Proposal for a Report on Public-Key Cryptography

for

Thomas Davis

University of Nebraska at Omaha

by

Matthew Sutton

Advanced Writing for IS&T

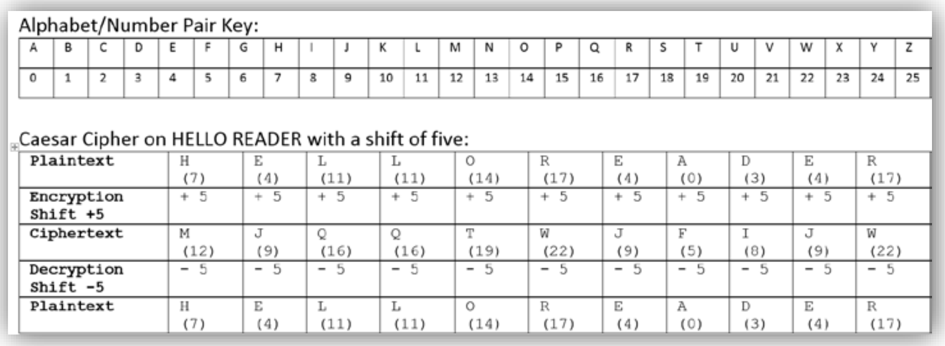
March 2, 2017

Approach

Problem Statement

Cryptography is defined as “the science and art of designing and using methods of message concealment” (Barr, 2002, p. 2). It involves two main processes termed encryption and decryption. Encryption is a reversible mathematical function to convert readable information (plaintext) into an incomprehensible form (ciphertext). Decryption is the mathematical process of reversing ciphertext back into its readable plaintext form. Cryptography has helped many civilizations keep their top secrets confidential for millennia (Barr, 2002, p. 5). For more grasp on the usage of cryptography terms see Figure 1.

Fig. 1. Using the Caesar Cipher to encrypt and decrypt plaintext “HELLO READER” to ciphertext “MJQQT WJFIJW” using a shift of five letters.



Alphabet/Number Pair Key:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher on HELLO READER with a shift of five:

Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)
Encryption Shift +5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5
Ciphertext	M (12)	J (9)	Q (16)	Q (16)	T (19)	W (22)	J (9)	F (5)	I (8)	J (9)	W (22)
Decryption Shift -5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5
Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)

The two classifications of cryptography used today are symmetric and asymmetric (Gaithuru, Bakhtiari, Salleh, & Muteb, 2015, p. 236). Secret-key cryptography (symmetric cryptography) uses a single private-key to encrypt and decrypt. A fundamental problem with secret-key cryptography is securely communicating the key between sender and recipient. The key must have been pre-shared through another secured medium, or there is some risk the key may be exposed to eavesdroppers during its transit through the Internet. To counter this problem, the concept of public-key cryptography (asymmetric cryptography) was developed by Stanford University researchers in 1976 (Gaithuru, Bakhtiari, Salleh, & Muteb, 2015, p. 237).

Public-key cryptography works by creating a public/private key-pair for every party. Each party will make their public-key openly accessible, and will conversely secure their private key for their eyes only. To send a message using public-key cryptography, you encrypt the message using your recipient’s public-key and then transmit the ciphertext to them. The recipient then decrypts the ciphertext with their private key. Public-key cryptography is used for the broad concepts of key exchange, digital signatures, and message authentication (Barr, 2002, p. 243). More specifically, some applications of public-key cryptography are: encrypted e-mail, encrypted Internet browsing using HTTPS, e-commerce and mobile banking, authentication of smart phones and tablets, citizen passports, and mass transit ticketing (Moulds). Public-key cryptography must be adopted to allow widespread encryption to be practical (Moulds). Overall, my work will result in a comprehensive report on the concepts of public-key cryptography. A lay audience will understand the fundamentals of secure communication using public-key cryptography.

Scope of Work

The full project will include a technical report and presentation on cryptography with a focus on public-key cryptography. I estimate the report to be 15 pages long. I will also be writing two cover letters, one style sheet guide, one presentation outline, and one transmittal letter. I will develop many figures and examples to help the audience understand important concepts. Specifically, I will be creating: an example problem using the Caesar Cipher, a diagram explaining the basics of public-key cryptography, an example problem using the Diffie-Hellman Key Exchange protocol, and an example problem using the RSA cryptosystem. The report with end with a full reference list.

The presentation will condense the report into a ten-minute window. I may not be able to fit all the concepts from the report into the presentation. Testing will need to be done to determine how much content will fit within the time limit. I plan on starting the presentation with cryptography fundamentals and terminology. The presentation will then move into public-key cryptography and close out with the applications of the RSA cryptosystem.

