INFORMATION SECRECY AND PUBLIC-KEY CRYPTOGRAPHY

Getahun Mekuria, Eneyew Adugna and G. Deva Rajan
Department of Electrical & Computer Engineering
Addis Ababa University

ABSTRACT

The subject and need of information secrecy with emphasis to the choice of fully using an already established public channel is to be discussed. Related histories and current achievements made in the area of information hiding, notable persons who changed the course of its progress from ancient times to this last generation are to be introduced with the intention of making every one alert of the subject and the pitfalls of an unprotected information being conveyed on a public channel particularly in the areas of banking and financial related sectors and every one using such global networks as the Internet.

INTRODUCTION

The world today is in such a communication facility where speed and quality of information being conveyed on public communication networks between two continently isolated entities (persons, computer terminals, answering machines or pagers) have really been in a satisfactory reputation, even though many research labs. and doctoral desertions have yet to do intense works for novel inventions in this respect. But the world is suffering from one other phenomena- *security*. Every one in diplomatic affairs, military quarters, research labs or business sectors is concerned not how fast to send an information to some remotely located center, but how secure will the information be conveyed. A bank receiving an Electronic Fund Transfer (EFT) wants to be assured of the source and the authenticity of the EFT before authorizing someone to draw millions of dollars from its account. The tragic game between Russian biochemist Vladmir Levin and Citicorp bank of U.S. is one example of such pitfall [6]. With in a period of less than five months the former was able to draw $12 million from San Francisco, Tel-Aviv, and Netherlands branches of the bank. A survey made in Nov 1995 on 1,295 U.S. companies indicate that 20% of the companies [6] had suffered from break-ins in to their very sensitive databases by intruders whom they had not known [6]; and the loss due to security failures directly or indirectly affects each one of us. Therefore implementation of some secrecy facility on an already established communication system, on the one hand, and establishment of a fast and secure system, on the other hand, are becoming hot issues of every communication service provider for reliable and lasting customer satisfaction.

INFORMATION SECURITY

So today the world is calling for a firm mathematical and engineering solution to the problem of information secrecy. Two of such solutions have so far been known: *Cryptography* and *Steganography*. The former deals with scrambling of an information in a way that the scrambled information becomes unintelligent before transmission on a certain public channel. The later, however, deals with the technique of hiding a *message data* under an *innocent looking data* so that any one who gets access to read the innocent looking data never suspects of the presence of some secret data hidden. Depending on the area of application and the available communication facility, the innocent looking data can be. a text; hiding another text or image message; or an image, also hiding other text or image messages. In this paper we shall present the historical review of cryptography and the basic ideas so far developed to maintain confidentiality and message authentication, and the authors will look forward for other opportunity to present about features of Steganography in the future.

In the general sense, information security can be achieved either by using secure communication channels between the communicating parties, which has a serious economic and complexity implications; or by providing a coding or scrambling of information so as to make it unintelligent to an *intruder,* or *an adversary*. The science and engineering approach of this technique is what we call *Cryptography*. Cryptography came from two Greek words: *kruptus*, meaning *secret* or *hidden*; and *graphy*, meaning writing; so that

cryptography deals with the technique of secret or hidden writing, the mathematical and engineering approach to the invention and implementation of hidden information communication. In view of what history witnesses and the present trend in use have been discussed in the following sections.

