MEMORANDUM

TO: Thomas Davis, Professor

FROM: Matthew Sutton

DATE: February 13th, 2017

SUBJECT: Feasibility Assessment for a Report on Public-Key Cryptography

Public-key cryptography, also known as asymmetric cryptography, has been publically used since 1976 to encrypt messages without first communicating a shared secret (also known as a key) (Gaithuru, Bakhtiari, Salleh, & Muteb, 2015). It is this concept of non-secret encryption that makes public-key cryptography a popular solution for secure communication. A report on the functionality of public-key cryptography can be informative to those wishing to understand a system for secure communication. Being security-savvy in the digital age will help prevent unauthorized modification and prevent unauthorized disclosure of private information. This memo analyses my preliminary research on the subject and demonstrates the feasibility of a report on public-key cryptography.

Significance of Public-Key Cryptography

As the world has become more and more connected by technology, it has become obvious that our communications need to be secured. Every day there are new data breaches reported in the news. White-hat security researchers, black-hat hackers, and state-sponsored entities are repeatedly finding new ways to eavesdrop and manipulate all forms of digital communication. This has led to a loss in integrity and confidentiality of data in our world. However, there are safeguards that can be put into place to protect against eavesdroppers. The main defense against these adversaries is encryption: a reversible mathematical function to convert information into an incomprehensible form, called ciphertext, where only those who are authorized to view the information can return the ciphertext back to its legible plaintext. The process of reversing the ciphertext to plaintext is termed decryption.

Encryption has two forms: symmetric and asymmetric. Symmetric cryptography (private-key cryptography) uses a single key to encrypt and decrypt. A fundamental problem with symmetric cryptography is securely communicating the key between sender and recipient. The key must have been pre-shared through another secured medium, or you risk the key being exposed to eavesdroppers during its transit through the Internet. So, if you wanted to send an encrypted message to a new recipient, how do you reasonably guarantee secure transmission of keys? Asymmetric cryptography (public-key cryptography) will help you securely exchange keys by using a two-key pair during the encryption and decryption processes. Each enrolled user has a private key they must secure and a public key that can be openly distributed to those who wish to message them. Anything encrypted using a public key can only be decrypted by the same corresponding private key and vice-versa. Public-key cryptography also creates the ability for users to authenticate each other using digital signatures (Gaithuru, Bakhtiari, Salleh, & Muteb, 2015). For example, Bob can digitally sign his own message by encrypting it with his private key. Any recipient of Bob's ciphertext then must use the bob's public key to decrypt. If the process is successful, you can be reasonably sure the message came from Bob because only Bob can release messages that can be decrypted by his public key.

Purpose of Report

This report will deconstruct all the fundamentals and terms for public-key cryptosystems. For example, the straightforward cryptosystem, RSA, will be broken down and its mathematics demonstrated. A reader will get the full explanation of the asymmetric encryption process described using text, figures, and flowcharts. They will also gain all the knowledge they need to be able to send and receive encrypted messages using public-key cryptography software. Anyone could take this report, read it, and fully understand all the fundamentals of public-key cryptography.

Intended Audience

The audience for this report is a layperson who wants to learn how to secure their digital communications. This could be a student, manager, teacher, small business owner, etc. It is a good idea to start securing your communications, and your high-risk data, with encryption. I assume that my audience has a normal understanding of computer operation. They should be able to easily navigate their operating system. I will also assume that they have at least some college education, or at least couple years of experience working an information technology job. Most probably, the audience will know nothing about encryption practices because it is not a common study. Encryption was, for me, not taught anytime during K-12 education. Overall, the report will give a layperson all the information they need to understand and start using public-key encryption.

Scope of Report

The major pieces of public-key cryptography I will write on are: what currently uses asymmetric encryption, the risks of not using encryption, the initial required definitions, how asymmetric encryption works, how the keys are generated, how to secure the private key, how the RSA cryptosystem works, and how to start using public-key message software (such as Pretty Good Privacy). I may touch on some additional topics, such as the future of public-key cryptography, if I need to add additional length to the paper.

People are always discovering new ways to apply asymmetric cryptosystems, but these methods are too complex for a lay audience to understand. A lot of advanced mathematics are involved that may lose an encryption-novice reader. For instance, an elliptic curve cryptosystem (ECC) uses points from an X/Y graph with a large wobbly line (that looks similar to a standard doorknob) to encrypt and decrypt. ECC takes advantage of the difficulty in solving the discrete logarithm problem rather than integer factorization (Gaithuru, Bakhtiari, Salleh, & Muteb, 2015). A good contrasting example is to imagine ECC as calculus and RSA as algebra. I have decided to only explain cryptosystems that have an algebra level of math to prevent incomprehension.

Experience with Public-Key Cryptography

I have taken the cryptography course here at UNO for my major. Symmetric and asymmetric cryptosystems were covered intensively. We discussed many public-key methods for secure key exchanges. During my final examination, RSA was used during test questions. I had to do all the calculations for RSA by hand. With respect to actively applying public-key encryption concepts in software, I have used Pretty Good Privacy (PGP) which uses public-key encryption to send emails. My last tidbit of experience comes from my employment at Offutt Air Force Base. We used public-key encryption for secure military email.

