"CRYPTOGRAPHY AND DATA SECURITY: FROM CRYPTOGRAPHIC TECHNIQUES TO DATA PROTECTION"

Course: Cybersecurity and Cybercrime

Student: Benedetta Simonini

July 2020

Table of contents

Introduction

Data security is critical not only for businesses but also for home computer users.[1] From client to payment information, personal files, or bank account details, all this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Indeed, data lost due to disasters, such as a flood or fire, is crushing, but losing it because of hackers or malware infection can have much greater consequences.

Therefore, data security is the science that studies the methods to protect data in computer and communication systems.[2] It embodies cryptographic controls to face security threats.

Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into an unintelligible form (ciphertext).[3] Every cryptosystem consists of five elements: plaintext, encryption algorithm, decryption algorithm, ciphertext, and Key. The plaintext is messages or data that are in their normal, readable (not encrypted) form. Encryption is the process of converting plaintext to ciphertext by using a key. Ciphertext results from the encryption performed on plaintext using an algorithm, called a cipher.[4] Decryption is the process of retrieving the plaintext back from the ciphertext. Finally, the Key uses the information to control the cryptosystem (cipher system), and it is known by the sender and the receiver only.

By means of this paper, the cryptographic techniques that are relevant for data securitization will be technically analyzed. Moreover, it will be shown that even though these techniques are strong, they present some vulnerabilities to cyber-attacks and they would need to be improved. Thus, after having explained the role of cryptography for data security, I will expose this science in relation to the General Data Protection Regulation, or GDPR.

Therefore, the first section analyzes the relevance of cryptography for data security. The second section examines the broad varieties of cryptographic techniques based on symmetric and asymmetric key encryption algorithms. It is relevant to analyze these techniques from a technical point of view to understand how to implement them to secure data. Then, given the relevance of the topic for several organizations, in the third part, the paper analyzes the pros and cons of encryption at the

[1] Lessig, L. (1999). Code and Other Laws of Cyberspace. p. 35.

[2] Data privacy vs. data security [definitions and comparisons] – Data privacy manager. (2020, July 8). Retrieved from https://dataprivacymanager.net/security-vs-privacy/

[3] What is encryption and how does it work? (2020, April 16). Retrieved from https://searchsecurity.techtarget.com/definition/encryption

[4] Berti, Hansche, Hare (2003). *Official (ISC)² Guide to the CISSP Exam*. Auerbach Publications. pp. 379. ISBN 0-8493-1707-X.

organizational level. Finally, the last section focuses on data protection with regard to the GDPR for cryptography.

1. Cryptography in data security

1.1 Role in securing data

Lawrence Lessig (1999) wrote, "Encryption technologies are the most important technological breakthrough in the last one thousand years".[5] It might seem a slight exaggeration but it emphasizes the importance of encryption technologies in today's digital world. Indeed, encrypted data play a significant role in the protection of data subjects' privacy.

Cryptography is the science of using mathematics to encrypt and decrypt data.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptography provided secrecy for information sent over channels where eavesdropping and message interception was possible. The sender selected a cipher and an encryption key, and either gave it directly to the receiver or else sent it indirectly over a slow but secure channel - typically a trusted courier. Modern cryptography protects data transmitted over high-speed electronic lines or stored in computer systems. Figure 1 below shows how a classical information channel works.

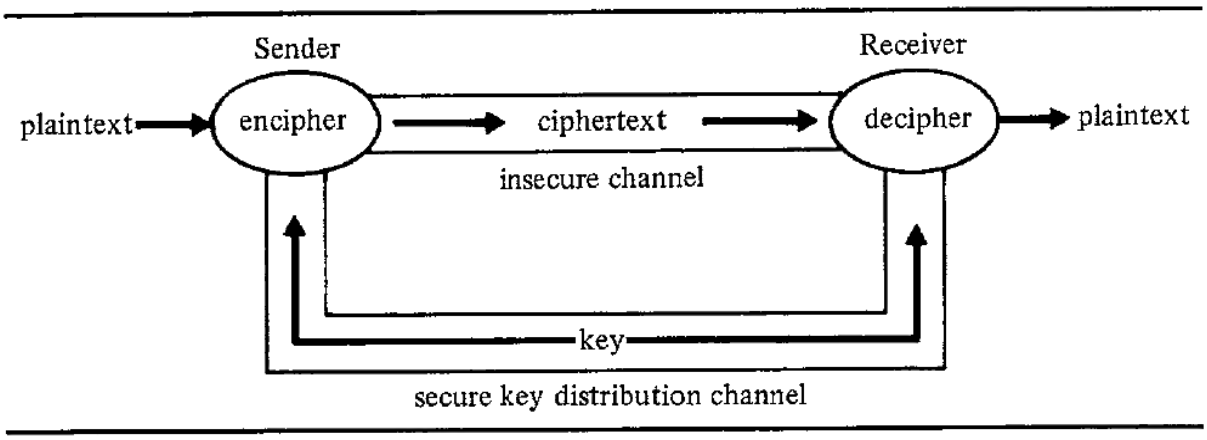

Figure 1. Classical information channel.
Source: Denning, D. E. (1982). *Cryptography and data security*. p.4.

[5] Lessig, *supra* note 1

There are two principal objectives: secrecy (or privacy), to prevent the unauthorized *disclosure* of data, and authenticity or integrity, to prevent the unauthorized *modification* of data. Within computer systems, the data are vulnerable to several threats (see Fig. 2).

