Use of Cryptography in communication

~ University Junior Assistant Ioana-Julieta Vasile (University of Bucharest)

Abstract:*This work envisages the presentation and analysis of important cryptographic systems in the field as well as the way these systems have been applied during the course of time. The work presents the advantages and disadvantages that derive from the use of cryptography while also emphasizing the importance cryptography has had along the way. Not least, the present article shall analyze the "Pretty Good Privacy" model – a widely used system nowadays, whose decryption key has yet to be found.*

Key words: code, message, communication, privacy, technological revolution

Introduction

The paper presents itself as a theoretical and practical approach to the phenomenon that characterizes communication and the means it is achieved through, without being endangered by unforeseeable factors that would alter the information flow. All along human history, both the desire and necessity of confidentiality in communication have perfected the science of secret writings, today known as cryptography. Now more than ever, cryptography is a safe method of maintaining the secret character of a communication. Messages were often intercepted during the communication process between two persons, thus jeopardizing the communication itself. In order to keep information secret, mankind has sought to develop various techniques by which meaningful information would be rendered meaningless during the time of its travel to the recipient. The recipient then, using similar techniques, would restore the message back to its original intended form, resting assured of its secrecy.

Currently, information plays a crucial role in the establishment of inter-human relations. Thanks to IT development, people on

different continents can immediately interact through e-mail, videoconference or chat programs. Also due to technological development, people's way of communicating has changed, and the exchange of information is accessible to everyone, fast and up to date. Along with the development of communication channels however, various methods of intercepting (e-) mail and phone conversations have also emerged. Information confidentiality has become an intensively debated topic these days in the wake of illegal intercept of communication. As such, cryptographers around the world have tried to create powerful encryption systems, which an unwanted party would not be able to decipher.

Evolution of cryptographic systems

From the very beginning, one must mention the confusion within the terminology of the cryptography field. The notions of "code" and "cipher" are often used to designate one and the same thing, although theoretically there is a clear difference between the two. "Code" refers to the word-level substitution, whereas "cipher" is the letter-level substitution. In daily life though, people use one of these terms to represent the meaning of the other, and the most utilized one is the "code".

Cryptology is the science that deals with information security, and its purpose is to fulfill four security criteria: *confidentiality, authentication, data integrity and non-repudiation.*

Confidentiality makes sure that nobody apart from the recipient may "read" the message. Currently, this criterion is more and more highlighted by human rights promoters and any attempt to breach one's confidentiality is harshly criticized and even more so – punished. In the past, the indiscretion that a received letter might also have been read by the recipient's relatives or close friends was easily overlooked; today however this is more than blameworthy since modern society emphasizes the individual and his / her privacy.

Authentication implies the possibility of identifying the information source, thus preventing a forged signature on the message. Letters that had been sent to kings or queens have every so often been intercepted by enemy spies who tampered with the content of the message, thus manipulating the judgment of the consignee. This is why in past times as well as today, every piece of information is personally signed so that it would not raise questions on the recipient's part. Still, even if a king has a custom seal applied on hot wax poured onto the letter, or even if an electronic authentication should provide enough credentials to the recipient, sender authentication is more or less credible, bearing in mind the various methods of forging the sender's signature.

Data integrity enables the protection of the sent information. Just like authentication, data integrity guarantees the truthfulness of the message being sent. If it is intercepted and if the content of the message is altered, unauthorized persons are able to modify the information content, misleading the recipient. Data manipulation may entail processes like insertions, delays, or substitutions.

Non-repudiation is the fourth security factor of cryptography. This deals with the denial prevention of previous engagements or actions. It refers to actions by individuals seeking to inflict moral or material damage (mostly) through the use of the Internet, but also through letters; it also pertains to the impossibility of convicting these indi-

viduals due to lack of proof. Currently, the latter is no longer an issue, since every piece of e-mail, and any bank transfers are made via the Internet, any intruder trying to breach the network and alter the data would easily be detected and pursued through the viable electronic address track down systems.

If all of these factors are observed, information transmission is secure. Let's not for - get the fact that along with the development of the data security field, counter measures have also gained momentum, in the form of various groups acting towards breaching the security barriers of the data transmission.

The first secret writings go back to ancient Egypt and Babylon, but also Greece. The first tangible piece of evidence as to the use of secret writing is recorded during the reign of the roman emperor Julius Caesar, who also was the creator of the cipher that bears his name. Still, before this cipher, in Herodotus' testimonials[1] one may observe an early form of the writing used by Julius Caesar.

