threats, aligning with several of the 20 Critical Security Controls:

- *Control 7: Email and Web Browser Protections*
    - This could involve the deployment of protocols like SSL/TLS, as previously described which uses both types of encryptions
- *Control 13: Data Protection*
    - Properly designed encryption makes it more challenging for attackers to exploit data, contributing to the mitigation of insider threats and enhanced data protection.
- *Control 15: Wireless Access Control*
    - Implementing wireless security involves incorporating concepts like encryption. Examples of wireless security protocols that utilize encryption include WPA2 and WPA3.
    - "Utilize Advanced Encryption Standard (AES) to encrypt data packets over the wireless connection (RSI Security)"

How encryption improves Confidentiality, Integrity, and Availability:

- *Confidentiality:*
    - Encryption ensures that only authorized personnel can access the sensitive data. It achieves confidentiality by changing the data so that it is unreadable to anyone that does not have the decryption key. This prevents unauthorized access and eavesdropping (Net Spot).
- *Integrity:*
    - When data is encrypted, any unauthorized changes to the encrypted content become apparent when the hash functions compute the message digests. This allows for testing of any unauthorized modifications or tampering during transmission or at rest.
- *Availability:*
    - By maintaining confidentiality through encryption, data is protected from unauthorized access, alterations, or compromises. This safeguards the unaltered and secure data, making it readily available to authorized users when needed, thus enhancing overall data availability

Before explaining my experience with Encryption lets set the stage first:

Gpg4win, GnuPG, and Kleopatra

Gpg4win is an encryption software that allows a user to sign and encrypt files and emails (gpg4win). It uses the help of encryption, protects the data from being read from unwanted parties, and digital signatures, ensures that data is not tampered with and authenticates the sender, to transport information securely.

Figure 6: Gpg4win logo

Gpg4win is an installer for Windows and contains several Free Software components but in this case we will only be looking at 2 of the 5,

GnuPg or GPG is a free open-source command-line tool and application that allows users to implement OpenPGP standards to secure information. It is the backend of Gpg4win, functioning as the primary encryption tool (gpg4win). In some cases, it employs both asymmetric and symmetric methods. It not only lets users encrypt and decrypt but also "sign communication data using a unique personal key that designates the ownership of the data (authentication and non-repudiation) and security against modification and tampering (improves CIA) (Singer and Guide)." GPG is the successor to the earlier encryption standard, PGP or Pretty Good Privacy.

Figure 7: GnuPG logo

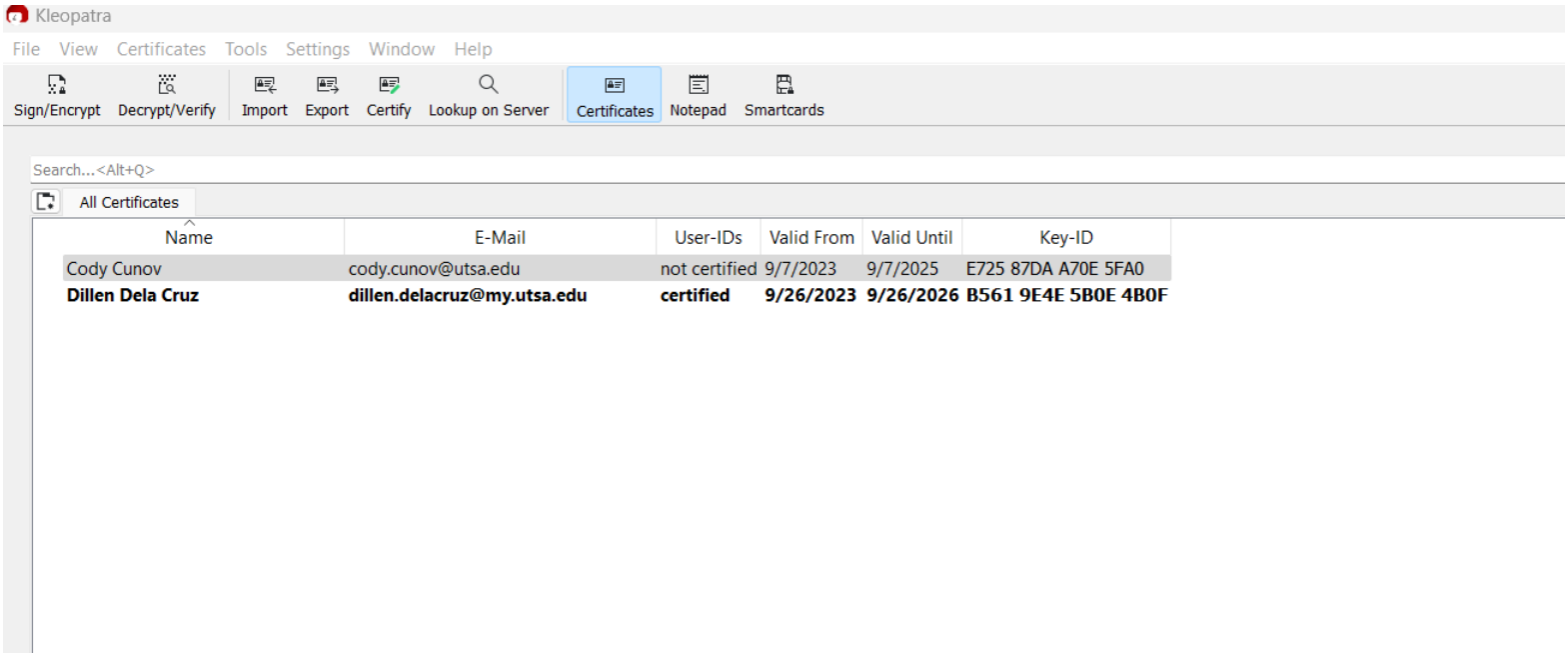
Kleopatra is a certificate manager for OpenPGP, X.509 (S/MIME) and common crypto dialogs (gpg4win). It is the preferred certificate manager for Gpg4win, providing simple import and export of certificates to and from certificate servers (key servers) for both OpenPGP and X.509 certificates. With Kleopatra you can also certify OpenPGP certificates of a trusted person (GPG4win). The software component functions as the graphical user interface (GUI) to GnuPG.