Among the threats to secrecy, it is relevant to include *browsing*, *leakage*, and *inference*.

Browsing refers to searching through main memory or secondary storage for information (e.g., confidential data or proprietary software programs). Browsing poses a more serious threat than eavesdropping in the communication channel and it is possible only if the user has access to the system and unauthorized regions of memory.

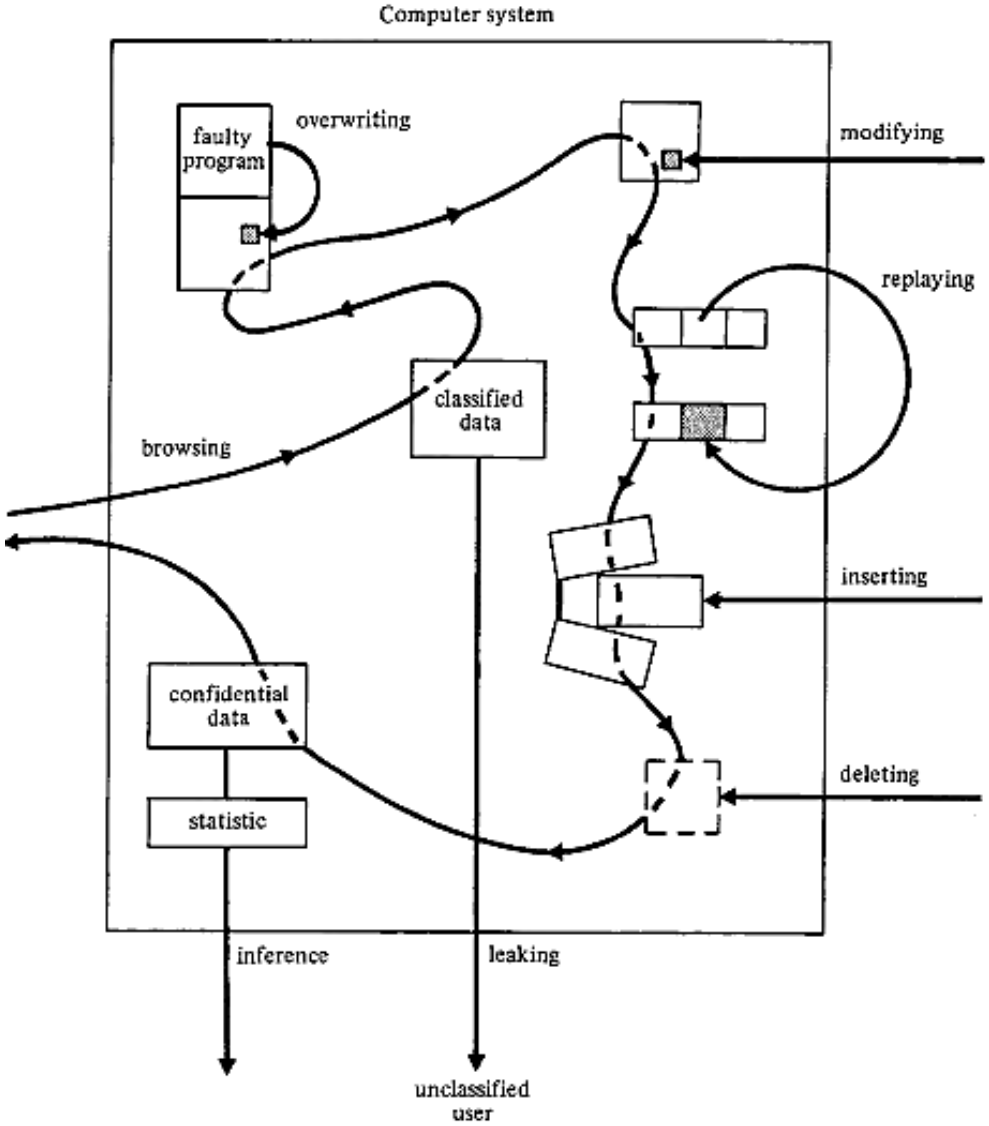

Figure 2. Threats to data stored in computer systems.
Source: Denning, D. E. (1982), *Cryptography and data security.* p. 5.

Thus, what is the role of cryptography in securing these data? Cryptography can protect against browsing by making the information incomprehensible. It is especially useful for protecting data on

tapes and discs that, if stolen, can no longer be protected by the system. However, cryptography cannot protect data from disclosure while it is being processed in the clear. Thus, if the access is not controlled, encrypted data can also be vulnerable to ciphertext searching (e.g., finding employees making identical salaries by searching for records with identical ciphertext salaries). Cryptographic solutions to this problem will be described in the second section.

Leakage is about the transmission of data to unauthorized users by processes with legitimate access to the data.
As Denning (1982, 6) argues, "Inference refers to the deduction of confidential data about a particular individual by correlating released statistics about groups of individuals". For instance, if Paul is the only non-Ph.D. faculty member in a Mathematics department, Paul's salary could be inferred by correlating the average salary of all faculty in the department with the average salary of all Ph.D. faculty in the department. Even though cryptography can protect the data records from browsing, it does not provide a mathematical framework for determining which statistics can be released without disclosing sensitive data. Therefore, in this framework, the main cryptographic goals refer to the main aspect of information security.