Identification of Audience

This report is for entities and individuals who are interested in learning a protocol for establishing secure communication without requiring a previously shared secret key. This could be an individual who wants to obtain more knowledge about privacy and confidentiality in the digital world, or maybe a company that wishes to establish secure channels over their network. A high-level manager who is being persuaded by his IT staff to implement network encryption could use this report to gain a fundamental understanding of cryptography before making important decisions.

This report is geared toward a lay person who is new to cryptography. Cryptography classes are not common through K-12 standard education. Only those who are interested in subjects such as computer science, web development, and cybersecurity may have been exposed cryptography. I will assume my audience is familiar with an algebra level of math. For those who already understand cryptography concepts, this report will help them review their cryptography knowledge. For others, this report will serve as a comprehensive exploration into the science of cryptography with a focus on public-key cryptography.

Author's Qualifications

I have taken the cryptography course here at UNO for my major. Symmetric and asymmetric cryptosystems were covered intensively. We studied many public-key methods for secure key exchanges. During my final examination, the RSA cryptosystem, which I will be covering in this report, was used for test questions. I had to do 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 where I used public-key encryption for email.

Work Plan

The report will be composed throughout March and April. It will be written in Microsoft Word and exported in the PDF format. To obtain research for the report, I have been exploring online journal databases for relevant articles and papers. I also have a few cryptography books that I am finding myself referencing quite often. My observations have led me to believe there is a sufficient amount of information on cryptography to meet the ten-page minimum requirement. The additional cover letters, style sheet guide, presentation outline, and transmittal letter will each be composed in Microsoft Word as well. See page 11 for a timeline outlining the composition timeframes for these documents. I have personally noted that each document type has specific formatting and implementation. *Technical Communication*, by John Lannon and Laura Guark, has chapters dedicated to explaining the purpose, design, and conduct for all project materials. I will continually review important chapters in *Technical Communication,* as well as course materials from Blackboard, to ensure I am composing all documents correctly.

I have identified four topics which require examples, figures, and/or diagrams: Caesar Cipher, public-key cryptography, Diffie-Hellman key exchange protocol, and the RSA cryptosystem. The Caesar Cipher example already has been completed and is used in this proposal's problem statement. It may be reused in the report. Public-key cryptography's procedure is best shown via diagram. Luicdchart.com will be my resource for creating diagrams. For Diffie-Hellman Key Exchange and RSA, I will have to create my own working examples to outline in the report. I am not yet certain what visual aids I will include in these sections.

Microsoft PowerPoint will be used to make a slide deck for presentations. The presentation is required to be accompanied with an outline. I will complete the outline first and then build the presentation using information from the report. I will then time the presentation and adjust its length accordingly. If there is time, I may develop a live RSA demonstration.

Outline

I. Introduction

Public-key cryptography is a cryptosystem for parties who wish to establish secure communications without the need to have had previously communicated a secret key. Each party has a public key that can be openly distributed and a private key for their eyes only.

II. Cryptography Fundamentals

This section contains information relevant to a new explorer of cryptography. Someone who is familiar with cryptography would not need to go over these topics unless they want a refresher.

A. Definitions

i. Cryptography

"Cryptography is the science and art of designing and using methods of message concealment" (Barr, 2002, p. 2)

ii. Plaintext (Cleartext)

Plaintext is readable data.

iii. Ciphertext

Ciphertext is incomprehensible data after being run through encryption.

iv. Encryption

Encryption is a reversible mathematical function to convert plaintext into ciphertext where only authorized parties should be able to reverse the process.

v. Decryption

Decryption is the process of reversing ciphertext back to plaintext.

vi. Key

A key is the input into an encryption algorithm used to generate ciphertext.

vii. Cryptosystem

A cryptosystem is the combined system of key generation, encryption, and decryption.

viii. Confidentiality

Confidentiality is one of the prime tenants of information assurance. It states there should be no unauthorized access to data.

ix. Cipher

Mathematical formula or function applied to the data to transform the plaintext into ciphertext (Shelton, 2015).

B. Different Types of Ciphers

i. Substitution Cipher
Substitution ciphers replace letters of the alphabet to encode the plaintext.

ii. Monoalphabetic Cipher
A substitution cipher where the cipher alphabet is fixed through the entire encryption process.

iii. Polyalphabetic Cipher
A substitution cipher where the cipher alphabet is changed during the encryption process.

