République Tunisienne
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Tunis El Manar
École Nationale d'Ingénieurs de Tunis

Information Technology and Communication Department

End of year project I

Cryptography uses in cybersecurity

Developed by :

Bouslama Marouane

Neifar Ahmed

Supervised By :

Mrs. Ben Slimane Maroua

Class : Computer science engineering 1st year 1

Academic year: 2021/2022

Acknowledgements

First of all, we would thank all the members of the jury for accepting to evaluate this work and to attend its presentation.

Our deep gratitude to our supervisor Mrs. Maroua Ben Slimane for her patience, and support in overcoming the many obstacles we encountered during the realization of the project, for her wise advice and for her valuable cooperation.
It was a great pleasure to work with her.

We would like to thank our colleagues for their cooperation and of course their friendship.

Finally, we would like to express our deepest gratitude for the affection and support shown to us by all the administrative staff and professors of ENIT.

We would also like to express our infinite thanks to our friends for accepting nothing less than excellence from us. Last but not least, we would like to thank our families.

Summary

The network revolution is becoming bigger and more complex and data need to be secured against cybercrimes.

Why are cyberattacks rising?
It is because they are cheaper, easier, and less risky than physical attacks. Due to the anonymous nature of the Internet, cybercriminals are difficult to identify and prosecute.

As part of the end-of-the-year project, we present the most important information about cybersecurity and cryptography, two complementary topics that ensure cyberspace security, we discuss the different algorithms of encryption and we propose a comparative analysis.

keywords : Cybersecurity, Cyberattacks, Cybercriminals, Cryptography, Encryption, Algorithm, Comparative analysis.

Contents

List of Figures

List of Tables

General Introduction

Our society, economy and critical infrastructure have become heavily dependent on computer networks and information technology solutions. As our reliance on information technology increases, cyberattacks become more attractive and potentially more catastrophic.
Cybercrimes caused billions of dollars in losses affecting the global economy with the intent of maliciously affecting critical and confidential information. With these crimes occurring on a daily basis, security in cyberspace has become an urgent response.

It is within this context that enters the subject of our end-of-the-year project. The first chapter introduces cybersecurity, its history, the common cyberthreats and domains, some good practices to avoid cyberattacks and the new challenges facing it.
The second chapter presents cryptography as a solution, its origin, the different techniques and algorithms of encryption, then a comparative analysis, limitations of basic algorithms and their evolution.

Chapter 1

Cybersecurity

Introduction

In this chapter, we introduce cybersecurity, also known as information technology (IT) security, which is the protection of Internet-connected systems, such as hardware, software and data, from cyber threats.
We give an overview of history then we provide the common cyberthreats and the primary domains of IT security.
Finally, we give solutions, practices to implement strong cybersecurity and some information about the new challenges facing information technology.

1.1 Rise of Cybersecurity

In this section, we present the key events and developments of cyber attacks and network security.

1.1.1 Birth of computer security

In **1971**, a developer working at Advanced Research Projects Agency Network named Bob Thomas, wrote the first computer worm. A program that prints "I'm a crawler; catch me if you can".
This was the first time a program transferred itself from one computer to another.[19]

Then in **1973**, Ray Tomlinson, a researcher in the same agency developed a program called Reaper, which finds and removes creeper virus on ARPANET computers.

1.1.2 From ARPANET to internet

In **1983** TCP/IP became the global standard for network communications and gave rise to the Internet.
In **1988**, the Internet started to be attacked when Robert Morris, a graduate student from Cornell University, released a dozen lines of code that constituted the first Internet worm. It replicated wildly, infecting and crashing about 60,000 computers connected to the internet and causing millions of dollars in damage. [19]

1.1.3 The Antivirus Industry Explodes

In **1990**, Microsoft experienced a huge increase in the PC market which leads to an increase in virus activity. The antivirus industry responded with products like McAfee, Norton Antivirus and Kaspersky

Lately in match **1999**, a virus called Melissa was distributed through Microsoft Outlook. which sends an email with the subject "Important Information" and an attachment called list.doc, as shown in figure 1.1. When opened, the virus disables the security features of Word and Outlook and mails itself to the top 50 people in the user's contact list. After a few days cybersecurity experts had contained the spread then removed the infections entirely thanks to antivirus.