1.2 Cryptographic goals

Cryptography can also be defined as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.
The principal goals of cryptography are the following: (1) confidentiality or privacy, to prevent the unauthorized *disclosure* of data; (2) data integrity, to prevent the unauthorized *modification* of data; (3) authentication; (4) non-repudiation.

1. **Confidentiality:** Is a term synonymous with secrecy and privacy. There are several approaches to providing confidentiality, ranging from physical protection to mathematical algorithms, which render data unintelligible.
2. **Data Integrity:** Addresses the unauthorized alteration of data: to ensure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.
3. **Authentication:** Is a service related to the identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. The information delivered over a channel should be authenticated as to the origin, date of origin, data

content, time sent, etc. For these reasons, this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication.

4. **Non-repudiation:** Is a service that prevents an entity from denying the validity of previous commitments or actions. Thus, this is widely used in information security and it refers to a service that provides proof of the origin and the integrity of the data. Finally, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and the integrity of that message.

It is fundamental for cryptography to adequately address these areas in theory and practice so that it could be about the prevention and detection of cheating and other malicious activities.

1.3 Cryptography vulnerabilities and cyber-attacks

Even though the relevance of cryptography for data security is evident, encryption is often a target of cyber-attacks and DDoS attacks. It is argued that encryption-based cyber-attacks have increased by the 90% each year since 2015.[6] Also, according to researchers, 80% of page loads on millions of sites sampled are encrypted.[7] Thus, while encryption has always been reassuring for organizations and consumers, it is also opening up new threat vectors for cybercriminals. What often happens is that organizations use to disrupt basic encryption protocols or bypass them. Therefore, Transport Layer Security (TLS) and Secure Socket Layers (SSL) adoption have become the norm for organizations of all sizes and in all industries due to several driving factors: the EU General Data Protection Regulation (GDPR), Google search results ranking preferences, browser warnings for HTTP (Cleartext) sites, and the growing importance of privacy.

A large percentage of attacks target the TLS/SSL protocol governing client-server authentication and secure communications. Also among service providers, the attacks targeting secure web services, such as HTTPS, rose significantly.[8] The HTTPS traffic can serve as a perfect backdoor for malware or data extraction. The data extraction happens because the attackers might exploit the vulnerability of the connection. Thus, the connection could be the opening malware needs to spread rapidly throughout the weak points of a network.

Concerning protocols, as more companies are adopting better encryption practices, cybercriminals are turning to SSL/TLS vulnerabilities to deliver malicious attacks. The growth in SSL/TLS usage

[6] Encryption-based cyberattacks are increasing: How to stay safe. (2018). Retrieved from https://www.arrayasolutions.com/encryption-based-cyber-attacks-are-increasing-how-to-stay-safe/

[7] Defend against encrypted threats. Retrieved from: https://www.f5.com/labs

[8] NETSCOUT. (2019). Network security infrastructure report. Retrieved from https://www.netscout.com/report/

includes both legitimate and malicious activities, as criminals rely on valid SSL certificates to distribute their content. Thus, it is central to the security arsenal to be able to encrypt traffic securely and to attest to its authenticity without slowing, compromising, or disrupting legitimate traffic.

2. Cryptographic techniques

The cryptographic techniques are divided into two generic types: *symmetric-key* and *asymmetric-key* (or public-key) encryption. Since these two categories can provide all security objectives, they will be examined in this section.

2.1 Symmetric-key encryption

This technique is known also as secret-key encryption; here one key is used both for encryption and for decryption. Symmetric-key systems are faster and simpler but the challenge is that both the sender and the receiver have to try to exchange keys securely. The most popular symmetric-key cryptography systems are Data Encryption System (DES) and Advanced Encryption Standard (AES), these will be explained later in this section.

This section analyzes two classes of symmetric-key encryption schemes commonly distinguished: block ciphers and stream ciphers.

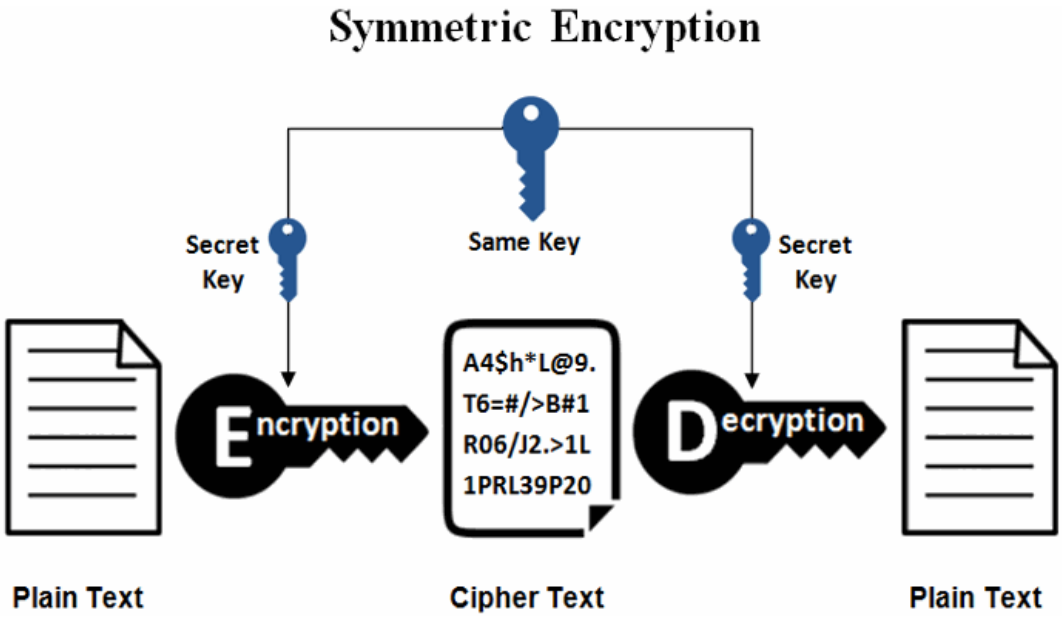

Figure 3. Symmetric-key encryption.
Source: Williams, E. (2020). Cryptography 101: Symmetric encryption.