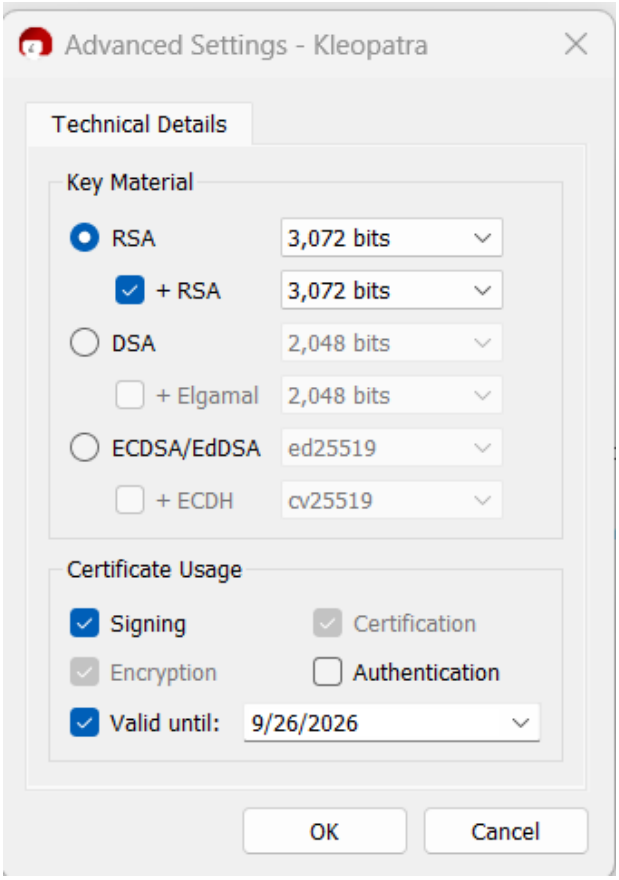
Figure 8: Kleopatra logo

My Experience

Here, I will describe what I did for this section of work. I provide relevant information to the lab and discuss what I did and how. In lab 2, steps 1 through 8 require the usage of Kleopatra.

Figure 9 and 10: Public Key and Private Key Setup





I generated my public and private key pair following these steps:

First, I went to 'File' and selected 'New OpenPGP Key Pair.' Then, I entered my full name and UTSA email address. In the 'Advanced settings,' I chose RSA with 2048-bit encryption and selected encryption as the only use while unselecting signing and authentication. I also ensured that the key would remain valid through the end of the semester.