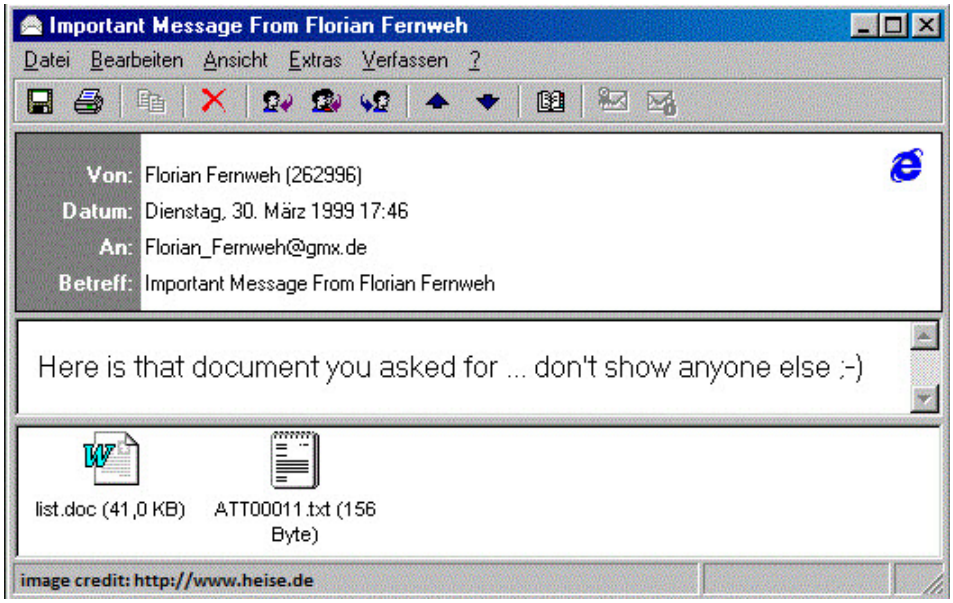


Figure 1.1: Email sended by infected computer
[19]

1.1.4 US Government recognizes cybersecurity

In the **2000's**, as a response to the increasing number of cyberattacks such as the spread of ILOVEYOU worm via an email with the subject "ILOVEYOU" and an attachment file called "LOVE-LETTER-FOR-YOU.txt.vbs" who sends a copy of itself to all addresses in the user's Outlook contacts and led to shutting down the Pentagon's and CIA's email systems, US Government created the first official U.S. government working group dedicated to cybersecurity.

1.1.5 The next generation

in the last few years, the use of cyberattacks has become too dangerous and scary. In **2010** a family of worms disrupted Iran's nuclear program to become the first Weponized malware program.

In addition to this, There is examples of a cyberattack used for espionage such as the largest data breach in history, when Yahoo suffered a breach that led to the theft of personal data from 3 billion users in **2013** and they didn't report the breach until 2016 !

Due to concerns about the security of personal data, the European Union began implementing in **2018**, the General Data Protection Regulation (GDPR) which establishes a mandatory data protection baseline.
[19]

1.2 Common cybersecurity threats

Just as physical security violations can occur in a variety of ways, with thieves climbing in through windows and shoplifters snatching items from store shelves, cybersecurity violations can too.
In this section, we will outline the most common types of cyberattacks.

1.2.1 Malware

A form of malicious software in which any file or program can be used to harm a computer user. This includes:

- **Virus:** A program that embeds itself into another software program. Once embedded, they make copies of themselves and insert these copies into other programs on the infected computer. When a user runs a virus-infected software, the

virus is activated, causing it to perform actions such as destroying or stealing data, recording the user's keystrokes, or rendering the device useless.