2.1.1 Block ciphers

Block cipher is an encryption scheme that takes a block of plaintext and generates a block of ciphertext bits. The choice of the block size does not directly affect the strength of the encryption scheme and it is fixed in a given scheme. The strength of the cipher depends upon the key length. The longer the block size, the more secure the system will be.
Even if any size of a block is acceptable, some aspects need to be taken into account while selecting the size of a block: first, very small block size would need to be avoided, second, it is not effective to have a large block size and a block size should be a multiple of 8 bit. The most relevant and popular block ciphers are:

1. DES: It is the quintessential block cipher and it is considered as a 'broken' block cipher, due primarily to its small key size.
2. 3DES: It is a variant scheme based on repeated DES applications. It is still a respected block cipher but it is inefficient compared to the new faster block ciphers available. In fact, due to its small block size (64-bit), this was proven ineffective against brute-force attacks.
3. AES: It is a relatively new block cipher based on the encryption algorithm Rijndael, which is a family of ciphers with different keys and block sizes.
4. IDEA: It is a sufficiently strong block cipher with a block size of 64 and a key size of 128 bits.
5. Twofish: This scheme of block cipher uses a block size of 128 bits and a key of variable length.

The three most relevant classes of block ciphers are *substitution*, *transposition* and *product* ciphers.

2.1.1.1 Substitution ciphers

Substitution is an easy way to hide a text – it consists of replacing one letter with another letter or perhaps a number or a symbol. This might sound simple but it is relevant and challenging to strategically replace each letter. In fact, it needs to be done in a way that enables both the sender and the receiver to encipher/decipher accurately (accuracy is a key point in securing data). In sum, both sides must know the algorithm for replacing each letter. Practically speaking, encoding or decoding algorithms that involve huge charts is not easily feasible. Thus, the methods should be easy to use and the ciphers should be easily understandable among them.
Another method of substitution is to convert the letters (of whatever alphabet) into numbers. This in turn opens up a host of opportunities for further encipherment, because it is possible to do the math on numbers much more easily than on letters.

These ciphers replace bits, characters, or blocks of characters with substitutes. A simple type of substitution cipher shifts each letter in the English alphabet forward by K positions (shifts past Z cycle back to A); K is the key to the cipher.[9] The cipher is often called a Caesar cipher because Julius Caesar used it with K = 3, the alphabet is shifted three spaces and each letter of the plaintext is replaced by the new letter. Caesar cipher is a very simple mono-alphabetic substitution (see Fig. 4) and from the figure below, it is possible to derive an explanatory example.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P
Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figure 4. Caesar Cipher.

Therefore, the following illustrates Caesar's method:

IMPATIENT WAITER

↓

LPSDWLHQW ZDLWHU

2.1.1.2 Transposition ciphers

Transposition ciphers rearrange characters according to some schemes. In this case, there is a change in the place of the plaintext letter in the message. The scramble-grams that many newspapers carry are simple examples of transposition ciphers. For example, {help} might become {eplh}. The letters are all the same, just their position change. In that case, enciphering the plaintext is straightforward but rather the challenge is enciphering the message in such a way that allies can be able to decipher it and enemies cannot. Thus, the transposition cipher depends on an algorithm – which the sender and recipient must agree on beforehand.

This rearrangement was classically done with the aid of some types of geometric figures.

[9] Denning, D. E. (1982). *Cryptography and data security*. Addison Wesley Publishing Company.

First, the plaintext was written into the figure according to some "write-in" path. Second, the cipher text was taken off the figure according to some "take-off" path.[10] The key contained the figure together with the write-in and take-off paths.

Thus, encipherment proceeded in two steps as shown in the following figure:

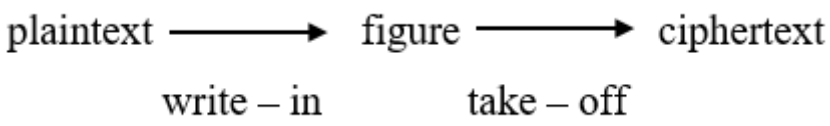

Figure 5. Transposition ciphers.

2.1.1.3 Product ciphers

Simple substitution and transposition ciphers individually do not provide a very high level of data security. However, by combining these transformations it is possible to obtain strong ciphers more secure than the individual components. The basic idea of a product cipher is to build a complex encryption function by composing several simple operations that offer complementary, but individually insufficient, protection. Basic operations include transpositions, translations, and linear transformations, arithmetic operations, modular multiplication, and simple substitutions.

Data Encryption Standard (DES)

DES is the quintessential block cipher. Even though it is now quite old and a bit out on the way, no discussion of block ciphers can omit mention of this construction. DES is a remarkably well-engineered algorithm that has had a powerful influence on cryptography. Despite it has been replaced by the Advanced Encryption Standard (AES), it is still used.