HISTORY AND DEVELOPMENT

Egyptians, Indians and ancient Hebrews are the recorded ancient users to different techniques of information hiding, though the techniques they were using has so far been secret itself. The reason being at that time, and even up to very recently, information secrecy was limited to the state affairs and military missions whereby the other people hadn't known not only the technique used but also the subject of hiding information itself. Around the last few decades of B.C. and the first few decades of A.D. Julius Caesar and Augusts Caesar used shifting of alphabets to encipher a text. Augustus Caesar used shifting of one character to the right [1]. According to this rule character A, for example, is replaced by B, G by H, Z by A etc cyclically. The transformation of a plain text in to something unintelligent by such replacement is known as *enciphering transformation* or simply *encryption*, and this value 'one' used in the transformation is known as the enciphering *key*. Up on reception, the intended receiver replaces each character by cyclically shifting one character to the left to get the original message. This reverse transformation is also known by a name *deciphering transformation* or simply *decryption*. The decryption key is also 'one' in this case. Julius Caesar on the other hand used a key of 'three' both for encryption and decryption [1]. These are the techniques so far known to be the earliest in the science of cryptography. Then up to the year 1500 different *monoalphabetic substitutions*, which means that a character is always substituted by one and only one other character, of different types and different enciphering discs came up to implement the developed ideas. In the year 1500, however, a new idea came in the scene; people started to replace one character by different other characters by applying different permutations and keeping the key identical for the encryption and decryption transformations. This technique is known to be *Polyalphabetic substitution*. The 1500's work of Johannes Trithemius [1] was the birth of that school of thought. Again other few centuries passed during which the rulers in states, officials in military commands, and the politicians in the diplomatic affairs rely on the polyalphabetic information hiding technique. Such works like Thomas Jefferson's wheel, the statesman and latter president of the United Satiates; Boris Hagelin's disk, a Swedish engineer; and also Shannon's 1949 paper on information secrecy, a year after his revolutionizing theory on communication systems, all referred and based on the polyalphabetic substitution technique [8]. Hagelin's enciphering disk was the one the Americans used in different designs as M-209 in the Army and as CSP-1500 in the Navy [3] to change the result of World War II and hence to change the course of history since then. In the first half of 1970s intense researches were made in the IBM corporation in response to the call made by NSA (National Standards Agency of U.S.) for development of a standardized encryption algorithm for information transmission within U.S. and also for information import and export to and from America. The work which had

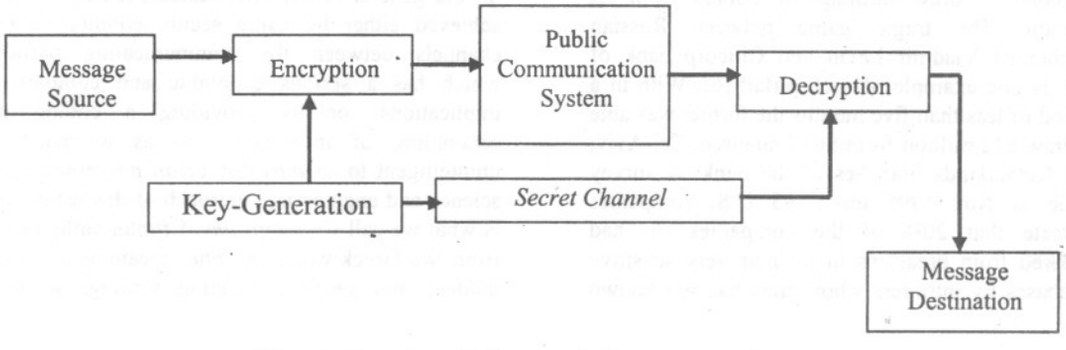

Figure1 Procedures in Symmetric Key cryptography

earlier started by Feistel and his group and later led by Tuchman in IBM Corporation [3],[8] came up with Data Encryption Standard (DES) in 1974, the first registered encryption standard in North America.

SYMMETRIC KEY CRYPTOGRAPHY

From those ancient times up to the year 1976 the cryptographic science is known by the name *Secret-Key Cryptography* and is also known by such alternate names like *conventional cryptography*, *symmetric-key cryptography*, etc. The reason for these name being the implementation of same keys in the encryption and decryption transformations to encipher a message before transmission and to recover the original message upon reception. To realize such a secured system an independent and secret channel must be established between the communicating parties for the exchange of the keys. This is the basic problem in symmetric-key cryptography. Assume two parties found at a continental distance from one another and they need to first establish some channel before communicating the actual message, and this is impossible due to many practical reasons. It is due to this reason that such works as Shannon's and any theory developed for the secret-key cryptosystem didn't bring a break-through to information secrecy theory. The procedures in Symmetric key cryptography are depicted in Fig.1 [8].

