THE ROLE OF CRYPTOGRAPHY IN INFORMATION AND DATA SECURITY

FATIMA MAIKUDI ABUBAKAR& SHITU ABDULLAHI LAME
Department of Library and Information Science, School Of Education, A.D. Rufa'i College for Legal and Islamic Studies Misau, Bauchi State, Nigeria

ABSRACT
The widespread of internet and electronic communication has led us to focus our attention on how this data can be transmitted securely over the network without been tampered with. This issue of security can be handled using cryptographic systems. This paper intends to give a highlight on what cryptography is, how it works and the role it plays in information security. Securing data across the network prevents eavesdropping and vulnerabilities.

INTRODUCTION
Securing data or information sent over the network is very important to the Internet and electronic communication in the world today. Information in any organization is an important asset that needs to be secured.Security nowadays is of major concern to the growth of the network which provides more services. Providing these services to the user in a secure way is very paramount. Attackers can easily gain information during its transmission across the network and then gain unauthorized access to the servers, to whom they are not able to access. Large volumes of personal and confidential information are electronically transmitted and stored every day on the net. The protection of systems and networks result in data availability, integrity and confidentiality. The role of cryptography as a means of security in the information era has led us to understanding of what cryptography is all about.

There is the need to have an assurance that information or message sent to one person is not intercepted and read by another person without the prior knowledge of the sender. Tools to ensure the privacy and confidentiality of data communication have existed for a long time. Similar tools exist in the electronic communication field. Cryptography is one of the key elements in providing security for modern e-commerce systems. J.Hu et al (2010) argued that software-based encryption has built-in security weaknesses due to storing and managing digital certificates/keys in a high risk environment such as a local hard disk or software. Cryptography allows people to carry over the confidence found in the physical world to the electronic world. It allows people to do business electronically without worries of deceit and deception. In the distant past, cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to ensure integrity of the message and authenticity of the sender. And as we have also seen, no infrastructure security controls are 100% effective. Therefore encryption is used for securing data and information in the world of computing today.

COMPUTER SECURITY
William S. (2011) shows that computer, security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity,

availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

DATA SECURITY

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure and modification. Techopedia encyclopedia defines data security as a protective digital measure that is applied to prevent corruption and unauthorized access to computers, databases, and websites. Examples of data security technology include software and hardware disc encryption, backups, data masking and data erasure.

CRYPTOGRAPHY

Meaning of cryptography

According to Sutton, et al (2009), cryptography is the art and science of preparing coded or protected communications intended to be intelligible only to the person possessing a key. Tom olzak (2012), of Inforsec institute also defined, cryptography as a science that applies complex mathematics and logic to design strong encryption methods. Cryptography (Greek *kryptos,* "secret"; *graphos,* "writing") refers both to the process or skill of communicating in or deciphering secret writings (codes, or ciphers) and to the use of codes to convert computerized data so that only the recipient will be able to read it using a key. The original message is known as the **plaintext**, while the coded message is called the **ciphertext**. The process of converting plaintext to ciphertext is known as **enciphering** or **encryption** and restoring the plaintext from the ciphertext is **deciphering** or **decryption**. The enciphering process usually involves an algorithm and a key. An encryption algorithm is a particular method of scrambling a computer program or a written set of instructions. The key specifies the actual scrambling process.

Encryption is the conversion of plaintext or data into unintelligible form by means of a reversible translation, based on a translation table or algorithm (William S. 2011). It is also called enciphering. Parker, Donn B. (2009) defines encryption as the process of converting messages or data into a form that cannot be read without decrypting or deciphering it. The root of the word encryption—*crypt*—comes from the Greek word *kryptos*, meaning "hidden" or "secret". Any message that needs to be sent to another recipient must be encrypted (cipher) first before sending the message and only the recipient can decrypt (decipher) the message with a key that is only known to him/her. Hackers or eavesdroppers can only see the encrypted message with can only be read by possessing the key.