DES encrypts data in 64-bit blocks with a 56-bit key. Therefore, it encrypts data 64 bits at a time. The key can be any 56-bit number and it can be changed at any time. A handful of numbers are considered weak keys, but they can easily be avoided. All security rests within the key.

A 64-bit block of plaintext goes in one end of the algorithm and a 64-bit block of ciphertext comes out the other end. DES is a symmetric algorithm: the same algorithm and key are used for both encryption and decryption (except for minor differences in the key schedule). At the simplest level,

[10] Ibid.

the algorithm was nothing more than a combination of two basic techniques of encryption: confusion and diffusion. The building block of DES is a single combination of these techniques on the text and it is based on the key. This is known as a round, and DES has 16 rounds, so it applies the same combination of techniques on the plaintext block 16 times.

Advanced Encryption Standard (AES)

Even though the DES presents several strong technicalities for data security purposes, this has been replaced by Advanced Encryption Standard, or AES, in 2002. The main problem was mostly linked to the relatively short key length of DES. Given the advancement in computing power, a key space of 2^{56} keys was just too small. Hence, AES is based on a *substitution-permutation network* and it is a sub-set of Rijndael. The algorithm may be used with three different types of keys with lengths - or block sizes - of 128, 192, and 256 bits, making it potentially stronger than the 56-bit key of DES. Therefore, these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256". AES with a 256-bit key size has a potential 115 quattuorvigintillion possible keys or 115 with 78 digits following it.[11] Thus, there is no known practical attack that could brute-force an AES-256 key. Therefore, national authorities and governments suggest regularly assessing whether the encryption method remains appropriate. Rather than develop a custom algorithm it is thus recommendable to use a trusted and verified algorithm to provide higher security to malicious attacks.

2.1.2 Stream ciphers

Stream ciphers (Vernam, LFSRs, RC4, GSM A5, OFB, and others) form an important class of symmetric-key encryption schemes. They are very simple block ciphers having a block length equal to one. They are useful because the encryption transformation can change for each symbol of plaintext being encrypted. Thus, when in some situations the transmission errors are highly probable, stream ciphers are advantageous because they have no error propagation. In addition, they can be used when the data have to be processed one symbol at a time (e.g., if the equipment has no memory or buffering of data is limited)

The encryption algorithm in this case is composed of three steps:

1. Assign a number to each character of the plain text and the key according to alphabetical order.

[11] How should we implement encryption? (2020). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/how-should-we-implement-encryption/

2. Add both the numbers (it means the corresponding plain-text character number and key character number).
3. Subtract the number from 26 if the added number is greater than 26. If this does not happen, it is necessary to leave it.

Because the algorithm behind symmetric encryption is less complex and executes faster, this is the preferred technique when transmitting data in bulk.

2.2 Public-key encryption

Public-key encryption is an asymmetric cryptography scheme that uses a pair of keys for encryption: a public key, that encrypts data, and a private key for decryption.
Thus, under this system, a pair of keys is used to encrypt and decrypt information. The public key is used for encryption and the private one is used for decryption. This technique is used mostly for *end-to-end encryption*. Therefore, in an *asymmetric* encryption scenario, the private key needs to be kept secret. The risk that a third party could obtain the key consequently arises e.g. if the secret key is stored at a cloud provider which also holds the public key or by *man-in-the-middle attacks.*

Public and private keys are different. Even if the public key is known by everyone, only the intended receiver can decode it because he alone knows the private key. The primary benefit of public-key encryption is that it allows those who have no pre-existing security arrangement to exchange messages and data securely.
Thus, the data encrypted by a public key is decrypted by the corresponding private key: the encrypted data is called ciphertext also here. Figure 6 below does not represent all the steps of the asymmetric encryption/decryption process but it allows us to understand the general logic of the process.

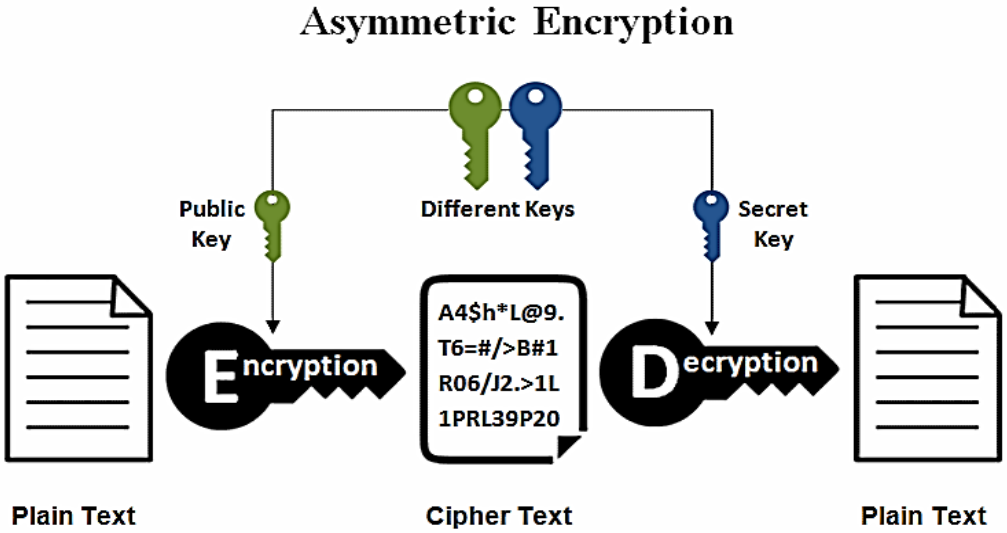

Figure 6. Asymmetric-key encryption.
Source: Williams, E. (2020). Cryptography 101: Symmetric encryption.

Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms such as DES. In fact, most of the public-key encryption is used for the transport of keys subsequently used for bulk data encryption by a symmetric algorithm and other applications including data integrity and authentication.

Public-key encryption's main objective is to provide confidentiality or privacy; moreover, it may also provide authentication guarantees in entity authentication and authenticated key establishment protocols. Typically, public-key cryptosystems can encrypt messages of limited length only and are slower than symmetric ciphers. To encrypt longer messages usually a public-key encryption scheme is used and this combines symmetric and asymmetric encryption like this:

- For the encryption, a random symmetric key 'sk' is generated, the message is symmetrically encrypted by 'sk', then 'sk' is asymmetrically encrypted using the recipient's public key.
- For the decryption, first the 'sk' key is asymmetrically decrypted using the recipient's private key, then the ciphertext is decrypted symmetrically using 'sk'.

The most relevant public-key cryptosystems are ElGamal (named for its inventor, Taher ElGamal), RSA (Rivest–Shamir–Adleman), and Elliptic Curve Cryptography (ECC), which is based on the algebraic structure of elliptic curves over finite fields. Here below, ElGamal and RSA will be analyzed.

ElGamal cryptosystem is based on the Discrete Logarithm Problem. ElGamal is more efficient for decryption and, for the same level of security, very short keys are required. However, it is not very

popular in the market. The ElGamal encryption consists of three components: the key generator, the encryption, and the decryption algorithm. Through these three steps, its security depends upon the difficulty of a certain problem related to computing discrete logarithms. The security of the ElGamal scheme depends on the properties of the underlying group as well as any padding scheme used on the transmitting data.

When the key pair is distributed it is not necessary to distribute the private key because this could allow someone to break encryption tunnels, or pretend to be the entity who has had their private key stolen. The Lenovo hack of a few years ago is a representative example of this: the key pair was distributed with the software and someone cracked the password on it just in few minutes. In fact, after this, anyone could crack the tunneled communication to Google. But, what is actually on a key? To understand this, it is relevant to examine the RSA key.
RSA algorithm (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) is one of the first public-key systems and it is used for securing data transmission. It has a potential maximum key size of 4096-bits. RSA is an asymmetric encryption algorithm that uses two keys, one to encrypt and the other to decrypt. Thus an RSA key pair, namely public key and private key, is generated as the base for the communication and the exchange of data.
RSA public-key cryptosystem is based on the math of modular exponentiations, together with the computational difficulty of the integer factorization problem. In practical terms, there is a modulus N which is the multiplication of two prime numbers: P and Q. Then, a value of (E) is selected, and the encryption key (the public-key) is (E,N). After this, a decryption key (D) is determined, and the private key becomes (D,N).
For several years, key sizes of 102-bits were commonplace. However, in 2007 the National Institute of Standards and Technology recommended increasing minimum key size due to advances in computing power. The minimum recommended was 2048-bits up to the year 2030, and 3072-bits after 2030.

The security of RSA depends on the strengths and the length of the key size. The RSA cryptosystem is the most popular public-key cryptosystem strength, which is based on the practical difficulty of factoring the very large numbers.
A typical application is in authenticating a sender, where the sender’s private key is used to encrypt a message, and then is decrypted by the receiver with the sender’s public key. However, it is also typically used for encrypting disks and files.

These are the main steps:

1. Encryption Function: It is considered as a one-way function of converting plaintext into ciphertext and it can be reversed only with the knowledge of a private key.
2. Key Generation: The difficulty of determining a private key from an RSA public key is equivalent to factoring in the modulus n. An attacker thus cannot use knowledge of an RSA public key to determine an RSA private key unless he can factor n. It is a one-way function where going from p & q values to modulus n is easy but the reverse is not possible.

The RSA scheme is more efficient for encryption and less efficient for decryption. In fact, for a particular security level, lengthy keys are required in RSA. RSA, in comparison to ElGamal, is widely accepted and used for security purposes.
To ensure security with the RSA algorithm some certificate providers should therefore increase the key size of their certificates to take account of the recommendation.
However, over time, vulnerabilities may be discovered in encryption algorithms that can eventually make them insecure. Thus, it is necessary to regularly assess whether the personal encryption method remains appropriate. In addition, it is relevant to ensure that the key size is sufficiently large to prevent brute force or other methods of attack over the lifetime of the data.
Finally, it is important to ensure that symmetric and asymmetric keys explained above remain secret because the key provides the ability to decrypt data.

3. Pros and cons of encryption

Since data can be compromised in many ways, the technical measures explained above, combined with also physical security and well-educated staff are key strategies to be implemented against cyber-attacks. Thus, to build a solid structure within an organization, it would be necessary to implement clearly defined policies into the infrastructure and effectively present them to the technical staff.
Even though it seems common sense to use data encryption in businesses and other entities for security, many organizations are opposed to encrypting data because of some of the obstacles involved with doing so. It emerges that cryptography has its pros and cons and organizations must look at all of the considerations to make an informed decision about encryption. Thus, now I will expose the critical as well as the positive points of encryption. Moreover, I examine how encryption is becoming a double-edged sword useful but not wholly sufficient for data protection.