PUBLIC-KEY CRYPTOGRAPHY

In Nov. 1976 another turning point occurred in cryptography when W. Diffie and M.E. Hellman, both from Sanford University, published their paper "*New Directions in Cryptography*" [2] in which they discussed the possibility of achieving encryption and decryption with different keys with out compromising the secrecy of the information. Due to the problem of establishing the secret channel as discussed in section **VI** Diffie and Hellman suggested of publicizing the encryption key while keeping secret the decryption key in order to use the public channel both for key exchange and message transmission. It is this information hiding system, which is called *public-key cryptography*.

In public key cryptography each subscriber in a certain public communication system generates his own key pair, one for encryption, the *public-key*, and the other for decryption, the *private-key*. The public key is to be publicized and stored in a trusted communication directory and the private key is to be kept secret as long as the public key is in use. The inherent feature of this type of secrecy is that the private key must be unique to the public key and computation of that unique private key must be infeasible with in reasonably limited time and space. This is achieved by designing an appropriate one way function **h** for the generation of the key pairs. Let **h** takes some seeds as input to generate the public key **e** and the private key **d**,

$$\mathbf{e,d} \leftarrow \mathbf{h(seed_1, seed_2,\ldots)} \qquad (1)$$

where $\leftarrow$ means "results in generation of" here and every where in this paper. Then it has been assumed that the encryption function **f** and decryption function **g** have been properly designed [8].

Assume entity **A** wants to send a secret and confidential message **m** to entity **B**, so **A** finds the public key of **B**, $\mathbf{e_b}$, from the trusted communication directory and encrypts message **m** and sends the encrypted message **S** to **B** on the public channel.

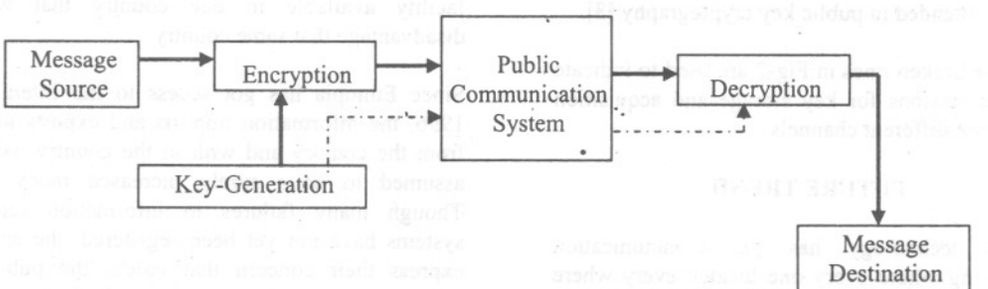

Figure 2 Procedures in Public key cryptography

$$S \leftarrow f(e_b, m) \quad (2)$$

An information encrypted by the public key of **B** gets decrypted only with the decryption key of **B**, d_b, which is known to **B** only. So, if an unauthorized third part gets access by any possible means between **A** and **B** and is able to down load the encrypted message, then no way to turn it in to its intelligent form. The proper design of the *one way function* **h** takes care for the infeasiblity of finding the decryption key given the encryption key.

Up on reception of **S**, **B** applies **g** and d_b on to **S** to recover the message **m** back to its original form and read.

$$m \leftarrow g(d_b, S) \quad (3)$$

Since the introduction of the polyalphabetic substitution people have come to be convinced that the secrecy of an information has to lie not in keeping secret the encryption and decryption transformations **f** and **g**, respectively, but only in the secrecy of the keys only. That is the reason for the publicity of so many encryption and decryption algorithms both in secret key and public key cryptosystems. In view of this the authors would also look forward to discuss some secure and reliable encryption/ decryption transformations in the category of public key cryptography in the future and show how this goal of secrecy is achieved.

