William Adams
Lab two: Encryption
IS 3513-002
October 8, 2023
Professor Wooldridge

The security and privacy of data and communications are of the utmost importance in today's society, which is becoming more digital and networked. Sensitive data protection is now a crucial concern in order to keep it safe from prying eyes and malevolent actors. In the second lab, Encryption, the objective of this lab was to get familiar with methods of encryption with emails and files. I used Kleopatra for the first time and did gain some knowledge on encrypting and decrypting messages. I have always been fascinated with the idea of encryption in the cyber space. The idea of encrypting data to make it where non authorized people can’t view it is fascinating to me. I have no prior experience with encrypting messages, so I was excited to get some experience with this skill.

In the beginning of the lab where I had to go to the “https://www.gpg4win.org/”, I have a mac laptop, so it was a little challenging to be able to install Kleopatra without having windows. I could have done a windows emulator, but I do have another windows laptop in my household that I could use to do the lab so that’s what I ended up doing. The download went very easy and was installed in about 30 seconds, it was also very easy to set up my OpenPGP key by just following the steps on the lab instructions. After I got my key, all set up and running, I went to the blackboard and downloaded the instructor’s key. After I downloaded the instructors key, I sent him an email of my public key that I had made. In the sixth step where we had to create a text message with a text editor, there was some hurdles that I had to overcome. At first, I thought I was supposed to make my message on Kleoatra, but I saw the instructions that said we were supposed to do it on word or notepad, so I did that instead. I went on notepad and made my message (what my favorite movie was). I then went back to Kleopatra and copied my message into clipboard, these steps to do get my message encrypted were easy to follow, as I was following the instructions the instructor gave us. I thought this part of the lab was very interesting and fun, having that message that I made get encrypted was very cool to me. I got the email that you got my message which was good to see to know I followed the right steps. I did mess up a little on the email at first because I didn’t make the right subject line, I then fixed it sent another email with my message. This skill can be very useful to a cyber security worker with encrypting sensitive data. The last part of the lab that I had to execute was decrypting the message that the professor gave me on the email. I did have a small mistake on this step because I was copying a wrong encrypted message and not the one, he gave me. After I figured out my mistake it worked, the message I got was: “but there is another reason for the high repute of mathematics: it is mathematics that offers the exact natural sciences a certain measure of security which, without mathematics, they could not attain. ~ Dr. Albert Einstein.”

In conclusion, I gained some knowledge and some needed experience with encrypting emails and files. I would like to keep exploring with encryption so that I can be more conformable with this skill because I believe it is very important. I didn’t have any major issues with this lab, which was nice, the only problem I had really was that I didn’t have a windows computer that I was currently using but that wasn’t a big problem. This lab provided a practical understanding of encryption and PKI. This lab has taught me the significance of using PKI and how it can be used in the real world, and I am beyond excited to take a deeper dive into it.

In today’s internet world, organizations rely on PKI to secure digital communication and sensitive data. With how much of our world is online, having the invention of PKI is a necessity. “In the early 1970s, the invention of Public Key Infrastructure (PKI) at the British intelligence agency GCHQ was first developed.” (Monton) I was honestly surprised on how early it was invented; malicious actors have on the internet for many of years so it makes sense on how early you would want to invent this. “The most common form of encryption used today involves a public key, which anyone can use to encrypt a message, and a private key (also known as a secret key), which only one person should be able to use to decrypt those messages.” (What) With this lab giving me some experience about encrypting emails and files, I thought this was how the use of public keys play in cyber.

For the WHO it can benefit for an organization by the use of PKI, I feel like this can only help everyone that is involved with the organization. This will benefit any organization that deals with sensitive data, financial transactions, or sensitive customer information. This also helps keep the integrity and confidentiality of the organization by keeping the customers sensitive information secured from unauthorized users. The person that benefits the most from the use of PKI is the organization, without the integrity of the origination you won’t be able to last long term. “Health insurer Anthem says the hacked database containing the personal information of 80 million people wasn't encrypted.” (Whitney) In this article that I found on the internet, this organization had over 80 million people’s personal information, mainly members and employees. It came out that the information wasn’t encrypted, and the organization didn’t have to encrypt their data. This can be detrimental for an organization because you have lost the integrity of the organization by having employees and members of the organizations personal information being leaked.