TYPES OF CRYPTOGRAPHY

There are two main types of cryptography:

SYMMETRIC KEY CRYPTOGRAPHY

Symmetric key cryptography also referred to as conventional encryption or secret key encryption was the only type of encryption in use prior to the development of public key encryption in the 1970s. According to William (2011), it is by far the most widely used of the two types of encryption systems. With this type of cryptography, the key is known only to the sender and the recipient. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

This method works well for communication within a limited number of people but it becomes impractical to exchange secret keys with large numbers of people. In addition, with secret key encryption the problem of communicating the key is a major problem since if the key falls into the hands of an intruder the information is no longer secured. An example of symmetric encryption is Data Encryption System (DES).

ASYMMETRIC KEY ENCRYPTION

This is also called a Public key cryptography. Two related keys are used, that is a public key and a private key. They are both used to perform complementary operations, such as encryption and decryption or signature generation and signature verification. According to William S. (2011) public key encryption was developed to address two key issues:

1. **Key distribution** – how to have secure communications without having the problem of distributing the key to a Key Distribution Center.
2. **Digital signatures** – how to verify that a message comes intact from the claimed sender

In the two-key system, one key encrypts the information and another, mathematically related key decrypts it. The computer sending an encrypted message uses a chosen private key that is never shared and so is known only to the sender. All computers authorized to receive and decrypt the message are given the matching public key. The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key. The following example illustrates how public key cryptography works:

- Bob wants to communicate secretly with Alice. Bob encrypts his message using Alice's public key (which Alice made available to everyone) and Bob sends the scrambled message to Alice.
- When Alice receives the message, she uses her private key to unscramble the message so that she can read it.
- When Alice sends a reply to Bob, she scrambles the message using Bob's public key.
- When Bob receives Alice's reply, he uses his private key to unscramble his message.

The major advantage of asymmetric encryption is that single key is not shared between the sender and receiver. Provided the private key is kept secret, confidential communication is possible using the public key. Examples of public key are encryption algorithms are RSA (Rivest, Shamir, Adleman), Elliptic curve, Diffie-Helman, and others.

BENEFITS OF PUBLIC KEY CRYPTOGRAHY

Digital signature

Public key cryptography provides a method for employing digital signatures. Digital signatures enable the receiver of information to verify the authenticity of the information's origin, and also verify that the information is not been tampered with. Thus, public key digital signatures provide authenticationand integrity of data. A digital signature also provides non-repudiation, which prevents the sender from claiming that he or she did not actually send the information. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is higher than a handwritten signature hence impossible to counterfeit.

DIGITAL CERTIFICATES

A digital signature is an authentication method that enables the sender of a message to attach a code that acts as a signature (William, 2011). Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message. It is simplify the task of establishing whether a public key truly belongs to the purported owner.

A certificate is a form of credential. Examples might be your driver's license, your social security card, or your birth certificate. Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them, lest someone use them to impersonate you.

A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid. Digital certificates are used to prevent attempts to substitute one person's key for another. A digital certificate consists of three things:

- A public key.
- Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
- One or more digital signatures.

IMPORTANCE OF USING CRYPTOSYSTEMS

Cryptographic techniques have long been in use to address the problems o f confidentiality, data integrity, and non-repudiation (J. Hu 2010). Cryptography is important because it enables all processes, transactions and communications to be safely performed electronically. It is especially important in communicating personal information that is vulnerable to distortion. Encryption is used for several operational technical reasons. It was shown by Cresson, W.C (1981) that the major role of encryption is concealment of data to achieve confidentiality, secrecy, or privacy.

Cryptography plays an important role in assuring the integrity of transactions in a society where the rights and obligations of persons are handled by information and communications systems. The piracy of information, and the consequential loss of the rights to this information, has been of great public concern, especially in the areas of proprietary software and commercial movies distributed for use on home videotape recorders. Also of concern are recently marketed products that allow nonpaying viewers to decrypt the signals of satellite- relay television signals.

However, cryptography is essential in everyday life. Online shopping also uses encryption to keep your credit card detail safe. Operating system software that automatically updates over the internet uses a public key algorithm to check that the update to be installed was really published by the right people, and not by someone trying to get into your computer.

Without cryptography use of ATM cash machines would not be possible, as the machines would not be able to reliably communicate with the bank computers. Without cryptography, even the idea of electronic voting would not be possible.