Herodotus tells us of the disputes between ancient Greece and Persia in the 5th century B.C., of Greece's war for freedom, and Persian oppression. From Herodotus' reports, the use of secret writings by the Greeks had been decisive in repelling a surprise attack by the Persians. An exiled Greek named Demaratos, living in the Persian city of Susa is said to have observed the Persians' prepara - tions for war. In his desire to warn the Greeks of the inherent attack, and in order to keep the message secret from the eyes of the road guards, Demaratos carved his message on a writing board, and then covered it in wax, thus rendering it blank again. It is said that when the board reached Greece, Cleomenes' daughter Gorgo was the one who discovered the secret behind the blank board. The wax was removed, and the message was spread around the country.

Thanks to the secret note, Greece successfully defended itself against the Persian attack.

Another of Herodotus' examples pres - ents a similarly clever strategy of hiding a message. Hystaeus, a Greek citizen of king Darius' court used an original method of concealing his message, upon delivery of a secret message to Aristagore, his substitute in Miletus. The message was to contain information intended to persuade Aristagore to start an uprise against the Persian king. To send his message, Hystaeus had one of his slaves shave his head and then, using a short pointed dagger carved his message on the slave's scalp. He waited for the hair to grow back and cover the message, and then he sent the messenger who delivered the precious information. Such writings have been reported ever since Herodotus, describing various techniques of hiding messages. Apparently, the most utilized one is the writing in invisible ink. Different recipes have been used in writing invisible messages, of which we name but a few: the secretion of a plant (Thithymallus), used by Pliny the Elder, an ancient Roman nobleman, scientist and historian. The substance, when applied to paper and then reheated, turns a brown color. Another example is the one used by Giovanni Porta, who described a method of hiding a message inside a boiled egg. Using a substance mixed from 30 grams of alum and half a liter of vinegar, he would apply it on the boiled egg's shell. The sponge-like surface would allow the substance to impregnate on the egg white while remaining invisible on

[1] Herodot, *Istorii, vol. II, Cartea a VII-a*, editura Științifică, București, 1964

the outside. The recipient would only have to peel the egg and read the message. Such recipes for invisible ink types are also described by Roman authors. In his work, Victor Udrinschi[2] shows the formulae for multiple types of invisible ink, and moreover, the substances that would reveal the hidden message, rendering it visible again.

The secret writing, by which information is hidden, is called steganography. The word comes from the Greek „steganos" which means „cover", and „graphein" meaning „to write". The use of steganography has proved to be safe to a certain extent, although a thorough checking of the messenger lead to the discovery of the message. This is why in order to render a message useless to the unintended party, cryptography has evolved alongside steganography. (from the Greek „kryptos" meaning „hidden"). Cryptographers deal with the design of encryption systems intended for safe delivery of information. As opposed to steganography, cryptography does not hide the message itself but its meaning through encryption: "in order to render a message meaningless, it will be encrypted by a special protocol, upon which both sender and recipient previously agree. This way, the recipient is able to reverse the encryption, giving sense to the message once again." Even if the enemy intercepts the message, it will be very difficult if not impossible to decrypt it. To better secure the information, cryptography and steganography can be used together just as the Germans did during the Second World War: "German agents in Latin America would shrink a text page by photocopying it, down to the point where its diameter would be less than a millimeter in size and then hide it in the top side of an ap - parently normal letter" .

On the other hand there are cryptanalysts, the ones who intercept and decipher secret messages. Often cryptanalysts are very well informed as to the encryption methods, and so manage to reproduce encrypted messages using cryptographers' patterns. This has determined the cryptographers to constantly develop more and more complex encryption systems and keep them secret for as much as possible.

Pretty good privacy (PGP)

Currently there is a method by which sent messages remain safe up to the point of delivery. The PGP software encryption program launched in 1991 by Phil Zimmermann has caused an ample debate around the existence of such an encryption system. The ideas of creating a powerful enough encryption system and its development have proven to be two different phenomena. Along with the launch of the PGP, two sides have emerged, the pros, and the cons. On the one hand, the side that supports the use of PGP is made up of common people and human rights activists, who see this program as the ideal platform for enforcing the right to confidentiality. On the other hand, the side against the PGP is made up of government institutions and security agencies which argue this program enables communication between evil-doers and therefore should be banned from use. Two consequences arise from the creation of PGP. First off, PGP is more and more used by normal people because it provides security to the message. Secondly, the vehement reaction of the security agencies pertaining to this program has once again demonstrated their

[2] Victor Udrinschi, *Criptografia. Diverse procedee de a coresponfa cifrat*, Editura Tipo-Atkis, Bucuresti, 1996, p. 116-123

inability to break PGP encrypted messages.