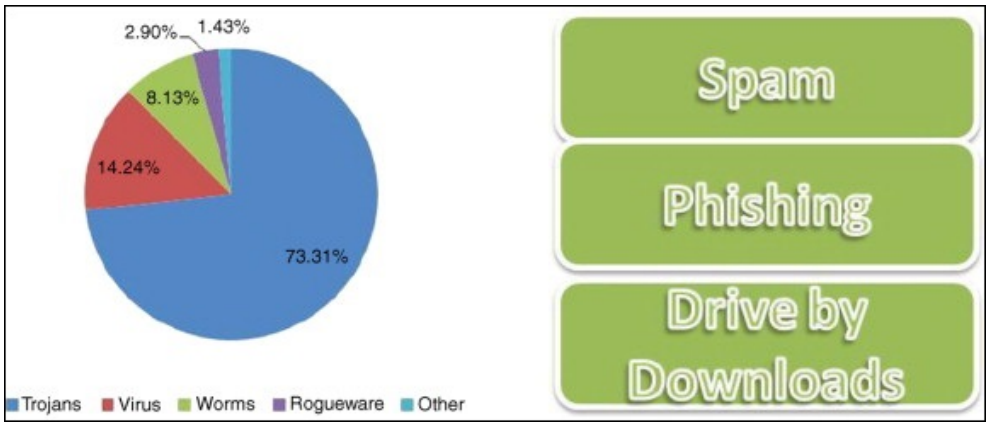
- **Worm:** Similar to a virus, but instead of setting up inside another software program, they install themselves in a completely separate location. For this reason, a worm does not require the user to activate it by using an infected program. Once a worm is installed on a machine's hard drive, it can replicate itself and send copies around the network at will.

- **Trojan:** It is a type of computer software that takes the form of regular software in disguise, such as utilities, games, and sometimes even antivirus programs. Once it runs on a computer, it causes problems such as killing background system processes, deleting hard disk data and corrupting the file distribution system.

- **Ransomware:** It involves the attacker locking the victim's computer system files, usually by encrypting them, and demanding payment to decrypt and unlock them.

- **Spyware:** A program that collects information about users and their browsing habits, sending the data to a remote user who can use this information for harmful purposes.
[8]

The figure 1.2 illustrates the percentages of different cyber threats.



[8]

Figure 1.2: Percentage of malicious software attacks

1.2.2 Social engineering

An attack that relies on human interaction to trick users into breaking security procedures to gain access to protected sensitive information.

The most common social engineering attack is phishing.
Phishing attacks are very common and involve fraudulent emails that are similar to emails from reputable sources. The goal is to steal sensitive data, such as credit card numbers and login information.
Phishing attacks can also be carried out through social networks and other online communities, through direct messages from other users, with a hidden agenda. Phishers often use social engineering and other public information sources to gather information about your work, interests and activities, giving the attacker an advantage in convincing you that they are not who they are.
Phishing attacks can also be carried out by phone (voice phishing) and text message (SMS phishing). [8]

1.2.3 Denial of service (DoS) attack

DoS attack is designed to shut down a machine or network, making it inaccessible to its users. a DoS attack is accomplished by flooding the target with traffic, or by sending messages that trigger a crash to legitimate users of services or resources they expect.

Web servers of high-profile organizations, such as banks, businesses, media companies, governments, and trade organizations are targeted by DoS attackers. Usually, it does not result in the theft of significant information or other assets, they can cost victims a significant amount of time and money to deal with.

A buffer overflow attack is the most common DoS attack. The concept is to send more traffic to a network address than the programmer has built the system to handle. [5]

1.2.4 Man-in-the-Middle (MitM) Attacks

It occurs when an attacker intercepts both sides of a transaction and inserts himself in the middle. As shown in Figure 1.3, a network attacker can steal and manipulate data by interrupting traffic. This type of attack typically exploits security vulnerabilities in the network, such as unsecured public WiFi, to insert itself between the visitor's device and the network.

The problem with this attack is that it is difficult to detect.
[16]

