Yaroslav Kechkin

Literature Review

Gulf Coast State College

MAN 4900

Wendy Payne, Guy Garrett

February 15, 2012

**Introduction**

In digital world of today people are concerned with their information stored on computers at home or work, information that they use on the Internet is secured and no one else can steal and use their information. The principles of CIA (Confidentiality, Integrity, and Availability) triad are used to give necessary protection to the information. Basic means of keeping the information secure in the digital world is through use of cryptography. “Encryption or cryptography is the art of converting message or data into a different form, such that no one can read the original code without possessing a key” (Clark, 1998).

Cryptography is concerned with protecting communications from being read by the wrong people. Codes and ciphers that are used to protect communications are called cryptographic systems. The application of codes and ciphers to messages to make them unreadable is called encryption. Encryption is a way of hiding secrets by applying mathematical functions to plain text to produce text that is difficult to decrypt. The basic unit used in encryption is a word of phrase that is used to produce encrypted message and to decrypt the message into a plaintext. There are two categories of encryption: Transposition – where the characters in a plaintext are rearranged to create ciphertext, and Substitution – where the characters of plaintext are replaced with other characters (mono and polyalphabetic substitutions).

In everyday, cryptography is used to protect the confidentiality and integrity of the information that is being transmitted over the Internet, radio, and phone (mostly Internet these days). Cryptography is used to prevent intruders (hackers) to understand the information that they can acquire through different means.  Cryptography can also be used to protect information’s integrity and authenticity of data. Checksums, as an example, are often used to verify the integrity of a block of information or a file. It can be used to determine if the information was altered or modified. Cryptographic checksums help prevent undetected modification of information by encrypting the checksum in a way that makes the checksum unique (MD5 and SHA-1 algorithms). The authenticity of data can also be protected by cryptography. Digital signatures can be used to protect confidentiality of the message and prove the authenticity of the sender. Digital signatures are combination of the checksum of the information and author’s private key and can be deciphered using receiver’s key.

**Literature Review**

The cryptography, as a science can be divided on two major parts: before use of mathematics and after. Julius Caesar was first to use the substitution by addition method. “Messages were encoded by substituting the letter in the text by one that is three positions to the right. A became D, V became Y etc.” (Cypher Research Laboratories, n.d.). This is called a Caesar shift and is monoalphabetic cypher. Such cyphers are easy to break by analyzing the pattern. To make decryption of a secret message harder multiple alphabets were introduced. As stated on the Cypher Research Laboratories web site, there were tries to create a polyalphabetic cyphers. Many tried, but “the best known being the French cryptographer Blaise De Vigenere to devise a practical poly alphabetic system which bears his name, the Vigenere Square. At the time, and for a considerable time afterwards this technique was believed to be unbreakable” (Cypher Research Laboratories, n.d.). Vigenere square uses 26 by 26 matrix composed of letters of alphabet. In the paper by the professor Kallam, he gave an example of 256 by 256 matrix composed of ASCII and Extended ASCII characters. He also stated that “if we can perform 1decryption per micro second it takes approximately 253\*10^19 years for trying all possible keys” hence ruling out the brute force attack (Kallam, Kumar, Vinaya, & Kumar, 2011). Use of polyalphabetic ciphers is easy and will take a very long time to break that is why such encryption techniques are still used today.

The risky part of using such cipher is the transmission of the key to decipher the message, because key can be intercepted and used by intruders to decipher the text. That is why the method of encrypting the keys was invented. It is called the Book cipher or Running key and used “widely available texts from regular books as the source of the key sequences” (telus.net, n.d.). It simplified the distribution of the key, but it was still vulnerable since the pattern could be found and used to decipher the key and then the message.

There are two different kind of cryptography: symmetric key and public key cryptography (asymmetric). Symmetric or “secret-key” cryptography uses a single key to encrypt and decrypt message. The best known block cipher algorithm is DES, which has 64-bit long block size and uses a 56-bit key during execution (Stallings, 2011, p. 67). However, most recently, it has been shown that DES cracking machine can break the algorithm and recover the key in 22 hours. The National Institute for Standards and Technology (NIST) has made competition for replacement of DES, for the best Advanced Encryption Standard (AES) and algorithm discovered by Rijndael that uses a 128-bit block size and a key size of 128, 192, 256 bits has been accepted as a replacement (Stallings, 2011, p. 67). Most likely it will be the worldwide successor of DES, as it provides enough security, and it is very likely that it will stay secure for a very long time (Menezes et al, 2001). The main problem of symmetric key cryptography is that sender and receiver need to agree about the common secret key, and that key needs to be securely stored and transmitted from sender to receiver. “This was extreme problem in communication, as there was always a fear that somebody can unnoticeably intercepts the conversation and finds out about the key” (Menezes et al, 2001).

To provide increased level of security, the Public Key Infrastructure (PKI) was introduced as a new security concept. “Public Key Infrastructure (PKI) is, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each entity involved in an online transaction. PKI allows the secure exchange of encrypted electronic data between parties over the internet. So, it can be used for email communication, web browsing, online banking, or lodging tax returns” (VeriSign, 2001). Public key cryptography uses a public/private pair of keys. The public key is publicly available while the private key is kept secret. Thus, the message is encrypted with the public key and it is almost impossible to be decrypted without the knowledge of the private key. The main disadvantage of Public Key cryptography over symmetric key cryptography is that much larger keys need to be used to provide the same level of security. “This was one of the main reasons why symmetric keys are most often used for encryption of important data, and PK keys are only used to provide safe transmission of symmetric keys and for creation of digital signatures in Public Key Infrastructure” (NOIE, 1997).