On the other hand, the use of encryption systems also simplifies the way we communicate. We are right in stating that the communication process is hardened by disturbing factors such as noise, which, in the Internet environment translate into abstention, or rather selective communication due to the fear that a third party may be eavesdropping or intercepting information. Today, more than two billion people use the Internet and are able to organize electronic meetings (of various sorts), in real-time, manage financial transactions, talk to friends or relatives no matter where they are in the world. The use of powerful encryption systems such as PGP is absolutely necessary to the wellbeing of the communication process.

In the economic field, encryption systems play a crucial role. Every so often a company is harmed by another company which has gained access to sensitive information and used it malevolently. The development of client-company relationships in the last decades requires constant data communication between the two parties, and encryption systems have offered a proper environment for this purpose. For example banks can immediately receive client reaction and if necessary adjust marketing strategies and modify program elements according to client preferences. Of course all these elements are confidential, as they are destined to the client-bank relationship.

The positive impact that PGP has had, has spread over cryptography in general, and the usage of this program as well as many other encryption programs has become indispensable when viewed in the context of Internet communications. The fate of cryptography nowadays depends on the arguments one can produce, be they pro or against it. As for the PGP software encryption program, it now enjoys an ever-growing number of users and the PGP Corporation has created additional encryption services intended for digital telephony and chat programs.

In Romania the PGP encryption system has not made that big an impact on society as it has done in the developed countries. The number of PGP users is limited and those who have even heard of it are reluctant to use it since they don't see its necessity. Although PGP or other encryption programs are free to download from the Internet, those who use encryption systems in Romania remain banks, corporations, or military forces. One of the main reasons why users of e-mail or digital telephony rely solely on the respective programs' security methods is NSA's, or other agencies' relative lack of interest toward us . One must add that the necessity to use PGP or other encryption software is up to each individual in part and if someone really wants his or her information to remain secret he or she will previously make sure of that.

Conclusions

The need of confidentiality in messages has determined the emergence of cryptography. Along with the first encryption systems, cipher and code cryptanalysis techniques have also evolved. The fight between the two (cryptographer and cryptanalyst), has contributed to the evolution of cryptographic systems and to the ever-growing people's interest in information confidentiality. Currently there is no answer on cryptanalysts side to such a powerful system as the PGP. As we have seen along the way however there is

no unbreakable or undecipherable code. It's probably only a question of time. In fact this is the most elegant aspect of the PGP: it's not the complexity of the system that baffles the cryptanalysts but the time needed to determine the values that lead to the decryption of the program.

In the future we can only hope that a new technological revolution will contribute to the decryption of programs such as PGP, and researchers claim that quantum physics will have something to say about it. According to theorists this new field will totally change the way computers function, boosting their performance by several orders of magnitude. Even if quantum computers will be of great help to cryptanalysts, the emergence of this new technology will also lead to the development of new and far more powerful encryption systems. And so the battle between cryptographers and cryptanalysts will go on and a total success on either side is improbable.

REFERENCES:

1. **Dinu, Mihai,** *Comunicarea. Repere fundamentale*, Editura Algos, Bucureşti, 2000
2. **Herodotus,** *Histories, vol. II, 7th book*, Editura Ştiinţifică, Bucureşti, 1964
3. **Mattelart, Armand, Mattelart, Michele,** *Istoria teoriilor comunicării,* Editura Polirom, Iaşi, 2001
4. **Singh, Simon, Cartea Codurilor.** *Istoria secretă a codurilor şi a spargerii lor,* Editura Humanitas, Bucureşti, 2005
5. **Udrinschi, Victor,** *Criptografia.Diverse procedee de a coresponda cifrat,* Editura Tipo-Atkis, Bucureşti, 1996

Websites:

6. http://forum.softpedia.com/lofiversion/index.php/t44945.html
7. http://portal.feaa.uaic.ro/C8/Protecţia%20şi%20securitatea%20siste/Suport_curs/criptografie.pdf