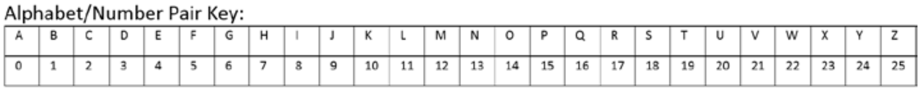
iv. Transposition Cipher
A transposition cipher rearranges plaintext to create ciphertext.

C. Caesar Cipher

i. History
Caesar Cipher was a monoalphabetic shift cipher used in 50 B.C. (Barr, 2002, p. 5).

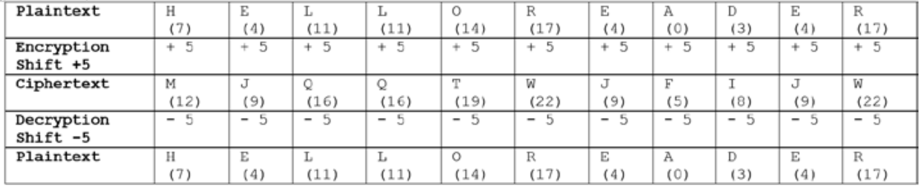
ii. Monoalphabetic Example

Alphabet/Number Pair Key:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher on HELLO READER with a shift of five:



Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)
Encryption Shift +5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5	+ 5
Ciphertext	M (12)	J (9)	Q (16)	Q (16)	T (19)	W (22)	J (9)	F (5)	I (8)	J (9)	W (22)
Decryption Shift -5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5	- 5
Plaintext	H (7)	E (4)	L (11)	L (11)	O (14)	R (17)	E (4)	A (0)	D (3)	E (4)	R (17)

iii. Polyalphabetic Example
Repeat the Caesar Cipher from above with a polyalphabetic shift.

III. Secret-Key Cryptography (Symmetric Cryptography)

A. History
"Secret-Key cryptography is the oldest form of encryption and has been used to safeguard communications for over three thousand years" (Shelton, 2015).

B. Definition

C. Pros

i. Fast on Large Data
Symmetric cryptography is designed to quickly encrypt and decrypt large amounts of data.

ii. Strong

The NSA's Advanced Encryption Standard is a Rijndael cipher with, at 128 bit key, has a complexity of $2^{126.1}$ (9.117640265872 × 10^37).

D. Cons

i. Must Have an Alternative Secure Channel to Transmit Keys
"All secret key algorithms or systems require that the party generating the key share or transfer it to the other party in a secure manner" (Shelton, 2015).

ii. Not Practical for Large Networks
Having a network of computers all communicating with each other using secret-key cryptography requires $n(n-1)/2$ keys (Odlyzko, 1994, p. 19). 20 million users all using encryption using symmetric cryptography would require 200 trillion total keys which is not practical (Odlyzko, 1994, p. 19).

IV. Public-Key Cryptography (Asymmetric Cryptography)

A. History

i. First Mention
In the 1960s, Government Communications Headquarters (GCHQ) cryptographer James H. Ellis wrote a classified journal on the need for non-secret encryption (Barr, 2002, p. 243).

ii. First Public-Key Cryptosystem
In the 1970s, Stanford Researchers Whit Diffie, Ralph Merkle, and Martin Hellman invented the first public-key cryptosystem entitled Diffie-Hellman key exchange (Odlyzko, 1994, p. 19).

iii. 1978, Ronald Rivest, Adi Shamir, and Leonard Adelman published their RSA public-key algorithm that is still in use today (Barr, 2002, p. 286).

B. Definition

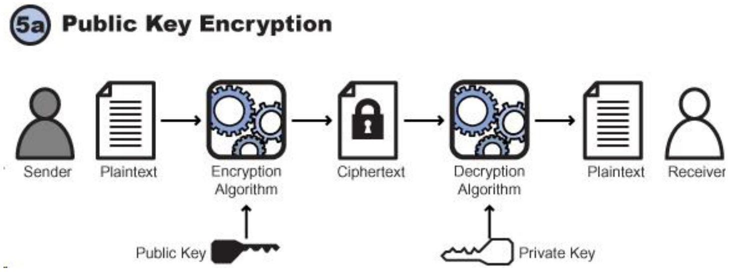
C. What Uses Public-Key Cryptography and Why Should I Care?

i. Applications
Encrypted e-mail, Internet browsing using HTTPS, e-commerce and mobile banking, authentication of smart phones and tablets, citizen passports, and mass transit ticketing (Moulds).

ii. Public-Key's Purpose
Without public-key cryptography there would be an impossible basis for secure communications on the Internet (Moulds).