3.1 Pros of data encryption

- Separation: Data encryption allows the data to remain separated from the device security where it is stored. Security is included with the encryption that allows administrators to store and transmit data via unsecured means.
- No data breaches: Data encryption avoids the potential complications that accompany data breaches, which provide ensured protection of intellectual property and other similar types of data.
- Encryption is on the data: Because the encryption is on the data itself, the data is secure regardless of how it is transmitted. An exception to the rule can be transmission tools, such as email because sometimes a typical email account does not provide the necessary security.
- Encryption Equals Confidentiality: Several organizations are required to meet specific confidentiality requirements and other associated regulations. Encrypting data means that it can only be read by the recipient who has the key to opening such data.

3.2 Cons of data encryption

- Encryption Keys: Undoubtedly, data encryption is a monumental task for an IT specialist. The more data encryption keys there are the more difficult IT administrative tasks for maintaining all of the keys can be. If the key is lost to the encryption, thus the data associated with it are lost.
- Expense: Data encryption can prove to be quite costly because the systems that maintain data encryption must have the capacity and the necessary upgrades to perform such tasks. Without capable systems, the reduction of systems operations can be significantly compromised.
- Unrealistic Requirements: If an organization does not understand some of the restraints imposed by data encryption technology, it is easy to set unrealistic standards and requirements that could jeopardize data encryption security.
- Compatibility: Data encryption technology can be tricky when you are layering it with existing programs and applications. Thus, this can negatively affect routine operations within the system.

Finally, in cryptography - widely used to hide the content of a secret message - a known message passes through the network and government departments know most of the algorithms. Also, on the one side, some of the stronger algorithms among those exposed in the previous section are currently resistant to brute-force attacks. On the other side, large expensive computing power is required for cracking, and ultimately as the technology increases, the strength reduces.

4. Data protection and GDPR

Data protection involves measures for protecting individuals during the processing of their data. Data protection and privacy laws forbid the dissemination of this information and, in a privacy context we are not talking about protection *of* data, but protection *from* data. Concerning this, it is worth noting that the German Constitutional Court has coined the phrase "right to informational self-determination".[12] This prevents the enterprises and government agencies from simply doing whatever they want with the data of private citizens. In addition, this legislation guarantees the fundamental right of individuals to determine whether and how their data should be used or released.

Therefore, after years of intensive negotiations, the GDPR has come into force on May 25th, 2018. Due to its legal form of a Regulation, the GDPR will be binding in its entirety and it is directly applicable in all Member States of the European Union.

The GDPR requires the implementation of appropriate technical and organizational measures to ensure a secure personal data process. The final version of the GDPR does not provide a further definition of encrypted data but mentions encryption in several provisions as a compliance requirement.[13] Recognizing the relevance of encryption for securing data, Article 32 of the GDPR regards encryption as an appropriate technical and organizational measure that ensures the security of processing, depending on the nature of the risks.[14] It emerges that this does not deal with the applicability of the GDPR, but rather with the protection of personal data. It derives that encryption solutions are widely available and they could be deployed at a relatively low cost.[15]

The encryption mechanisms exposed above play a critical role in keeping online criminals away from personal data. Therefore, in this last section, I will explain the GDPR's scope in encryption, its effects on security measures, and then the impact of different encryption techniques upon the GDPR's Material Scope.

[12] Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*(1), 84-88. doi:10.1016/j.clsr.2008.11.002

[13] Home. (2020). Retrieved from https://ico.org.uk/ https://ico.org.uk/

[14] Vollmer, N. (2020). Article 32 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan. Retrieved from https://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

[15] Encryption. (2020). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

4.1 GDPR's scope in encryption

The material scope of GDPR is personal data. This means that the GDPR applies when "personal data" is processed and depending on how personal data is defined, the effect of a valid encryption of this data might be different. The GDPR follows a "black/white approach", therefore the data can be either personal or not. This means that if the data has a personal reference, all data protection rules apply and if not, it is outside the GDPR's scope.[16]

However, whether or not encryption is the right measure to put in place depends on personal circumstances - the sort of processing someone is undertaking, the risks that might be posed to individuals' rights and freedoms, and the state of the art of technology available to someone to protect its own data. Concerning this, recital 83 of the UK GDPR affirms:

"In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of the implementation in relation to the risks and the nature of the personal data to be protected."[17]

Therefore, in order to keep data secured - meaning protecting them from losses, theft, or unauthorized access – encryption should be properly used. However, if encryption has not been used to protect data, there is a possibility that regulatory action might be pursued.

Thus, the GDPR's broad territorial scope leads towards a new awareness of data controllers (also established outside the EU) regarding their processing of personal data. Therefore, technologies that minimize the use of personal data – especially encryption – and which avoid the application of the GDPR become even more important.

4.2 Impact of different encryption techniques upon the GDPR's Material Scope

As shown in section 2, in the symmetric *cryptography* scenario, the encryption is performed by a secret-key, which both parties have access to. Hence, it is possible to derive that safe key management is a necessary condition to avoid the applicability of the GDPR. However, this can hardly be achieved when only using *symmetric cryptography*, because any holder of the key can easily re-identify the data subjects through decryption of the dataset.