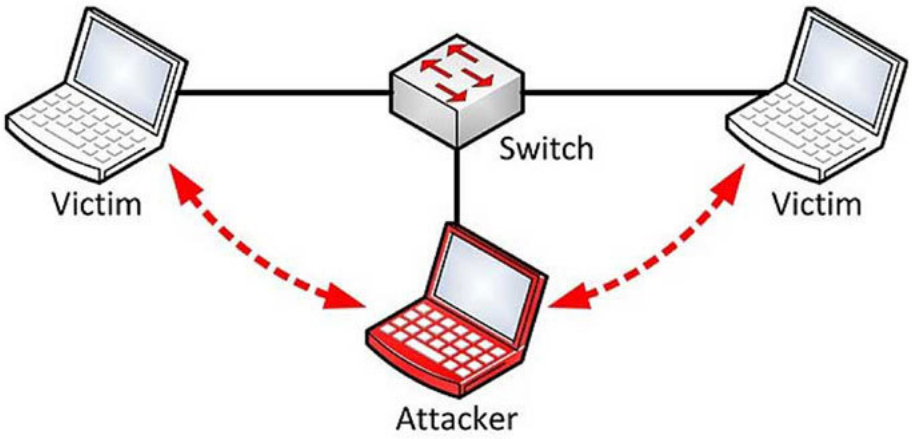


Figure 1.3: Man-in-the-Middle attacks
[16]

1.2.5 SQL Injection

SQL (Structured Language Query) injection is a cyberattack used to control and steal data from databases. Cybercriminals insert malicious code into databases through SQL allowing them to access confidential information in the database. SQL injection attacks can lead to unauthorized access to sensitive data such as passwords, credit card details or personal user information. Many high-profile data breaches in recent years have been caused by SQL injection attacks, resulting in reputational damage and regulatory fines.

In some cases, attackers can gain persistent backdoors into an organization's systems that can go unnoticed for a long time.

1.3 Cybersecurity domains

It should be obvious by now that wherever there is a computerized device or system, there may be hackers looking for ways to abuse or compromise it. In our increasingly information technology-saturated world, this means that cybersecurity countermeasures are all around us. In this section, we will cover the main areas where cybersecurity plays an important role.

1.3.1 Network security

Network security is the protection of data, devices and systems connected to the network for operation.
Network security protects these systems from malware/ransomware, network intrusions, etc., creating a secure platform for users, computers and programs to perform their functions in the IT environment.

As enterprises move to hybrid and multi-cloud environments, their data, applications and devices are being dispersed across locations and geographies. Users want to access enterprise systems and data from anywhere and on any device. As a result, traditional perimeter-based approaches to network security are being phased out.

1.3.2 Cloud security

Cloud security is a holistic bundle of technologies, protocols and best practices that protect the cloud computing environment, the applications running in the cloud and the data held in the cloud.
As enterprises continue to migrate to the cloud, most cloud providers follow best security practices and take proactive steps to protect the integrity of their servers. However, enterprises need to make their own considerations when it comes to protecting the data, applications and workloads running on the cloud.

1.3.3 Application security

Application security is a discipline of processes and tools designed to protect applications from threats throughout the application life cycle. Application security helps organizations protect the various applications used by internal and external customers, business partners and employees, such as legacy, desktop, web, mobile, etc.
Application security is important because today's applications can often be accessed over a variety of networks and connections to the cloud, increasing the vulnerability to security threats and vulnerabilities.

1.4 Cybersecurity solutions

The following practices and techniques can help implement strong cybersecurity, reduce vulnerability to cyberattacks, and protect critical information systems.

1.4.1 Firewalls

Firewalls control inbound and outbound network traffic to protect against untrusted networks and potentially malicious attacks.
A firewall is a set of protocols that specify what can and cannot enter your network, scan the sources of payloads and determine if those sources are trusted.
The main drawback of firewalls is that they can be circumvented if hackers send trusted payloads to avoid detection. Therefore, you should use an Intrusion Prevention System (IPS) along with a firewall.
IPS is a solution designed to identify malicious network activity. IPS uses "anomaly-based detection" to look for patterns in data, applications, IP addresses, and network packets that may suggest an intrusion. [7]

The figure 1.4 shows that firewall secure transactions between subnets.