In PKI, a public and private key are created simultaneously using the same algorithm (RSA is the most popular one to use) by a certificate authority (CA). “Public keys are stored within digital certificates along with other relevant information (user information, expiration date, usage, who issued the certificate etc.). The CA enters the information contained within the certificate when it is issued and this information cannot be changed” (Articsoft.com, 2012). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else.

“You can design a PKI solution to meet the following security and technical requirements of your organization:

**Confidentiality.** You use a PKI to encrypt data that is stored or transmitted.

**Integrity.** You use a PKI to digitally sign data. A digital signature helps you identify whether another user or process modified the data.

**Authenticity.**A PKI provides several authenticity mechanisms. Authentication data passes through hash algorithms, such as Shivest Hash Algorithm 1 (SHA1), to produce a message digest. The message digest is then digitally signed by using the sender’s private key to prove that the message digest was produced by the sender.

**Nonrepudiation.** When data is digitally signed, the digital signature provides proof of the integrity of the signed data and proof of the origin of the data. A third party can verify the integrity and origin of the data at any time. This verification cannot be refuted by the owner of the certificate that digitally signed the data” (Microsoft, 2003)

The last survey that has been undertaken by OASIS PKI group shows the major PKI’s obstacles are:

· Software application does not support enough PKI,

· PKI is too expensive,

· PKI is not understood enough.

This survey has been undertaken in more than thirty countries including Australia. Almost half of the respondents are coming from IT, and more than 75% of them had five or more years of experience in Information Security (Doyle and Hanna, 2003).

In the perfect world, the PKI would be able to have the suitable software and hardware that would be able to provide perfectly secure key pair to the users, and to provide perfectly secure place where users can publish their public keys and store their private keys. However, we do not live in a perfect world. The first most important problem with the PKI structure offered by the Gatekeeper project is that it uses old vulnerable cryptographic algorithms like DES that had been broken and replaced by the newer AES (Whittle, 1998). Governments strongly suggest that only authentication keys use strong encryption, as in that case an authentication process can never be used for criminal purposes (Walsh, 1996).

**Conclusion**

The concept of public-key cryptography was invented by Whitfield Diffie and Martin Hellman, and independently by Ralph Merkle. Diffie and Hellman first presented this concept at the 1976 National Computer Conference (Diffe, Hellman, 1976). Since 1976, numerous public-key cryptography algorithms have been proposed. Many of these are insecure. Of those still considered secure, many are impractical. Either they have too large a key or the ciphertext is much larger than the plaintext. “Only a few algorithms are both secure and practical. Of these secure and practical public-key algorithms, some are only suitable for key distribution. Others are suitable for encryption (and by extension for key distribution). Still others are only useful for digital signatures. Only three algorithms work well for both encryption and digital signatures: RSA, ElGamal, and Rabin” (Schneier, n.d.). Invention of PKI “led to important applications we often hear of today. Digital signatures, PGP (pretty good privacy), use of public certificates, various authentication protocols are all in the domain of public key cryptography” (LogicalSecurity.com, n.d.). The symmetric and asymmetric algorithms are undergoing some improvements to withstand constant attempts to gain access to keys to be able to decipher text. RSA 512 and RSA 1024 are most secure. algorithms as of today. They use tremendously big keys for encryption which makes them very slow in encryption and decryption but they are secure to use.

**References**

Articsoft.com (2012). An Introduction to PKI. Retrieved from <http://www.articsoft.com/public_key_infrastructure.htm>

Clark R (1998). Message Transmission Security. Retrieved from <http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html>

Cypher Research Laboratories (n.d.). A Brief History of Cryptography. Retrieved from <http://www.cypher.com.au/crypto_history.htm>

Diffie W., & Hellman, M. E. (1976). "Multiuser Cryptographic Techniques," *Proceedings of AFIPS National Computer Conference*, pp. 109-112.

Diffie W., & Hellman, M. E. (November, 1976). "New Directions in Cryptography," *IEEE Transactions on Information Theory,* 22(6), 644-654.

Doyle, P., & Hanna S. (2003). Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage. Retrieved from <http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf>.

Kallam, R. B., Kumar, S. U., Vinaya, A., & Kumar, V. S. (2011). A Contemporary Polyalphabetic Cipher using Comprehensive Vigenere Table. *World of Computer Science and Information Technology Journal (WCSIT),* 1(4), 167-171.

LogicalSecurity.com (n.d.). History of Cryptography. Retrieved from <http://www.logicalsecurity.com/resources/whitepapers/Cryptography.pdf>

Menezes, A., Oorschot, P., Vanstone, S. (2001). Handbook of Applied Cryptography, 5th ed. CRC Press.

Microsoft (March 28, 2003). PKI Technologies. Retrieved from <http://technet.microsoft.com/en-us/library/cc779826(v=ws.10).aspx>

NOIE (National Office for the Information Economy) (1997). GATEKEEPER: A Strategy for Public Key Technology Use in the Government. Australian Government: Office of Government Information Technology.

Schneider, B. (November, 1995). Applied Cryptography, 2nd ed. Wiley, John & Sons, Inc.

Stallings, W. (2011). Cryptography and Network Security, 5th ed. Upper Saddle River, New Jersey: Pearson Education, Inc.

Telus.net (n.d.). Polyalphabetic Substitution Ciphers. Retrieved from <http://www3.telus.net/Voiculescu/vigenere/index.html>

VeriSign (2001). Administrator’s Handbook. Retrieved from <http://www.verisign.com.au/managedpki/documents/admin/AdminHandbk.pdf>

Walsh, G. (1996). The Walsh Report. Retrieved from <http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm>.

Whittle, R. (1998). Rough critique of the 6 May Project Gatekeeper report. Office of Government Information Technology.