Therefore, safe transportation might be achieved when encrypting the *symmetric* key with an *asymmetric* encryption technique, or hybrid cryptosystem. Thus, decryption in this scenario, when

[16] Forgo, N. (2015), International Data Privacy Law, p. 54 (59)

[17] EUR-Lex - 32016R0679 - EN - EUR-Lex. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

not asymmetrically encrypting the key, will be reasonably likely in most of the cases, and the data protection law would thus be applicable for the controller or processor of the symmetrically encrypted database.

Instead, in asymmetric cryptography, where two keys are used, the encryption key can be made public and there is no need to agree on a common secret by the parties in advance, as the recipient only knows the second secret-key. Thus, if the secret-key is held safely by the recipient, a third party, e.g. a cloud provider which stores or transports the encrypted data, does not have access to the private key and will not be able to decrypt the data - with reasonable efforts - and therefore does not fall under the scope of the GDPR. However, the controller always needs to monitor the technological development regarding the key used and possible innovative technological ways of decryption. Therefore, since *asymmetric* encryption has a significantly lower performance than *symmetric* encryption, in practice *hybrid* encryption is mostly used.

Conclusions

By means of my paper, I explained in depth the cryptographic techniques central to provide data security throughout the network. It is possible to conclude that these techniques are a good way of securing data as well as they are focal points to provide data protection in a system. However, I showed that the different types of cryptographic algorithms have to be implemented carefully and therefore it is important to choose the right algorithm, the right key size, and the right software within an organization. Also, it is highly relevant to keep the key secure in order to prevent brute force or other types of attacks.

Even though these techniques are mathematically strong to cyber-attacks, this is not enough. It is ultimately relevant to distinguish between symmetric and asymmetric key encryption to understand which of the two may provide stronger security. I have shown that symmetric encryption is an old technique, while asymmetric is the newer one, but it takes longer to execute this latter because it uses different types of keys for the encryption and the decryption processes. Therefore, on the one side, symmetric encryption is used when transmitting data in bulk, on the other side the asymmetric is more secure because of the use of different types of keys. Even though they have both pros and cons, asymmetric encryption definitely seems to be a better choice from a security perspective.

Finally, I explained that encryption serves as a technical and organizational measure to ensure the security of the processing in several parts of the Regulation. Concerning data protection and GDPR, I aimed to show that encrypting personal data can lead to the non-applicability of the GDPR and might thus be an important privacy preserving technology for controllers. The GDPR applies to personal data, and on the one side, this is a positive aspect for the European citizens, which are more

protected. On the other side, this is negative for organizations outside the EU, which will have to comply with a new and strict set of rules. Thus, there is still legal uncertainty regarding the applicability of the GDPR for encrypted data.

References

Berti, Hansche, Hare (2003). *Official (ISC)² Guide to the CISSP Exam*. Auerbach Publications. pp. 379. ISBN 0-8493-1707-X

Data privacy vs. data security [definitions and comparisons] – Data privacy manager. (2020). Retrieved from https://dataprivacymanager.net/security-vs-privacy/

Data security: Definition, explanation and guide. (2020). Retrieved from https://www.varonis.com/blog/data-security/

Defend against encrypted threats. (2019). Retrieved from https://www.f5.com/labs

Denning, D. E. (1982). *Cryptography and data security*. Addison Wesley Publishing Company.

Encryption. (2020). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/

Encryption-based cyberattacks are increasing: How to stay safe. (2018). Retrieved from https://www.arrayasolutions.com/encryption-based-cyber-attacks-are-increasing-how-to-stay-safe/

EUR-Lex - 32016R0679 - EN - EUR-Lex. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Forgo, N. (2015), International Data Privacy Law, p. 54 (59)

Home. (2020). Retrieved from https://ico.org.uk/

Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Review*, *25*(1), 84-88. doi:10.1016/j.clsr.2008.11.002

How should we implement encryption? (2020). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/how-should-we-implement-encryption/

Lek, K., & Rajapakse, N. (2012). *Cryptography: Protocols, design, and applications*. Nova Science Pub.

Lessig, L. (1999). Code and Other Laws of Cyberspace.

NETSCOUT. (2019). Network security infrastructure report. Retrieved from https://www.netscout.com/report/

Porcedda, M. G. (2012). Data protection and the prevention of cybercrime - The EU as an area of security? *SSRN Electronic Journal*. doi:10.2139/ssrn.2169340.

Reyad, O. (2018), "Cryptography and data Security: An introduction".

Rout, H. & Mishra, B.R., (2015). Pros and Cons of Cryptography, Steganography and Perturbation techniques. Journal of Electronics and Communication Engineering (IOSR-JECE).

Saleh M., Omara F., Aly A., (2016) "Data Security Using Cryptography and Steganography Techniques", International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6.

Spindler, G., & Schmechel, P. (2016). Personal Data and Encryption in the European General Data Protection Regulation, JIPITEC 163 para 1.

Stallings W., (2005) "Cryptography and Network Security Principles and Practices, Fourth Edition" Print ISBN-13: 978-0-13-187316-2.

Vollmer, N. (2020). Article 32 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy according to plan. Retrieved from https://www.privacy-regulation.eu/en/article-32-security-of-processing-GDPR.htm

What is encryption and how does it work? (2020). Retrieved from https://searchsecurity.techtarget.com/definition/encryption

Williams, E. (2020). Cryptography 101: Symmetric encryption. Retrieved from https://medium.com/@emilywilliams_43022/cryptography-101-symmetric-encryption-444aac6bb7a3