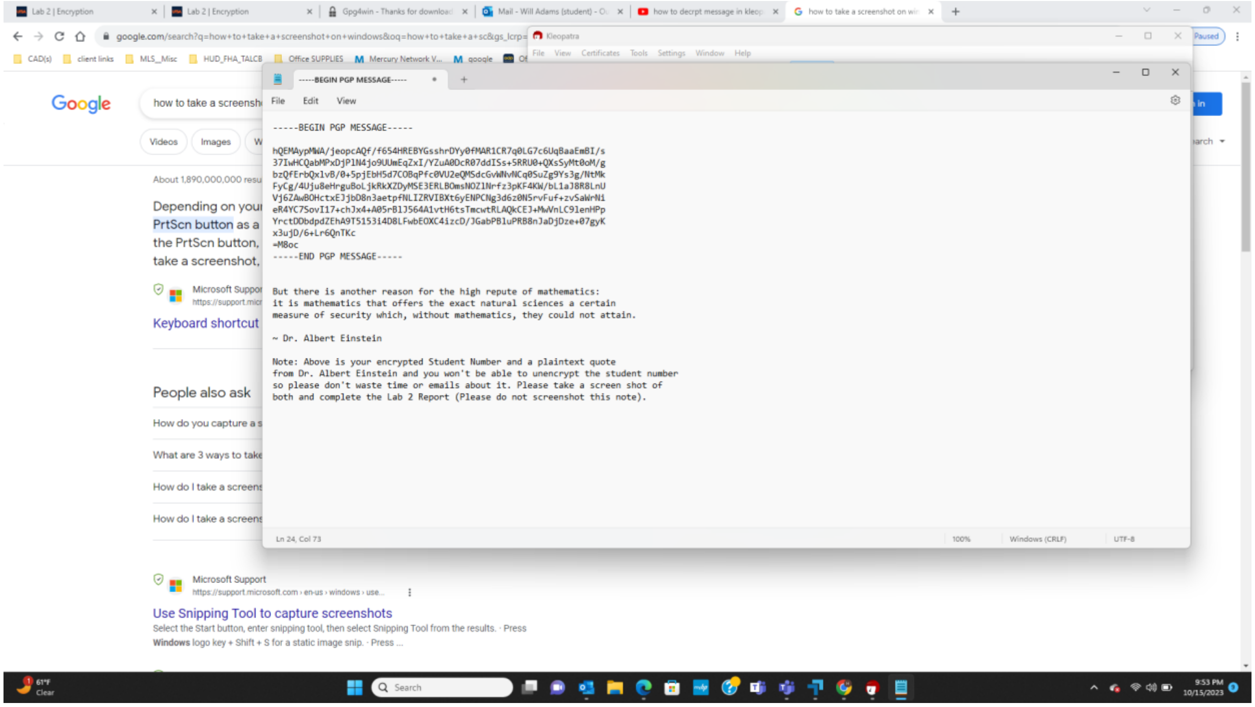
For the WHAT it can benefit for an organization by the use of PKI, it can benefit long-term success as an organization by having secure security procedures such as encryption. With the use of encryptions tactics, I do believe that can make an organization feel more trusted by future clients or employees to work with them. Asymmetric cryptography is used in PKI, a multidimensional security architecture, to safeguard digital communication and data. Each user in this system is given two cryptographic keys: a public key that is meant to be shared widely and a private key that should be kept to themselves. Messages and data are encrypted using the public key, making them inaccessible to unauthorized parties. The owner can access the original data by using the private key, which is used to decrypt data. This can be very valuable to have for any organization, having the ability to secure communications, data privacy, and digital identity verification is crucial. I think it is pretty interesting on the different types of keys there are as well, how you have your public keys and private keys which is pretty fascinating to me how they both have different uses and functions.

For the WHEN it can benefit for an organization by the use of PKI, I don't think there's any specific "when" because it can be used at all times to protect data from being broken into. It is relevant at all time periods because cyber-attacks happen 24/7. As cyber-attacks become more and more sophisticated, organizations need to adapt their security measures, and this is one of the best practices to do so. "Nearly 4000 new cyber-attacks occur every day. Every 14 seconds, a company falls victim to a ransomware attack, which can result in devastating financial losses while 560,000 new pieces of malware are detected every day." (James) Having almost 560,000 attacks basically every single day is just insanity to me. The need to take every security procedure you can is crucial because of how vulnerable organizations are, even if you have the best security budgets and teams. Especially with how much data and sensitive information that is transmitted and transported every single day in today's internet world, it is crucial to add extra layers to your security.

For the WHY it can benefit for an organization by the use of PKI, it enhances security by protecting data from unauthorized users' access, ensuring data integrity, and preventing future breaches. There are tons of reasons why I believe that the use of PKI can benefit an organization but the main reason I see is that it can stop unauthored users from viewing sensitive information. "The importance of encryption cannot be understated in the slightest because even the biggest corporations with the largest cybersecurity budgets fall victim to data breaches. That being said, even if your data is in a secure infrastructure, there is still a chance that your data could be compromised. With data encryption, however, your files can be that much more impenetrable even if they were stolen." (Chen) I found this quote to be very fascinating to me because even the companies that have the highest of budgets with their security, they still have multiple breaches. Malicious actors have always found new ways to breach systems no matter how many patches and updates security teams put in, so the addition of encryption can only help with the security of an organization. With cyber-attacks making organizations lose billions of dollars every year, I don't see a reason why organizations wouldn't want to take that extra step and encrypt their important data.

For the HOW it can benefit for an organization by the use of PKI, with the implementation of PKI within an organization, there are tons of ways these big organization can utilize these techniques. Some of the ways they can use encryption are to secure email communication, digital signatures, and the encryption of sensitive data. With big organizations having a lot of confidential information to handle, it is essential to encrypt the information so unauthorized users can’t view it. “Data encryption protects your sensitive data by rendering it inaccessible, even if stolen. Decrypting well-encrypted data without the key is theoretically possible, but it would require all the world’s computing power and many years to succeed.” (Cocoara) I found this quote to be very interesting because if you encrypt your data well it’s almost impossible to decrypt it.

Appendix



```
-----BEGIN PGP MESSAGE-----

hQEMAypMWA/jeopcAQf/f654HREBYGsshrDYy0fMAR1CR7q0LG7c6UqBaaEmBI/s
37IwHCQabMPxDjPlN4jo9UUmEqZxI/YZuA0DcR07ddISs+5RRU0+QXsSyMt0oM/g
bzQfErbQxlvB/0+5pjEbH5d7COBqPfc0VU2eQMSdcGvWNvNCq0SuZg9Ys3g/NtMk
FyCg/4Uju8eHrguBoLjkRkXZDyMSE3ERLBOmsNOZ1Nrfz3pKF4KW/bL1aJ8R8LnU
Vj6ZAwBOHctxEJjbD8n3aetpfNLIZRVIBXt6yENPCNg3d6z0N5rvFuf+zvSaWrNi
eR4YC7SovI17+chJx4+A05rBlJ564A1vtH6tsTmcwtRLAQkCEJ+MwVnLC9lenHPp
YrctDDbdpdZEhA9T5153i4D8LFwbEOXC4izcD/JGabPBluPRB8nJaDjDze+07gyK
x3ujD/6+Lr6QnTKc
=M8oc
-----END PGP MESSAGE-----


But there is another reason for the high repute of mathematics:
it is mathematics that offers the exact natural sciences a certain
measure of security which, without mathematics, they could not attain.

~ Dr. Albert Einstein

Note: Above is your encrypted Student Number and a plaintext quote
from Dr. Albert Einstein and you won't be able to unencrypt the student number
so please don't waste time or emails about it. Please take a screen shot of
both and complete the Lab 2 Report (Please do not screenshot this note).
```

Figure 1 decryption message that I got.

Bibliography

Chen, S. (2023, June 12). *What is Data Encryption and why is it important?*. TitanFile. https://www.titanfile.com/blog/what-is-data-encryption-and-why-is-it-important/

Cocoara, Z. (2023, February 24). *Five key benefits of data encryption for Security*. Endpoint Protector Blog. https://www.endpointprotector.com/blog/five-key-benefits-of-data-encryption-for-security/#:~:text=How%20does%20data%20encryption%20help,and%20many%20years%20to%20succeed.

Monton, A. (2021, December 14). *History of the internet: The development of PKI*. GlobalSign. https://www.globalsign.com/en-sg/blog/history-internet-development-pki#:~:text=In%20the%20early%201970s%2C%20the,PKI%20discoveries%20were%20made%20public.

Scarfone, K. (2022, April 14). *The benefits and challenges of managed pkis: TechTarget*. Security. https://www.techtarget.com/searchsecurity/tip/The-benefits-and-challenges-of-managed-PKIs

What is PKI? A public key infrastructure definitive guide. Keyfactor. (2023, June 23). https://www.keyfactor.com/education-center/what-is-pki/#:~:text=What%20is%20PKI%3F-,A%20Public%20Key%20Infrastructure%20Definitive%20Guide,end%2Dto%2Dend%20communications.

Whiteney, L. (n.d.). *Anthem's stolen customer data not encrypted*. CNET. https://www.cnet.com/tech/services-and-software/anthems-hacked-customer-data-was-not-encrypted/