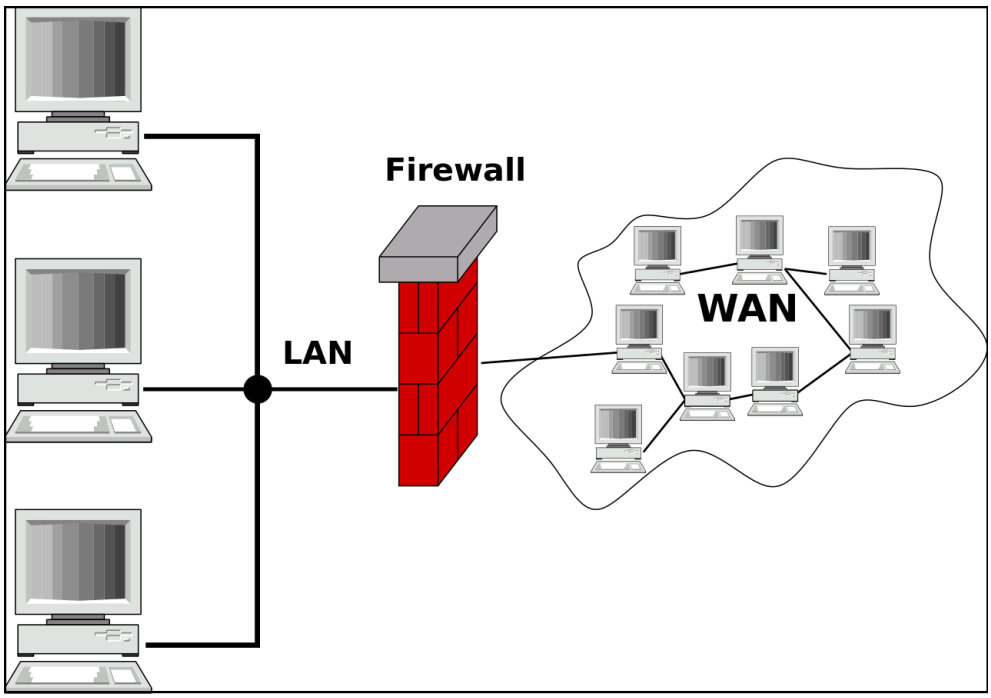


Figure 1.4: Firewall operation
[15]

1.4.2 Access Control

Controlling access to information is important so that the organization can maintain the confidentiality, integrity and availability of that information. Access

control prevents unauthorized users from retrieving, using or tampering with information.
The main steps in controlling user access to information are :

- **Identification:** is the process of assigning each user and system their own unique name.
- **Authentication:** is the process of validating the user's identity. There are three primary methods to authenticate users. These methods are based on:
Something a user knows like PIN, password, phrase, or passcode.
Something a user has like a smart card, ATM card, or token.
Something a user is like a retina scan, fingerprint, or voice scan

Identification and authentication are usually done through the use of a username and password respectively.
[12]
- **Authorization:** A user's access rights, like what he or she can or cannot do in an application or system. For example, an authorization may restrict one user to only having access to view data, while another user may have access to view and change data. Authorization should be based on the minimum necessary access that a user needs to do his or her job.
[20]

1.4.3 Antimalware

Anti-malware software is designed to detect known viruses and other malwares that may have a harmful effect on users or devices.

Anti-malware programs provide a way to protect against known threats. The effectiveness of an anti-virus program depends heavily on how often it is updated. Most anti-virus programs rely on a library or database of known viruses, which they use to compare with the programs on the user's device. If a match is found, the malicious program is removed or placed in quarantine, and the user can decide to recover from it or remove the program manually.

Malware removal software has many benefits, especially keeping your computer safe. But that's not all there is to anti-malware, you can benefit from it in many ways.
- Protection from hackers: Hackers get into your computer through malware. With anti-malware software installed, you can browse the web safely.
- Privacy protection: Cybercriminals use your personal information to their advantage. Anti-malware software prevents the installation of any software that steals

personal information.
- Free up junk in your computer: If junk is consuming your computer's memory, anti-malware will notify you so you can free up some space. This eliminates the useless files stored on your computer.

One limitation of traditional antimalware software is that they only provide protection against known threats. Therefore, if someone cooks up a new malicious code, the anti-malware program may not be able to detect it when scanning.