As Shannon's 1948 theory revolutionized communication systems, so is the idea of public key cryptography by Diffie and Hellman to information secrecy. After this idea was developed not only is information hiding technique developed by avoiding that bottle-neck of the secret channel, but also the science that deals with breaking techniques of hidden information, *Cryptoanalysis*, has also developed drastically. Fig-2 indicates the sessions attended in public key cryptography [8].

Note: the broken lines in Fig-2 are used to indicate different sessions for key storage and acquisition and are not different channels.

FUTURE TREND

Today's technology has put communication engineering where every one located every where on the globe can get connections to any networking system through mobile and wireless communication facilities, making the issue of secrecy more complicated. Personal Communication systems (PCS), Low earth Orbiting satellites (LEOs) of IRIDUIM technology, and remote sensing networking devices of today's technology form the frame work of such systems. Computer Telephony Integration (CTI) which is used for voice-to-text and voice-to-fax messaging systems of recent achievements also need some secrecy backings for fast and reliable information exchange in voice or text mode. So the issue of secrecy in general and of public key cryptography in particular is to be merged to the newly invented hardware and system packages to make the world a fast and secure communication platform.

CONCLUSION

The aim for the production of this paper is two fold. The first one is to show the engineers and applied mathematicians in the country the subject of information secrecy, i.e. to review what has so far been made, and to invite and encourage them for new researches in the proper design of those functions **h**, **f**, and **g** to achieve secrecy through public key cryptography.

The need for information through out the world is unquestionable and as people every where get connection to the Internet the problem gets complicated. As someone gets deeper in to the subject it is clearly seen that different countries have different policies set towards information import and export with respect to their boundary. For example according to Sept.16 1998's release on information security from White House [7], U.S. America doesn't allow any encrypted message to be imported from the seven countries Libya, Iraq, Iran, Syria, Cuba, Sudan, and North Korea. This is basically to protect transmission and reception of information using the communication facility available in one country that would disadvantage that same country.

Since Ethiopia has got access to the Internet in 1996, the information imports and exports to and from the country and with in the country itself is assumed to have surely increased many fold. Though many failures to information security systems have not yet been registered, the authors express their concern that unless the public is

informed about the subject, particularly the engineers in the area; and unless the government gives attention and policies for secrecy are set at this earliest time, in a very recent future individuals who use the available communication resource to endanger the country will surely appear and crimes of different sorts that would humiliate every sector: private, business, local, diplomatic, governmental or non-governmental organizations surely appear. So, the second objective is a call for firm actions and policies to be set towards information secrecy based on the available cryptosystems at this earliest time before it becomes too late. And for this goal the authors suggest that if any measure is to be taken and any policy to information is to be set, then *public-key cryptography* would be the ideal solution.

ACKNOWLEDGMENT

The authors would like to acknowledge the department of Electrical Engineering, Addis Ababa University, for extending all the available facilities and encouragement given for the production of the paper.

REFERENCES

[1] "*Encyclopedia Britannica*," William Benton Pub. 15th Ed. Vol. 5 pp. 322-333, 1974.

[2] W. Diffie and M.E. Hellman: "*New Directions in Cryptography,*" IEEE Trans. Inform Theory. vol. IT-22, pp. 644-654, Nov 1976.

[3] Proceedings of the IEEE vol. 76 No-5, pp. 533- 574, May 1988.

[4] Arto Salomaa: "*Public Key Cryptography*" 2nd Ed. Springer-Verlag, 1996.

[5] A. J. Menzes, P.C. van Oorschot and S.A. Vanstone : "*Hand Book of Applied Cryptography,*" CRC Press, 1997.

[6] Michael Alexander: "*Net Security: Your Digital Doberman,*" Vantana Commu. Group, Inc. 1997.

[7] "The White House Briefing Room, Fact Sheet" Sept. 1998. S
Source: http//library.whitehouse.gov/PressReleases-plain.cgi?date=0&briefing=4

[8] Getahun Mekuria: "*Cryptography for Text and Image Data Communication*" M.Sc. Thesis, June 1999.