D. How Public-Key Cryptography Works

i. Explanation (Shelton, 2015)



ii. Provides Authentication
Authentication is defined as obtaining the identification of the sender (Shelton, 2015).

iii. Sender Non-Repudiation
Non-repudiation is defined as the inability of a sender to refute that they signed something encrypted with their private key (Shelton, 2015).

iv. Key Exchange
For 3000 years we did not have a viable key exchange method (Shelton, 2015). Public-key cryptography has enabled the ability for mass key exchange throughout the Internet without the need to store the inexplicably large number of keys it would take for secret-key encryption to achieve this purpose.

v. Digital Signature
Digital Signatures reverse the key-exchange process and sign a message with your private key let others decrypt with your public key. This means it's guaranteed to have come from you and creates non-repudiation.

vi. Message Authentication
Hashing the message and attaching the hash to the message to provide integrity.

V. Public-Key Cryptography Examples

A. Diffie-Hellman

i. Methodology
The methodology for Diffie-Hellman requires the use of prime numbers and modulus (Odlyzko, 1994, p. 19).

B. RSA Cryptosystem Algorithm

i. The methodology for RSA requires the use of prime numbers and modulus, but is still secure today (Odlyzko, 1994, p. 19).

C. Key Exchange Example

        i. Diffie-Hellman key exchange example.

        ii. RSA key exchange example.

    D. Digital Signatures Example Using RSA

VI. Conclusion

Budget

Summary

The estimated budget for this project is $7153.63. Time costs are estimated to be approximately $6930 for 198 hours of work. Time costs were calculated using an hourly rate of $35 for 198 hours of work. Material costs are estimated to be approximately $223.63.   See the following page for full expense tables.

Time Costs

Overall, I estimate that I will be spending approximately 198 hours working on this project. I calculated that it took me ten hours to hit the mid-completion point of this proposal assignment. This led me to use ten hours as my baseline for activity time estimations. The two most expensive time costs are writing the main report ($2,625) and researching ($875). I believe it will take me almost 75 hours to write my main report based on my speeds working through the memo and this proposal.

Material Costs

Material expenses account for only three percent of the project's budget. The UNO library fee ($56.20) is the most expensive item in the table. Two other costly items are a Lucidchart.com subscription ($40) and an Adobe Creative Cloud subscription ($40). Lucidchart is needed to create diagrams. Adobe Creative Cloud contains Adobe Photoshop which will be useful for creating impressive visuals for my report. All the printing materials required for this project will cost approximately $53. Travel costs include gas and mileage which will cost approximately $31.

Time Costs ($35/hour)

Activity	Time (hours)	Cost
Writing Main Report	75	$2,625
Writing Cover Letters – A2 & A3	20	$700
Writing Proposal	20	$700
Writing Outline	5	$175
Writing Transmittal Letter	10	$350
Creating Style Sheet	5	$175
Creating Presentation	5	$175
Practicing Presentation	5	$175
Researching	25	$875
Final Revising	10	$350
In-class Lectures	16	$560
Peer Reviews	2	$70
Total:	**198 hours**	**$6930**

Material Costs

Item	Quantity	Cost
UNO Library Fee	1	$56.20
Gas – $2.50/gal Estimate – Premium Gas	10 Gallons	$25.00
Mileage – $0.575/mi – To and From Class	0.9mi x 12 trips	$6.21
Lucidchart.com – Subscription	2 Months	$40.00
Adobe Creative Cloud – Subscription	2 Months	$40.00
MavCard Printing – B/W Duplex	100 Sheets	$7.00
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
	Sub Total:	**$220.41**
	*Taxable Amt:	$46.00
	Sales Tax (7%):	**$3.22**
	Total:	**$223.63**

Grand Total

Table	Cost
Time Costs	$6930.00
Material Expenses	$223.63
Grand Total:	**$7153.63**