APPLICATIONS OF CRYPTOGRAPHY

Thawte crypto challenge (undated) pointed out that the main applications of cryptography were in the military during and before World War II in which encrypted messages were sent to opponents prior to attack. The cryptosystem is most commonly used for providing privacy and ensuring authenticity of digital data. It is used by web servers and browsers to secure web traffic,

it is also used to ensure privacy and authenticity of Email, remote login sessions, and in electronic credit-card payment systems.

The use of cryptography rose with the invention of more powerful computers and network after the world war in the field of banking transaction and password creation.

Goyal S, (2012) outlined some of the areas were cryptography is also applied. These include:

1. Secure Message Transmission of data over the network
2. Monitoring Communication
3. Fractional Observing of Data
4. Transferring Files on Network
5. Certificates and Authentication
6. Technique Use of Secure Socket Layer Protocol
7. Digital Signature and Authentication
8. Quantum Key Distribution

RECOMMENDATION

When people started doing business online and needed to transfer funds electronically, the applications of cryptography for integrity began to surpass its use for secrecy. Hundreds of thousands of people interact electronically every day, whether it is through e-mail, e-commerce (business conducted over the Internet), ATM machines, or cellular phones. The constant increase of information transmitted electronically has lead to an increased reliance on cryptography and authentication.

Since information and data security is of paramount importance to development and success of internet and electronic communication, it is best known to apply cryptographic algorithms as a protection against eavesdropping and hackers. Some recommendations are as follows;

1. Encryption is highly recommended in Electronic Funds Transfer Systems to overcome the problem of password hijackers.
2. The encryption system should also be applied in the Electronic Mail Systems since it is the major method of communication in the world today.
3. Likewise, the rising popularity of cable and telephone-related services, indicates a future need for better and additional applications of encryption. Timesharing service bureaus as well as data base information provider all require encryption systems.
4. In the field of medical sciences, it is strongly recommended for health advocates and medical practitioners to work towards the implementation of electronic medical records (EMR) privacy by creating awareness about patients rights related to the release of data to laboratories, physicians, hospitals, and other medical facilities.

SUMMARY AND CONCLUSION

In the age of rapid growth of digital data storage and communication, cryptography plays an integral role in our society. It is a challenge to respect the serious concerns of information and data security in the internet and electronic communication. In this article security issues involving data and information has been highlighted and what cryptography is, how it work and some of its application have also been shown in terms of securing information. As mentioned earlier, cryptography can provide authentication and Validation of data. Cryptography remains a fascinating topic of discussion.

Cryptography is expected to play an important role in assuring the integrity of transactions in a society where the rights and obligations of persons are handled by information and communications systems.

REFERENCES

Bradley Mitchell intro.To client and server network.Compnetworking.abour.com/od/basicnetworkingfaqs/a/client-server.html 2014)

Cresson W. C (1981). *Future Applications of Cryptography*. Retrieved on 23 March , 2014 from http//www.cs.washington.edu/research/projects/0004469/pd.

Goyal S. (2012). *A survey on the applications of cryptography.* International journal of Science and Technology Volume 1 No 3 March 2012.

J.Hu, X.D, Hoang & I. Khalil, (2010). *An embedded DSP hardware encryption module for secure commerce transaction.* Security and communication network. *Retrieved Dec 22 2013 from http//www.interscience.wiley.com.*

Olzak inforsec institute retrieved February 2014 from http//resources.infosecinstitute.com/role-of-cryptography

Parker, Donn B. *"Encryption."* Microsoft® Encarta® 2009 [DVD]. Redmond, WA: Microsoft Corporation, 2008.

Sutton, William G., and Rubin, Aviel D. *"Cryptography."* Microsoft® Encarta® 2009 [DVD]. Redmond, WA: Microsof t Corporation, 2008.

Techopedia dictionary Retrieved may 2014 from http//www.techopedia.com/definition/26464/data/security.

Thawte Cryptochallenge importance of cryptography Retrieved Jan 2014 from http//www.cryptochallenge.com

Trappe, W., & Washington, L. C. (2002). *Introduction to cryptography with coding theory.* New Jersey: Prentice Hall.

William S. (2011). *Cryptography and Network Security principles and practice.* (5th edition) .prentice hall upper saddle river. Pearson Education Inc.

(www.tutorialspoint.com/unix_socket/client_server model.html 2014 by tutorialspoint.)