1.4.4 Data loss prevention (DLP)

The term DLP refers to Data Loss and Data Breach Prevention for defense organizations. It is a set of tools and processes to ensure that sensitive data is not lost, misused or accessed by unauthorized users. DLP software classifies regulated, confidential and business-critical data and identifies violations of organization-defined policies or within predefined policy packages, often driven by regulatory compliance. Once these violations are identified, DLP enforces remediation through alerts, encryption and other protections to prevent end-users from accidentally or maliciously sharing data that could put the organization at risk.
File security solutions, such as Firewalls, are an important part of DLP's strategy. Such solutions protect data at rest, in motion and in use, and detect file-based data leakage. [3]

1.4.5 Encryption

Encryption attempts to make the information unreadable to people who are not explicitly authorized to view that data. People or devices can be authorized to access encrypted data in a variety of ways, but usually this access is granted through a password or decryption key. There are various strengths and methods of encryption, and as technology evolves, older encryption methods are no longer considered secure. Sensitive information should be encrypted using the best available methods whenever possible.

Data can be encrypted in several ways:

- **Virtual Private Network (VPN):** is software that protects a user's identity by encrypting their data and masking their IP address and location. When someone uses a VPN, they are no longer connected directly to the Internet, but to a secure server that then connects to the Internet on their behalf. VPNs are often used in businesses and are increasingly necessary for individuals, especially those using

public wifi at cafes or airports.

- **Data storage:** Data saved on storage media such as hard drives or phones can often be encrypted to prevent unauthorized access in the event of data loss or theft. Encryption can be applied to entire disks or to individual files and folders. Usually, this protection is accomplished with full-disk encryption software such as Microsoft's Bitlocker for Windows or Apple's FileVault for MacOS.

- **Encrypted communication:** An example of encrypted communication is accessing a website encrypted with a Transport Layer Security (TLS) session. The URL of these sites will start with https:// and most browsers will display a lock in the address bar to indicate that the session has been encrypted. The information transmitted between you and the secure site will only be visible to you and the destination you are connecting to.
[14]

1.5 Latest Cybersecurity issues

Cybersecurity is constantly challenged by hackers, data loss, privacy, risk management, and changes in a cybersecurity strategy.
One of the most problematic elements of cybersecurity is the constant change in security risk. As new technologies emerge and technologies are used in new or different ways, new avenues of attack are developed.
In this section, we present some of the new technologies that pose a challenge to cybersecurity and make the job more difficult.

1.5.1 Internet of Things (IoT) attacks

The Internet of Things or IoT is the most vulnerable to data security threats. Every digital, mechanical, and computing smart device that can transmit data over an Internet network is known as the IoT, such as laptops, cell phones, routers, webcams, cars, and even home security systems.
To access personal devices that contain your sensitive information, hackers use devices around you such as wearable smart watches, baby monitors, smart refrigerators or smart lights.
Today, the IoT industry is a prime target for attackers to compromise sensitive user information. By 2022, approximately 12 billion devices will be online, however, more connected devices mean greater risk, making IoT networks more vulnerable to cyber intrusions and infections. This in turn will open a wide space for hackers

to compromise data security and use it for malicious purposes.
[1]

The figure 1.5 shows the great growth of the Internet of Things industry.

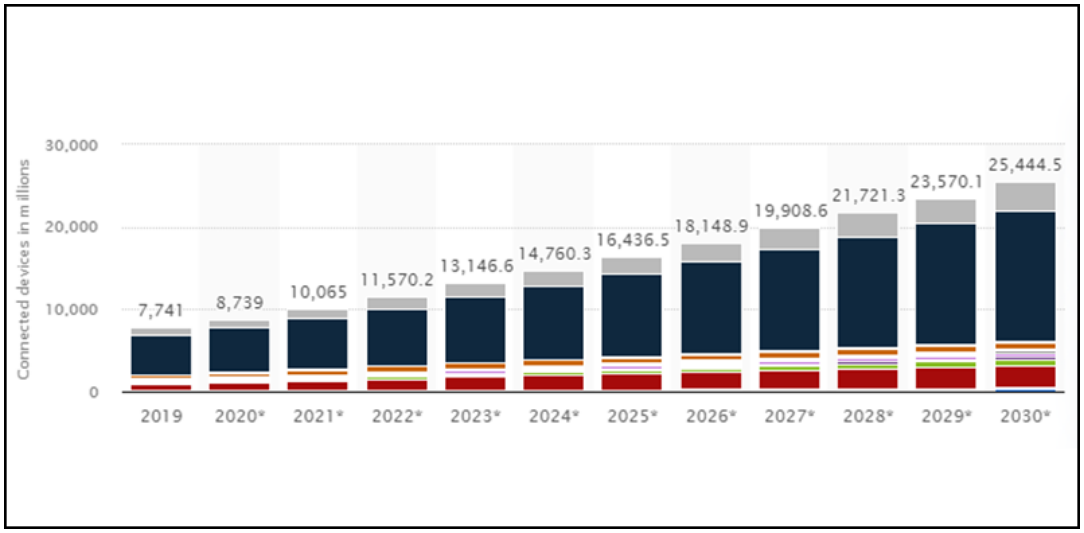


Figure 1.5: Number of IoT connected devices worldwide
[21]

