Cryptography and Network Security

Saint Leo University

COM 450- Network Defense and Security

Instructor: Dr. Omar

Group members:

Ivanna, Tracey, Romario, Chevon

March 13, 2018

Abstract

This paper will look at different aspects of Cryptography, including different Cryptography techniques, past use of Cryptography and present use of it. The paper will

look at how Enigma was used, and will also focus on Symmetric and Asymmetric encryption, to understand RSA Cryptography and Digital Signatures. We will go in depth with our explanation of how each technique works and our findings about such techniques.

Asymmetric vs Symmetric Encryption

Cryptography utilizes encryption and decryption to ensure secure, private communication (Rivest). Encryption is the process of converting a message into a

secret, unreadable code while decryption is the process of converting the unreadable code back to plain text (Bishoi). In computer science, we carry out these processes through the use of algorithms and keys.

There are two basic types of encryption [and decryption], symmetric and asymmetric. In symmetric encryption, a key is used to both encrypt and decrypt the message. When a message is encrypted using a key, the person who it is being sent to must have a matching public key to decrypt it.This method of encryption is called ‘secret key’ encryption as the public key must be kept private considering it is used for both encryption and decryption.

On the other hand, asymmetric encryption uses both a public key and a private key. While in symmetric encryption, each user is only given a public key, in asymmetric encryption each user is given a public key and private key pair. The known public key, from the person who is sending the message, is used to encrypt the message however, a private key, belonging only to the person who is meant to receive the message, is needed to decrypt it. This method is called public key encryption because the key used to encrypt is published, however the key used to decrypt is kept secret (Bishoi).

Symmetric and asymmetric encryption have many more differences than the fact that they use different keys. Asymmetric encryption uses much more processing time and resources than symmetric encryption. Additionally, symmetric encryption provides a small amount of authentication considering the person’s key must match while in asymmetric the private key is related to the person receiving, not both (Bishoi). However, symmetric encryption is much less secure than asymmetric encryption as once the key is found then it can easily be decrypted. Symmetric is also less secure

because communication can be intercepted when the key is being shared, while in asymmetric there is no need to share the key and it therefore cannot be intercepted.

RSA Cryptography

RSA Cryptography, which gets its name from its founders: Rivest, Shamir, and Adelman, is a type of cryptography that makes use of asymmetric encryption. The RSA technique uses large complex prime numbers for encryption, which makes it more very difficult to decipher without knowing the private key. According to Makaar and Singh, the "RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm" because of the level of security it provides (Makaar and Singh, 2013).

The RSA algorithm is one which makes use of the fact that it is easy to find the product of two large numbers, but difficult to factor a large product and find the original numbers. The algorithm does have its flaws however. If the prime numbers that are selected are too small, then it might not be too difficult to decipher the key "by using random probability theory and side channel attacks," and if the prime numbers that are selected are too large, then "it consumes more time and the performance gets Degraded" (Singh and Kinger, 2013). Therefore, the primes used for creating the keys have to be strategically selected.

RSA has a number of uses. RSA could be used to encrypt users' data and messages across the internet, but because it is relatively slow, it is mostly used for exchanging private keys for symmetric cryptography. It is also used to authenticate digital signatures particularly for emails. Also, the Secure Socket Layer (SSL) in TCP/IP networks use RSA Cryptography for exchanging the keys for authenticating a SSL certificate (Simpson, 1997).

While RSA Cryptography provides quite a good level of security, as with any information or network security technique, there are are still attacks that can compromise its security. Attacks on RSA include Low Private Exponent, Partial Key Exposure, and Implementation (side-channel) attacks. Thus, RSA is usually used in combination with other cryptography techniques.

Enigma

The enigma machine provided a significant contribution to cryptology and network security. A German engineer named Arthur Scherbius invented the machine and was used by Nazi Germany in World War II. During this period, it encrypted the intel messages sent between the German soldiers. It was noted to be impossible to decrypt, and for a while, many believed that it the would never be solved.

The enigma machine was made up of several components which included a 26-letter keyboard, 26 lamps (to show letters), a power supply, removable wired wheels, fixed wired reflector, and a fixed wired entry wheel (Churchhouse, 2002). The level of security that it provided came from how the machine was able to encrypt and decrypt its messages. The sender would type the word that they wanted into the machine and it would be translated before outputting the encrypted message. This encoded message would seem like gibberish to others who did not have an enigma machine at their disposal. The receiver, who would have access to the machine would then type this message into the enigma machine, which would decrypt the message. However, what made the enigma machine so complex, was the fact that the letters were being randomly scrambled each time. Additionally, the extra layer of security came from the

fact that the receiving enigma machine must have been set up the same way the sender machine was.

Alan Turing eventually found a way to decrypt the German enigma machine by studying the Germans instead of the machine. The machine itself was successful in encrypting messages, but the way the Germans had used it was the key to solving the riddle. They have used a specific receiving operation to ensure that the messages were decoded successfully, which led to their messages eventually being decrypted (Churchhouse, 2002). It is undisputed that the enigma machine holds great significance in both the world of cryptography and our own history.

Digital Signatures

The times of needing to obtain a signature have changed. It used to be that when a time-sensitive document needed to be signed, it was a long process. It either had to be mailed or printed and signed then sent back to the sender. However, a digital signature is continuing to grow as a way of meeting the need for faster and more secure authentication that cannot easily be forged or compromised.

There are a couple of ways you can break down a digital signature. The best example of a digital signature is at the bottom of your email. It will look like useless text or just some random information, but in fact, that set of random text will be your digital signature. Your signature is made using algorithms and the combination of two files one that holds the message and another that contains information in a key (McDowell, M., & Householder 2009). The reason why the digital signature is used is to make sure the email has not changed and to make sure the email is from the person that sent it.

The digital signature uses a standard global protocol called Public Key Infrastructure, and it creates two keys. There is a public and private using mathematical algorithm. The public key and private key are linked mathematically to each other. A hash is a unique digital fingerprint is created by using the signer private key. The hash is used only for the specific document(Turner 2015). There cannot be any changes or the digital signature would become invalid.

The real reason digital signature is around is to keep your computer safe from spoofing. Spoofing is somebody sending your email a virus trying to hack into your network system. People fall for this trick a lot because of not checking there digital signature which will tell you if the email has been changed in any way. Any change to a digitally signed document renders the signature invalid hence the digitally signed document cannot be altered without detection. If the digital signature has any change to it do not open it, this goes to say that a hacker is trying to get into your network system.

Conclusion

To conclude, cryptography is the art of encrypting and decrypting data. There are two basic ways of encrypting data, asymmetric and symmetric, which have evolved to increase the efficiency of cryptography. This includes techniques such as RSA cryptography, machines such as the enigma and communication methods such as digital signatures.

References

Bishoi, Tanmoy & Ghosh, Ramkrishna & Sinha Roy, Tanmoy. (2015). AN ALGORITHM ON TEXT BASED SECURITY IN MODERN CRYPTOGRAPHY. 5. 9-14.

Churchhouse, R. F. (2002). Codes and Ciphers : Julius Caesar, the Enigma, and the Internet. Cambridge: Cambridge University Press.

Maakar, S.K., & Singh, S.L. (2013). A Performance Analysis of DES and RSA Cryptography.

McDowell, M., & Householder, A. (n.d.). Security Tip (ST04-018). December 17, 2009, from https://www.us-cert.gov/ncas/tips/ST04-018

Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier.

Simpson, S. (1997). Cryptography in Everyday Life. Retrieved March 13, 2018, from http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/life.html

Singh, Gurpreet & Kinger, Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. International Journal of Computer Applications. 67. 33-38. 10.5120/11507-7224.

Turner, Dawn M. “What Is a Digital Signature - What It Does, How It Works.”*Cryptomathic - Security Solutions*, 10 Dec. 2015, www.cryptomathic.com/news-events/blog/what-is-a-digital-signature-what-it-does-how-it-works.

Young, Bill. “Lecture 44: Symmetric vs Symmetric Encryption.” Foundation of Computer

Security. Department of Computer Science, University of Texas at Austin.