After completing these settings, I named the public key file as 'MyLastname_abc123_Public_Key.asc. In addition, I had also imported my professors public key so that when I want to send him a message I can use his public key to encrypt my message

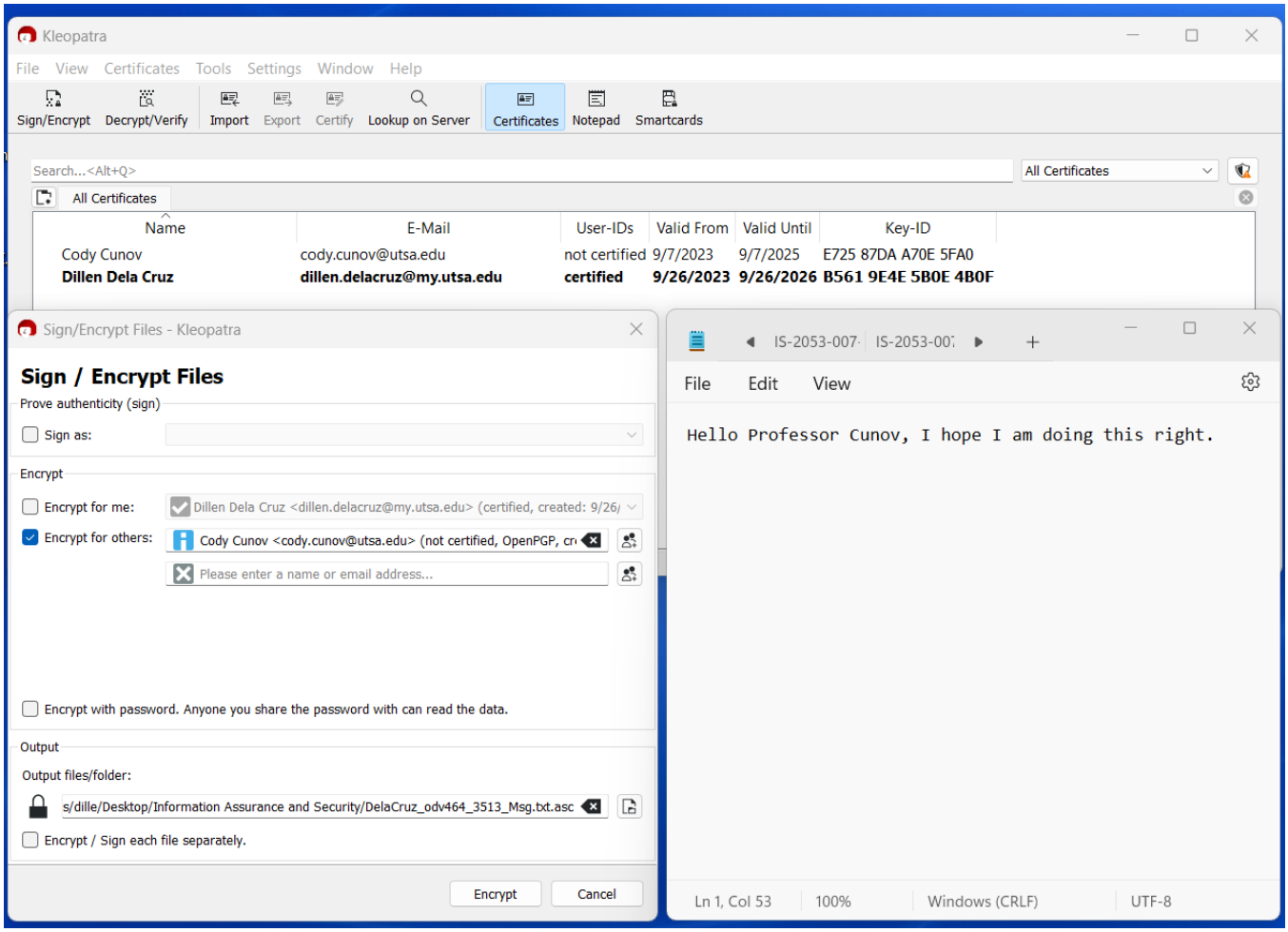


Figure 11: Encrypting Text

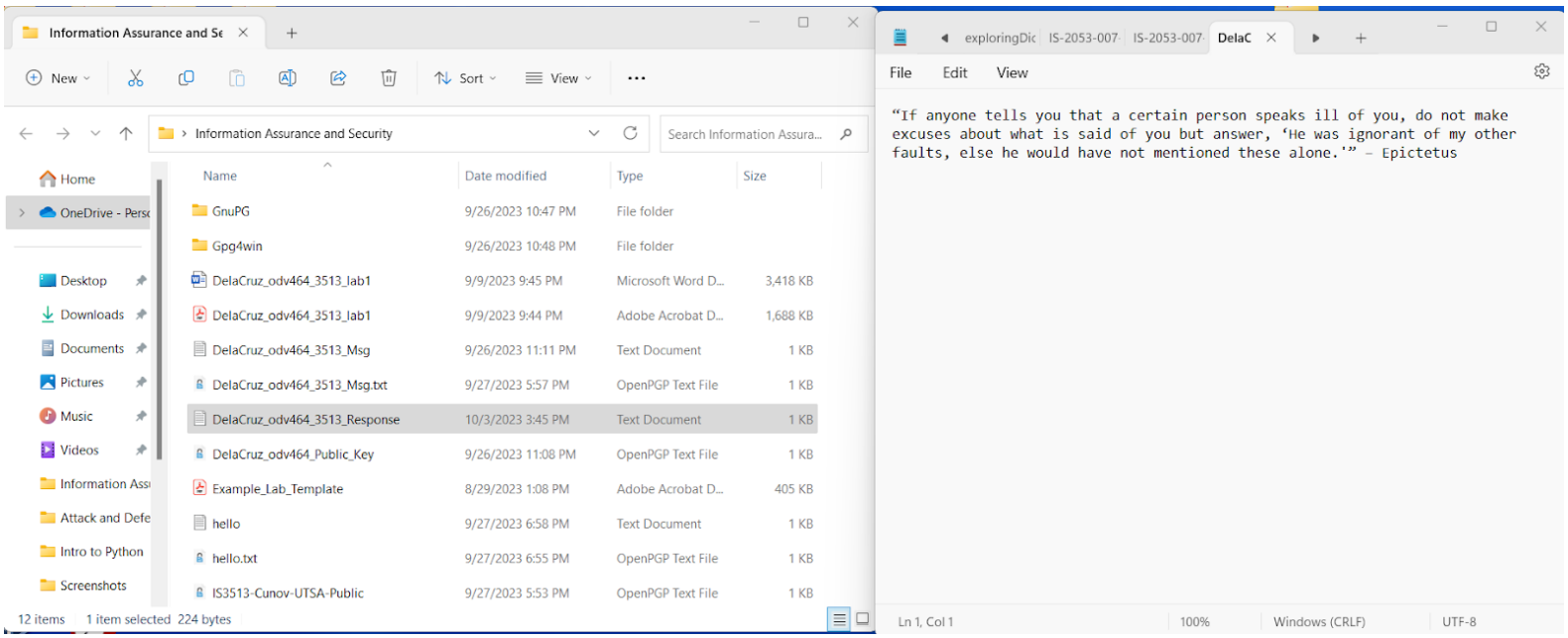