1.5.2 Machine learning and artificial intelligence attacks

A bot(robot) is a type of software that runs simple programs on the Internet, such as "crawling" websites at a much faster rate than humans to obtain and analyze predetermined types of information. Because bots do what they are told and operate autonomously, they make excellent tools for hackers, especially when you string them together into a temporary collective called a botnet. Hackers have also started using artificial intelligence (AI) in their attacks. Artificial intelligence refers to a computer system that interprets external data, learns from it, and uses what it learns to perform tasks and achieve goals. Artificial intelligence is useful for hackers deploying botnets because, in the past, humans have always had to perform certain functions when launching attacks to distribute bot code to target machines. Humans also had to monitor the attack to assess its effectiveness. Artificial intelligence changes this equation by taking humans out of the equation; it allows hackers to launch more attacks more frequently and makes them more effective because AI can detect successful defenses and react faster than humans. [18]

Conclusion

In this first chapter, we have talked about the history and the beginnings of cybersecurity, the different types of cyber threats that can be encountered frequently, the primary domains where cybersecurity plays an important role, then we have given some practices and solutions to implement strong IT security.
Finally, we have presented some new challenges facing cybersecurity such as the arrival of the internet of things and artificial intelligence.
In the next chapter, we will focus on encryption which is a good practice to secure data and plays an important role in cybersecurity.

Chapter 2

Cryptography

Introduction

Cryptography is a method of utilizing complex mathematical principles in storing and exchanging data in a particular form so that only those concerned with the data can read and process it. In this chapter, we will introduce the most common algorithms of cryptography, compare their performance, differentiate the various cryptographic threats which lead us to the limitations of the basic algorithms and specify how they evolved to be used nowadays.

2.1 Origin of cryptography and its evolution

In its early days, cryptography was primarily means converting messages into unreadable groups of numbers in order to protect the content of the message as it was transmitted from one person to another. In modern times, cryptography has evolved from basic message confidentiality to a number of stages that include message integrity checking, sender/receiver authentication, and digital signatures (New World, 2007)[2]. As cryptography became more and more complex and diverse special traits and categories were created where most algorithms fits in, in the following section we will list the most important types of cryptography techniques.

2.2 Different techniques of encryption

Cryptography plays an important role in ensuring secure communication between multiple entities. In many contemporary studies, researchers have contributed to determining the best cryptographic mechanism in terms of its performance results.

The selection of cryptographic techniques based on a particular environment is a big question. To answer this question, many existing studies claim that the choice of technology depends entirely on the desired qualitative attributes, such as efficiency and security. There are various types of encryption but as presented in the figure 2.1 most researches focus mainly on the algorithms of two types which are symmetric and asymmetric encryption .[4]