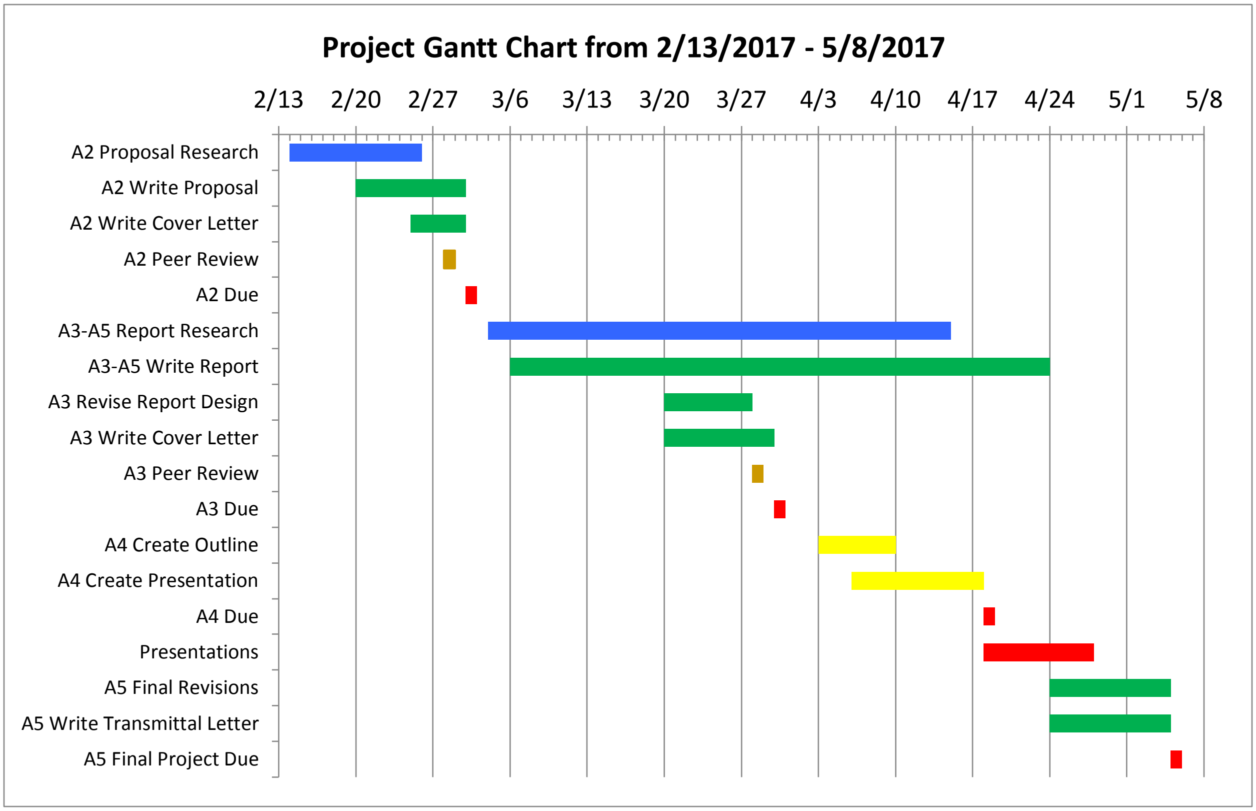
Timeline

To create the project timeline, I reviewed the class schedule and syllabus to obtain important milestones. Next, I took each milestone and reviewed the types of documents due (e.g. A3 submission requires a cover letter, a 50% draft of your report, and a style sheet). I added every required project task into the table and identified any additional tasks, such as research, that may need to be completed in tandem. Overall, the longest task is the continuous action of writing the report.

Task Name	**Start Date**	**End Date**	**Duration (days) or Time Due**
A2 Proposal Research	2/14/2017	2/26/2017	12
A2 Write Proposal	2/20/2017	3/2/2017	10
A2 Write Cover Letter	2/25/2017	3/2/2017	5
A2 Peer Review	2/28/2017		1:30 PM
A2 Due	3/2/2017		1:30 PM
A3-A5 Report Research	3/4/2017	4/15/2017	42
A3-A5 Write Report	3/6/2017	4/24/2017	49
A3 Create Style Sheet	3/20/2017	3/28/2017	8
A3 Write Cover Letter	3/20/2017	3/30/2017	10
A3 Peer Review	3/28/2017		1:30 PM
A3 Due	3/30/2017		1:30 PM
A4 Create Outline	4/3/2017	4/10/2017	7
A4 Create Presentation	4/6/2017	4/18/2017	12
A4 Due	4/18/2017		1:30 PM
In-Class Presentations	4/18/2017	4/28/2017	10
A5 Final Revisions	4/24/2017	5/5/2017	11
A5 Write Transmittal Letter	4/24/2017	5/5/2017	11
A5 Final Project Due	5/5/2017		11:59 PM

Key

🟦	Research
🟩	Writing
🟨	Presentations
🟧	Peer Review
🟥	Due Date



References

Barr, T. H. (2002). *Invitation to Cryptology*. Upper Saddle River, NJ: Prentice Hall.

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

Lannon, J. M., & Gurak, L. J. (2014). *Technical Communication* (13th ed.). Boston: Pearson.

Moulds, R. (n.d.). What is a PKI and why is it important? Retrieved February 26, 2017, from https://www.thales-esecurity.com/blogs/2013/march/what-is-a-pki

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

Shelton, B. K. (2015, November 11). Introduction to Cryptography. Retrieved February 26, 2017, from http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm