Cryptology: Cryptanalysis of Encryption Techniques

David Buickian
Glendale Community College

Introduction

Cryptography is the enciphering and deciphering of messages in secret code or cipher.[1] Cryptography can also be considered the process of taking a piece of information and applying a mathematical algorithm to it in order to make it unreadable or incomprehensible to anyone except those specific people who possess the specific knowledge to decipher that piece of information.

History of Cryptography

The Beginnings

Cryptography has been in use since the Egyptian hieroglyphics.[2] The Caesar Cipher and the Skytala/Scytale were two of the most innovating and intricate types of ciphers in its era. The Caesar Cipher consists of transposing an alphabet either to the forward (A-Z) or backwards (Z-A). Let 'n' be any integer, therefore the alphabet can either be transposed 'n' number of spaces forward or 'n' number of spaces backward. The key to this cipher is the 'n' number that the alphabet had been transposed in order to decipher the message. Figure 1 demonstrates an example of the Caesar Cipher.

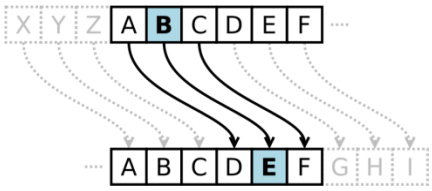

Figure 1: Caesar Cipher

The Skytala/Scytale is a mechanical cipher that utilizes a piece of thin paper consisting of only one row of letters and a rod that will be implemented to decipher the text. The useful aspect

---

[1] Merriam-Webster.com, s.v. "Cryptography," http://merriam-webster.com (accessed April 11, 2012)

[2] "History of Encryption" Sans.org. http://www.sans.org/reading_room/whitepapers/vpns/history-encryption_730 (accessed April 12, 2012).

of this cipher is the different versions and modulations that the cipher can implement such as various diameters of rods consisting of cylindrical, hexagonal and octahedral rods. Once the piece of paper has been spun around the rod the encode message would become clear and understandable.

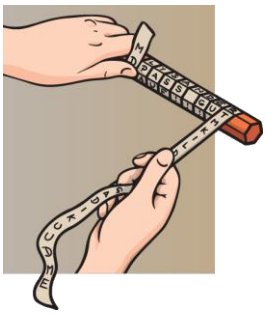

Figure 2: Skytala/Scytale

Growing Pains

This was the stage of when cryptography took a huge leap into the implementation of electronics and a new path into complex ciphers. The substitution cipher created corresponding numbers to every letter, symbol, and character. Therefore completely transforming the encode message. The transposition cipher establishes a multifaceted method of shifting columns and rows of not only words, letters, but numbers as well.

The Zimmermann Telegraph in 1917 brought attention to encryption on a global stage. The Zimmerman Telegraph was an encoded message from Germany to Mexico which the US government decoded and pushed the US into World War. Due to this event interest and attention grew about cryptography.

During World War II Nazi Germany utilized a mechanical cipher via the Enigma Machine.[3] The enigma machine implemented the substitution and transposition cipher simultaneously that encoded communications between military commanders and heads of state. However, the enigma machine had a security flaw in its system. The keys to the encoded messages needed to be physically written down, which created vulnerability. If the book of keys were to be found all of the encoded messages could be broken.

Modern

Three of the modern day encryption techniques that this paper will discuss are RSA, AES, and Blowfish. Modern encryption techniques were established during the 20th and 21st century. They implement complex mathematical functions in order to encode messages, with the accompaniment of keys. There are an abundance of modern encryption techniques; however, this

[3] "A Brief History of Cryptography" Cypher.com. http://www.cypher.com.au/crypto_history.htm (accessed April 12, 2012).

paper will critically analyze a commercial and widely used encryption, RSA, a standard in global encryption, AES, and an open-source encryption technique, Blowfish.

Basics: Relevance and Applications of Encryption Techniques

Communication via Internet

The Cyber community is continually growing.[4] Just as with any community, as it grows, unfortunately crime grows with it. Cyber security is an increasingly vital aspect in the digital world, not only maintaining, but protecting data. Since the internet was created in 1982 communication over the internet and devices that store data has increased. In 1991 only 1% of the world's information was being communicated via internet; by the year 1995 it was at 51% and by the time it was 2007 it was 97%. [5] With the use of the internet, online banking, online purchases and general communication is vulnerable until protecting by encryption. In fact the use of any type of electronic devices such as flash drives, iPods, external hard drives are all susceptible to unauthorized access without the correct precautions. Furthermore, due to the digitalization of all paperwork, such as e-books, to online banking, to paying bills online all personal information is vulnerable in the cyber community. If the vulnerability is not re-enforced identity theft occurs. Recently 1.5 million account numbers to credit card holders were hacked.[6] Even though credit card companies implement encryption software in order to protect their customer's personal information, hackers were still able to penetrate and retrieve information. Therefore, encryption is extremely vital when communicating digitally.

Financial Industry

The financial sector provides an example of an area were encryption and cryptography are heavily implemented and revered for protecting valuable data. An area where risk is an ever present danger is in the financial sector. Since 1987 Wall Street have been implementing algorithms that provide risk managements and predications of growth in the economy which traders use in buying and selling stocks. This type of trading is called high frequency trading. On October 19, 1987 a global financial flash crash spread from Hong Kong to Europe to Wall Street.[7] The Dow Jones Industrial average dropped 508 points approximately 22.6% at the time in only a few hours. Dow jones regained the entire loss the following day. This flash crash was due to faulty algorithms that produce incorrect predictions. The market crash was not due to a

---

[4] "Computer History Museum - Exhibits - Internet History" ComputerHistory.com. http://www.computerhistory.org/internet_history/ (accessed April 11, 2012).

[5] "Computer History Museum - Exhibits - Internet History" ComputerHistory.com. http://www.computerhistory.org/internet_history/ (accessed April 11, 2012).

[6] Bob Sullivan, "Global Payments: Under 1.5 million account numbers hacked" *MSNBC,* April 11, 2012, http://redtape.msnbc.msn.com/_news/2012/03/30/10940640-global-payments-under-15-million-account-numbers-hacked?lite

[7] Quants: The Alchemists of Wall Street, YoutTube video, 47:49 posted by VPROInternational March 4, 2012, http://www.youtube.com/watch?v=ed2FWNWwE3I

security breech or unauthorized access, but just a glitch in the system. This event occurred again but with much more severity recently on May 6, 2010. The Dow Jones Industrial Average dropped 1000 points at 2:45 pm EST and regained that loss at 3:00pm EST. Again this was not the result of unauthorized access, but a glitch in the system. The financial industry needs encryption in order to protect the daily transactions of stocks, bonds, and commodities that are being traded. The algorithms which produce predictions through the use of mathematical models also demand encryption software to maintain and protect the information being inputted and outputted. Without the use of encryption a security breech resulting from hackers can not only devastate the economy in a matter of seconds, but can paralyzed the financial sector for years to come. The severity and magnitude of encryption is thoroughly understood and implemented in the financial industry due to these events.

Features of Encryption Techniques

Rivest Shamir Adleman (RSA)

RSA was created in 1977 by three MIT students by the name of Ron Rivest, Adi Shamir, and Len Adleman. RSA is a public key system which implements public keys in order to utilizes the algorithm.[8] RSA is an asymmetric cipher meaning it employs two keys to encode and decode. RSA is a block cipher, meaning that the plaintext is divided into 64 bit-blocks which are then encoded. [9] The crux of RSA is the invertible mathematical function or trap door cipher.

RSA incorporated two complex mathematical functions as its crux encryption mechanism. The first being Number Theory: Prime factorization (trap door cipher),[10] second Fermat's Little Theorem.[11] A basic explanation of how RSA works is as follows.

Alice creates a message or plaintext then uses American Standard Code for Information Interchange (ASCII) to transform the letters symbols, and characters, in her plaintext to numbers. Once the numbers are achieved then the mathematical functions or algorithm can be implemented while utilizing Alice's private key and Bob's public key. Once the encoding is finished the results is the cipher text.

---

[8] Stallings, William. Cryptography and Network Security: Principles and Practice. Second ed. Upper Saddle River, NJ: Prentice Hall, 1999. Print.

[9] "RSA Encryption." -- from Wolfram MathWorld. Wolfram Alpha LLC. (accessed April 12, 2012)

[10] "Number Theory." -- from Wolfram MathWorld. Wolfram Alpha LLC. (accessed April 12, 2012)

[11] "Fermat's Little Theorem." -- from Wolfram MathWorld. Wolfram|Alpha. (accessed April 12, 2012)

The cipher text is sent to Bob which he uses the identical algorithm, however, utilizing Bob's private key and Alice's public key in order to decrypt the file. Once again returning the original message or plain text. Figure 3 displays a diagram of asymmetric encryption.

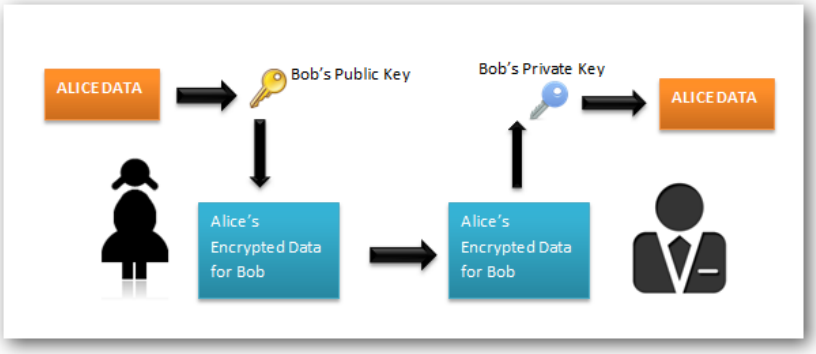

Figure 3: Asymmetric Encryption

RSA is used on a variety of different platforms; ranging from Virtual Private Networks (VPN to Secure Shell Host (SSH) to web browsers.[12] Not only is RSA used commercially, but the US Government and Military have implemented it on their networks.

Most common place where RSA is utilized is digital signatures. When people sign into any type of account, such as email, Facebook, online banking, RSA is implemented to insure that transaction is encrypted. [13]

The key size must be large enough to make brute-force attack impartial but small enough for practical encryption and decryption.

In practice, the key sizes that have been proposed do make brute-force impartial but result in encryption/decryption speeds that are too slow for general use.[14]

The National Institute of Standards and technologies have approved RSA and certified it as a recommended form of encryption.

Advanced Encryption Standard (AES)

AES was the result of a NIST competition in 1997.[15] The precursor to AES was DES the Digital Encryption Standard. NIST officially approved AES on November 26, 2001. The two lead cryptologists Joan Daemen and Vincent Rijmen.

---

[12] Cronkhite, Cathy, and Jack McCullough. Access Denied: The Complete Guide to Protecting Your Business Online. New York: Osborne/McGraw-Hill, 2001. Print.

[13] Davis, Tom. "RSA." Berkeley Math Circle. 17 Dec. 2000. (accessed April 12, 2012)

[14] "3.1.5 How Large a Key Should Be Used in the RSA Cryptosystem?" RSA Laboratories -. EMC Corp. (accessed April 12, 2012)

AES is a symmetric encryption, which encrypts in blocks.[16] A symmetric encryption is an encryption that uses only one private key to encrypt and decrypt data. Figure 4 displays how symmetric encryption works

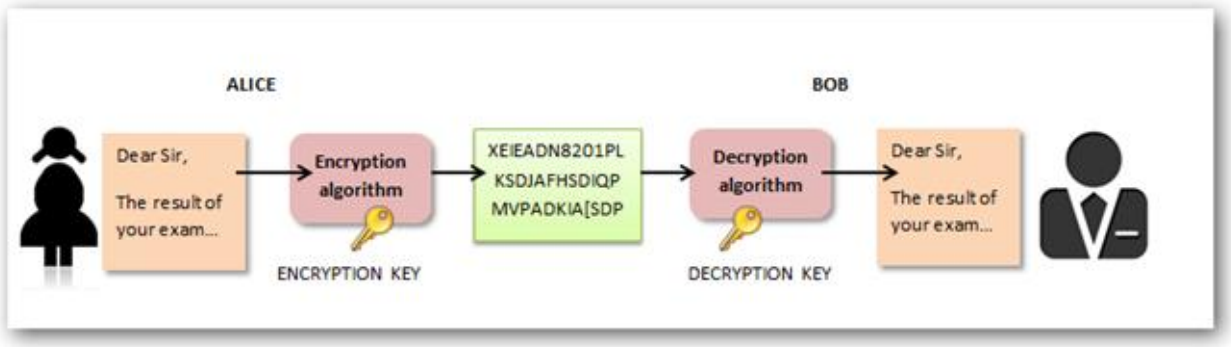

Figure 4: Symmetric Encryption

Alice creates a message or plaintext uses the private key to encrypt the data sends the cipher text to Bob. Bob uses the identical private key and algorithm to decrypt the message.

AES is industry standard by the National Institute of Standards and Technology. [17]Therefore AES has been subject to a variety of brutal tests such as speed of encryption/decryption, key strength, performance on different CPU's.[18] AES will work in a variety of current and future applications. AES works on: 32-bit microprocessors, 64-bit microprocessors, small 8-bit smart cards, DSPs, FPGAs, and custom ASICs.[19] Since is the standard of encryption NIST has certified that this encryption technique will suffice until the year 2030.

AES allows for variable key length, which allows for tradeoff between speed and security. [20]The longer the key the more secure the encryption will be, but slower to encrypt and decrypt. AES comes in three different key lengths; 128 bit key 16 bytes in length, 192 bit key 24 bytes in length, and 256 bit key 32 bytes in length.

---

[15] Shelton, Barry K., and Chris R. Johnson. "A Brief History of Encryption." Technology News: Encryption:. ECT News Network, Inc., 19 July 2010. Web. 12 Apr. 2012.
[16] "AES: Keeping Your Data Secure with Advance Encryption Standard." Object Moved. Web. 16 Apr. 2012.
[17] "C S R C - Cryptographic Toolkit." *NIST.gov*. Web. 12 Apr. 2012.
[18] Stallings, William. Cryptography and Network Security: Principles and Practice. Second ed. Upper Saddle River, NJ: Prentice Hall, 1999. Print.
[19] "Digital Signatures." NIST.gov. Web. 16 Apr. 2012.
[20] "C S R C - Cryptographic Toolkit." *NIST.gov*. Web. 12 Apr. 2012.

As of present the US government use 128 bit AES for the encryption unclassified documents and a 256 bit AES for classified documents.[21]

Blowfish

Blowfish is a symmetric encryption designed by Bruce Schneier in 1993. Bruce Schneier uploaded the encryption software to the internet making it open source and royalty free. [22]Blowfish is a 64 bit block cipher with varying key lengths beginning from 32 bits to 448 bits in length. [23]Blowfish is faster than the predecessor of AES, which is DES.

Symmetrical method uses a single key for encrypting and decrypting data. These keys are widely used for storing and protecting confidential information, since the keys are not very long and large amount of data can be encrypted very quickly.[24]

Feistel proposed that we can approximate the simple substitution cipher by utilizing the concept of a product cipher, which is performing of two or more basic ciphers in sequence in such a way that the final result or produce is cryptographically stronger than any of the component ciphers. Cipher that alternates substitutions and permutations.

Blowfish is an alternative to commercial mainstream encryption techniques such as RSA and AES.[25] Anyone who as an internet connection has the ability to utilize this encryption Easy to use convenient and compatible to both Apple and PC products. Blowfish is one of the fastest block ciphers. It only runs on 5K of memory.[26] Variable key length allows for a tradeoff between higher speed and higher security.

Blowfish has been in existence for nineteen years and has been open source for those nineteen years which gave the opportunity for programmers across the world to create applications and free software implementing Blowfish as its encryption technique.[27] Blowfish is used on Windows, Apple, Palm OS Linux based computers, email, online chat and Encryption

---

[21] Cronkhite, Cathy, and Jack McCullough. Access Denied: The Complete Guide to Protecting Your Business Online. New York: Osborne/McGraw-Hill, 2001. Print.

[22] "Cryptography Blow Fish Information Technology Seminar." *Final Year Projects, B Tech Projects, BE Projects, MCA Projects, MBA Projects, Mtech Projects*. Web. 12 Apr. 2012

[23] "The Blowfish Encryption Algorithm." Blowfish. Web. 19 Apr. 2012.

[24] "File Encryption Software - Cryptography - The Best Encryption Algorithms - Lost Password?" Password Manager XP. Web. 16 Apr. 2012.

[25] Gonzalez, Tom. *A Reflection Attack on Blowfish*. Columbia State University, 1 Jan. 2007. Web. 12 Apr. 2012.

[26] Cronkhite, Cathy, and Jack McCullough. Access Denied: The Complete Guide to Protecting Your Business Online. New York: Osborne/McGraw-Hill, 2001. Print.

[27] Stallings, William. Cryptography and Network Security: Principles and Practice. Second ed. Upper Saddle River, NJ: Prentice Hall, 1999. Print.

toolkits just to name a few.[28] Blowfish is one of the most extensive and widely used encryption techniques in the world.

Crux: Criteria on an Ideal Encryption

Assessing Encryption Needs

Everyone has special encryption needs. Certain people require high security where speed is not an issue, such as classified documents. Companies and governments would utilize this section of the encryption spectrum. RSA and AES are ideal encryption techniques specifically for this sector.

Certain people require fast encryption and decryption speeds, such as high frequency trading in the financial industry. The financial sector would utilize this section of the encryption spectrum. AES and Blowfish are ideal encryption techniques for this sector.

Certain people need comfort and convenience in their encryptions needs. The average person or small business owner would utilize this section of the financial spectrum. Blowfish is superior in this sector of encryption techniques.

Conclusion

Evaluation

Blowfish

Blowfish is far more suitable for the everyday person. It is easily accessed through the internet. Blowfish is easy to use, user friendly allowing the average person to be able to use it. It is free and downloadable from the internet. Since its publication it has been use on multiple platforms. Furthermore blowfish has a successor called Two Fish which is also open source and royalty free.

AES

AES is recommended by NIST implementing a symmetric cipher which enables for faster speeds of encryption and decryption. However, it is not free and must be bought. AES is far more complex thatn Blowfish allowing only certain people to be able to use it.

RSA

RSA is the top grossing encryption technique since 1977. It is very secure but has much slower speed of encryption and decryption due to its use of two keys. RSA is not open source and must be bought. Furthermore, RSA is a very complex cipher making it difficult for people to use on a daily basis.

---

[28] "The Blowfish Encryption Algorithm." *Blowfish*. N.p., n.d. Web. 14 June 2012.

Overview

Blowfish is the best catch between these three encryption ciphers. It displays the qualities of a high security and easy to use capabilities. The fact that Blowfish is free allows a much larger pool of consumers to be able to download and use Blowfish.

Nevertheless, these three encryption techniques are only a few in the vast empire of cryptography. There are constantly newer versions and innovations in the cryptographic community. Therefore encryptions techniques are always being updated, fixed, and re-enforced to be able to withstand hacking and new trends of digital vulnerabilities.