Potential Problems

It may be difficult to accurately break down encryption concepts into language for a lay audience. I will have to work hard to condense information into simpler arguments and come up with analogies to help my audience understand valuable concepts. There are some formulas I will need to input. Designing these formulas in Word using the Insert Equation function can sometimes be difficult. I hope to make the formulas easily readable.

Result of Research Conducted

Journals

Using the UNO Criss Library database search tools, I identified IT-focused databases and began my journal searches. The best databases for my topic were Academic Search Complete, IEEE Xplore, and the ACM Digital Library. Most searches turned up over 40,000 results. The downside is that much of the current articles on public-key cryptography are on advanced topics outside the scope of this paper. I was still able to find many good resources, although they are very old sources. I believe I know enough about this topic to differentiate between good and outdated material in my older sources. Three journal sources I found and their APA citation follows:

Gaithuru J. N., Bakhtiari M., Salleh M., & Muteb A. M. (2015). A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. *2015 9th Malaysian Software Engineering Conference (MySEC)*, 236-244. doi: 10.1109/MySEC.2015.7475227

Odlyzko, A. M. (1994). Public Key Cryptography. *AT&T Technical Journal, 73*(5), 17-23. doi:10.1002/j.1538-7305.1994.tb00606.x

Price, G. (2006). Public Key Infrastructures: A research agenda. *Journal of Computer Security*, *14*(5), 391-417.

Web sites

Google was my go-to for finding websites. Unfortunately, Google scholar did not have the type of whitepaper websites I was hoping to find. A standard Google search allotted me much more valuable content to work with. There are a lot of vendors and large companies that have guides for setting up public-key cryptography. I also found looked a good source for easy RSA mathematics. Three website sources I found and their APA citation follows:

Introduction to Digital Certificates. (n.d.). Retrieved February 02, 2017, from https://www.comodo.com/resources/small-business/digital-certificates-intro.php

Ouwehand, M. (2001, July 19). The (simple) mathematics of RSA. Retrieved February 02, 2017, from http://certauth.epfl.ch/rsa/rsa.html

Understanding Public Key Cryptography. (2005, May 19). Retrieved February 02, 2017, from

https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

Research Strategy

I do not plan to do any primary research because there is a decades of secondary research into public-key cryptography. However, to achieve comprehensive research, I will need to pull from more than journal articles and websites. I own three textbooks on cryptography that will greatly aide my research. I plan to re-read important chapters to gain a deeper understanding of the relevant topics. The JSTOR database also now has access to many books. During my preliminary research, I found a few books on JSTOR that may help me write my comprehensive report. The journal articles I have skimmed are good at explaining newer topics, so I believe these JSTOR books will give me more information of the basic topics of public-key cryptography that are more aligned with the scope of this paper. Essentially, I will comb through all my reading material and note all applicable secondary research, categorize the research, and then insert the most vital secondary research my document.

Research Costs

My research costs will be low because almost all the research I will do for this report will come from the Internet. The mandatory UNO Library Fee has covered my expenses for searching through journal databases. Without this fee, project costs would have climbed much higher due to the need to pay for journal subscriptions. I will need to drive to the library, and to class, which should not take more than 10 gallons of gas. My house is very close to campus. When the weather gets warmer I may walk to campus to cut gas costs. My final expenses are purchasing home printing materials.

Item	Quantity	Cost
UNO Library Fee	1	$56.20
Gas	10 Gallons	~$25.00*
MavCard Printing	20	$1.40
EPSON DURABrite Inkjet Ink – Black	1	~$16.00*
EPSON DURABrite Inkjet Ink – Multicolored	1	~$25.00*
HP All-In-One Printing Paper 8.5x11in – 500 sheets	1	~$5.00*
	Total:	**~$128.60**
	***Taxable Amt:**	**$71.00**
	Sales Tax (7%):	**$4.97**
	Grand Total:	**~$133.57**

Research Schedule

Quasi-daily, I will read new journal articles and websites over the next six weeks to document important information that could be used in the report. The overall research schedule will align with the class syllabus' course schedule. I believe it is best to use deadlines that align with when important assignments are due. This way, I will stay on track with class requirements. The Assignment 3 due date will be my one-hundred percent research completion point. A little under two months' time is a large enough period to complete all my research.

Date	Topic	Research Goals

February 21st	Peer Review 2	50% Complete – I have a good amount of information processed and inputted into my cover letter and proposal. Only a few more materials should be left for me to read their first time.
February 23rd	**Assignment 2 Due**	55% Complete – I have inputted final touches on Assignment 2 and am still working to complete research.
March 28th	Peer Review 3	95% Complete – By this stage, it is important to have almost all of my research complete so I can begin to organize and design the report.
March 30th	**Assignment 3 Due**	100% Complete – I have completed all final research and am beginning a major examination of the paper. Proofreading and organization focus begins.

Conclusion

With my report a layperson will be able to properly defend themselves from the threat of eavesdroppers. Encryption allows for the secure transfer of information between two parties over an unsecure medium. By encrypting your information into ciphertext before transmission, any entity that may be snooping on traffic will need to brute-force the decryption key. The processing time needed to brute-force a key will take ages to finish, thus, leaving your data intact for years. This is an important skill anyone can use to create secure communications between themselves and another party. Encryption is not going anywhere because it is the backbone of all confidential communication on the Internet. Knowing encryption skills may one day prove useful to you when confidential information must be sent over an unsecure network.