I created a text message using a text editor. I named the encrypted file using the convention 'MyLastname_abc123_3513_Msg.txt.'

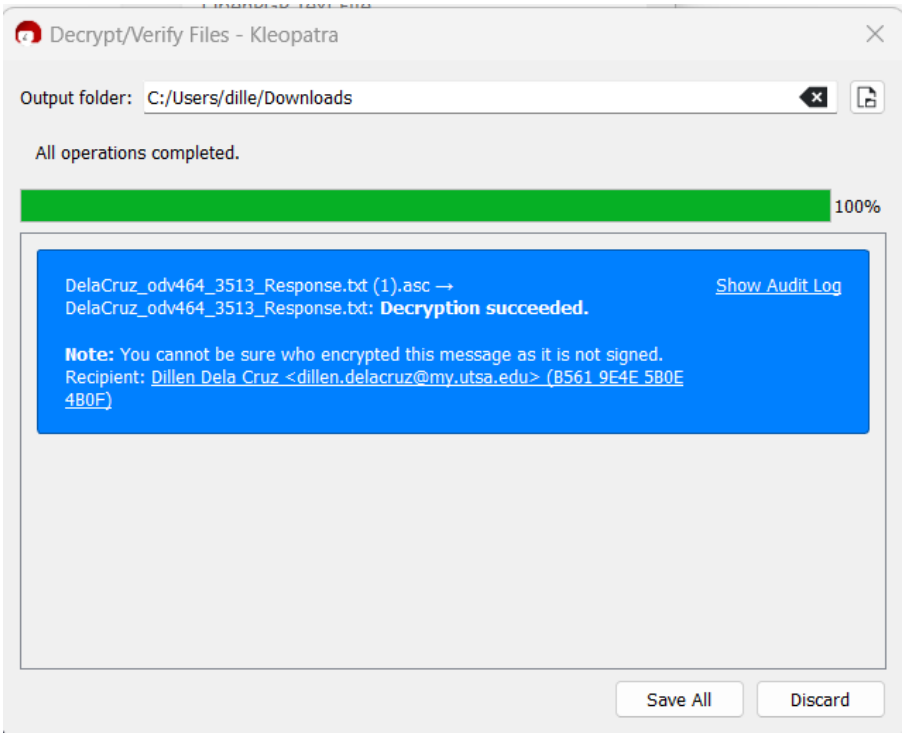
For the encryption process, it was important to set up Kleopatra correctly. So, I clicked on 'Settings,' then 'Configure Kleopatra,' and navigated to 'Crypto Operations,' where I selected 'Create signed or encrypted files as text files.' I also ensured that the file format would not be .gpg or .pgp.

To encrypt the text message using my professor's public key (and not mine), I chose the option 'Sign/Encrypt.' I located the text file I had created and selected 'Encrypt for others' using only his public key. Alternatively, I could have typed the message directly in the Notepad within Kleopatra, selected 'Recipients,' and chose 'Encrypt for others' using his public key. It was essential to include the '----Begin PGP Message----' and '----End PGP Message----' markers if I copied and pasted the message.

I made sure that he was the sole recipient of the message and did not sign it; I only encrypted it.

Finally, I sent both my public key and the encrypted message via email





For the last step, I downloaded my professor's response, which promptly opened Kleopatra. After saving the response to my chosen folder, it appeared as an unlocked text. From there, I was able to read the encrypted message given.

Figure 12 and 13: Decrypting Text

Conclusion:

In conclusion, this lab is designed to provide students with practical experience in encryption and decryption techniques through the use of PGP encryption with Kleopatra. Encryption, a method of converting information into a secret code, has a long history dating back to ancient civilizations like the Egyptians. The Caesar Cipher is one example of this practice. As technology has evolved, so too has encryption, with modern cryptographic methods relying on mathematical concepts such as number theory, modular arithmetic, and probability theory.

Encryption plays a vital role in ensuring the confidentiality, integrity, and availability of sensitive data. It offers two fundamental approaches: symmetric and asymmetric encryption. Symmetric encryption relies on a single key for both encryption and decryption, making it efficient and cost-effective for secure data storage. However, key distribution and management can become challenging on a larger scale.

Asymmetric encryption, on the other hand, uses two keys - a public key for encryption and a private key for decryption. It offers advantages like key distribution elimination and non-repudiation, making it suitable for secure communication between parties. However, it can be computationally intensive and less efficient for large data volumes.

In real-world scenarios, a combination of asymmetric and symmetric encryption is often used to secure data in motion or during transmission. Protocols like SSL/TLS exemplify this hybrid approach, establishing secure connections with asymmetric encryption and then transferring data within that secure environment using symmetric encryption.

The importance of encryption in cybersecurity is that it aligns with a few critical security controls (7,13,15), effectively safeguarding data's confidentiality, integrity, and availability. Moreover, it introduces the capabilities of non-repudiation and authentication, assuring the origin of data from a trusted source and preventing denial, thus further enhancing the principles of C.I.A.

Encryption tools like Gpg4win, which utilize both encryption and digital signatures, enhance data protection and authentication. GnuPG serves as the core encryption tool within Gpg4win, while Kleopatra simplifies certificate management and acts as the GUI for GnuPG.

Overall, this lab provides valuable insights into the world of encryption, preparing students to navigate the complex landscape of cryptography and to have a solid understanding of cryptographic principles.

Citation:

Introduction

Cryptography. “Caesar Cipher.” Computer Science, 25 April 2010, http://www.cs.trincoll.edu/~crypto/historical/caesar.html. Accessed 4 October 2023.

Cryptography. “Historical Ciphers.” Computer Science, http://www.cs.trincoll.edu/~crypto/historical/intro.html. Accessed 4 October 2023.

Encryption Consulting. “What is the difference between Symmetric and Asymmetric Encryption? Which is better for data security?” Encryption Consulting, https://www.encryptionconsulting.com/education-center/symmetric-vs-asymmetric-encryption/. Accessed 4 October 2023.

F5. “What is SSL/TLS Encryption? | F5.” F5 Networks, https://www.f5.com/glossary/ssl-tls-encryption. Accessed 5 October 2023.

GAO. “Science & Tech Spotlight: Securing Data for a Post-Quantum World.” Government Accountability Office, 8 March 2023, https://www.gao.gov/products/gao-23-106559. Accessed 4 October 2023.

Guide, Step, and Casey Crane. “Symmetric Encryption 101: Definition, How It Works & When It's Used.” The SSL Store, 4 November 2020, https://www.thesslstore.com/blog/symmetric-encryption-101-definition-how-it-works-when-its-used/. Accessed 4 October 2023.

Jain, Sandeep. “What is Asymmetric Encryption?” GeeksforGeeks, 20 March 2023, https://www.geeksforgeeks.org/what-is-asymmetric-encryption/. Accessed 5 October 2023.

Linkedin. “Symmetric vs Asymmetric Encryption Algorithms for File Systems.” LinkedIn, 1 September 2023, https://www.linkedin.com/advice/0/what-advantages-disadvantages-symmetric-asymmetric-2f. Accessed 4 October 2023.

Mann, Charles. “The science of encryption: prime numbers and mod n arithmetic 1. A Primer on Public-key Encryption.” Berkeley Math, https://math.berkeley.edu/~kpmann/encryption.pdf. Accessed 4 October 2023.

Net Spot. “WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences.” NetSpot, https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html. Accessed 5 October 2023.

RSI Security. “What are the 20 CIS Critical Security Controls?” RSI Security, 24 June 2020, https://blog.rsisecurity.com/what-are-the-20-cis-critical-security-controls/. Accessed 5 October 2023.

Saini, Ramraj. “Unlock The Secrets Of Cryptography With The Help Of Mathematics.” Careers360, 27 March 2023, https://www.careers360.com/premium/mathematics-in-cryptography. Accessed 4 October 2023.

Science Direct. “';;.'” ';;' - YouTube, 9 March 2019, https://www.sciencedirect.com/science/article/abs/pii/B9781597492836000039. Accessed 4 October 2023.

Simplilearn. “All You Need to Know About Asymmetric Encryption.” Simplilearn.com, 20 February 2023, https://www.simplilearn.com/tutorials/cryptography-tutorial/asymmetric-encryption. Accessed 5 October 2023.

Smirnoff, Peter, et al. “Symmetric Key Encryption - why, where and how it's used in banking.” Cryptomathic, 3 January 2020, https://www.cryptomathic.com/news-

events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking. Accessed 4 October 2023.

Stubbs, Rob, and Chris Allen. “An Overview of Symmetric Encryption and the Key Lifecycle.” Cryptomathic, 11 March 2020, https://www.cryptomathic.com/news-events/blog/an-overview-of-symmetric-encryption-and-the-key-lifecycle. Accessed 4 October 2023.

Tulane. “How to Learn Cryptography: Building Skills in Information Security.” Tulane School Of Professional Advancement, https://sopa.tulane.edu/blog/how-to-learn-cryptography. Accessed 4 October 2023.

UTSA. “Information Hiding and Cryptography.” docreader, 9 March 2019, https://docreader.readspeaker.com/docreader/?jsmode=1&cid=10662&lang=en_us&url=https%3A%2F%2Finst-fs-pdx-prod.inscloudgate.net%2Ffiles%2F9aa44937-6d98-4670-8676-4ca6aeb0fcc0%2FIS3513_02_02_Information%2520Hiding%25281%2529.pdf%3Ftoken%3DeyJ0eXAiOiJKV1QiLCJ. Accessed 4 October 2023.

Gpg4win, GnuPG, and Kleopatra

GnuPG. The GNU Privacy Guard, https://www.gnupg.org/. Accessed 5 October 2023.

gpg4win. “About Gpg4win.” Gpg4win, https://www.gpg4win.org/about.html. Accessed 5 October 2023.

GPG4win. “Features.” Gpg4win, https://www.gpg4win.org/features.html. Accessed 5 October 2023.

Singer, David, and Step Guide. “What Is GPG Encryption and Do You Need It?” Liquid Web, 12 February 2021, https://www.liquidweb.com/kb/is-gpg-still-useful-in-todays-insecure-world/. Accessed 5 October 2023.

Tails. “Encrypting text and files using GnuPG and Kleopatra.” Tails, https://tails.net/doc/encryption_and_privacy/kleopatra/. Accessed 5 October 2023.