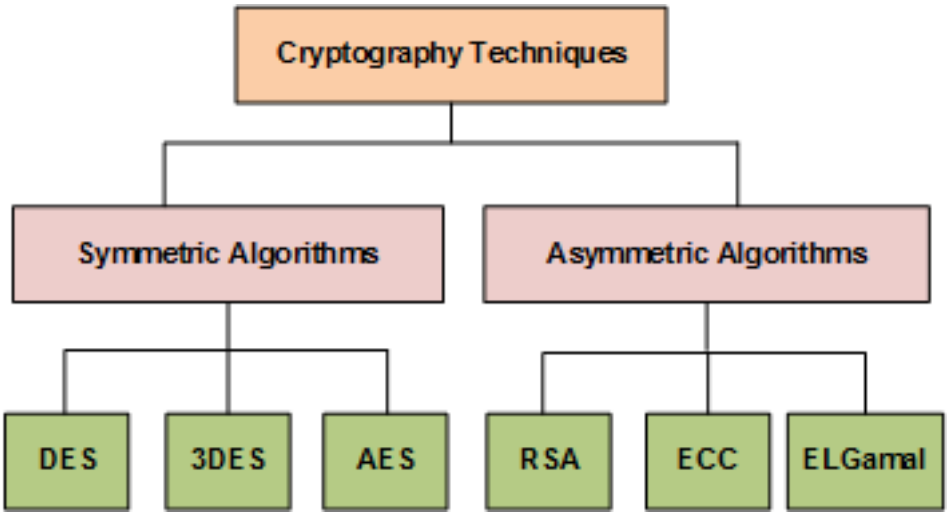


Figure 2.1: Taxonomy of cryptography techniques [4]

2.3 Symmetric encryption

In symmetric cryptography, We use the same key for both encryption and decryption as illustrated in the figure 2.2. Thus the key's exchange must be completed before sending the message. Keys are very important in symmetric cryptography because their security depends mainly on the length of the key . There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6 and BLOWFISH. [13]. In the rest of this section, we present the details of the different algorithms of symmetric encryption.

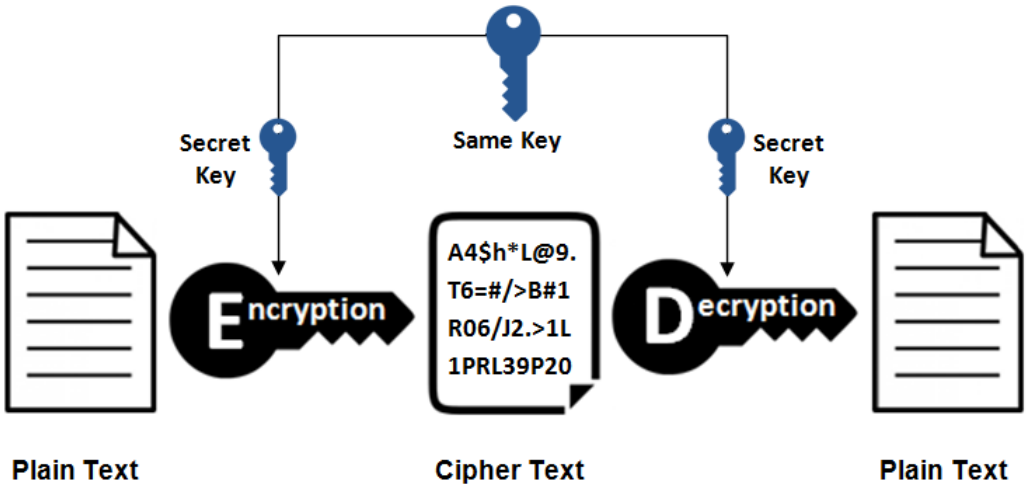


Figure 2.2: Symmetric encryption [17]

2.3.1 DES

DES (Data Encryption Standard) is an acronym for Data Encryption Standard. Encryption Standard. DES was introduced in the early 1970's at IBM. the early design of DES was based on Horst Feistel.DES is a symmetric encryption algorithm for encrypting and decrypting messages . In DES, only one secret key is used for encryption and decryption. the key size of DES is 56 bits. In order that encryption/decryption to take place, the sender and receiver must have the same key.DES encrypts a 64-bit block on a 64-bit block. The DES algorithm is one of the most widely used in many applications . It is widely used in the security of military, commercial and communication systems , 3DES encryption uses the same algorithm as DES but has a different key size (168 bits) The 3DES algorithm performs three operations on each block of data. Three operations are performed per data block. It is slower than DES .[4]

2.3.2 AES

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic (Federal Information Processing Standards) algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in

blocks of 128 bits. [9] It was introduced in 1997 by the NIST (National Institute of Standards and Technology). AES algorithm is used in small devices for encrypting a message to send over a network. Some other applications are monetary transactions and security applications.[4]
In the next section, we will present asymmetric encryption and its most prominent algorithms.

2.4 Asymmetric encryption

Asymmetric encryption, also known as public-key cryptography, is a relatively new method compared to symmetric encryption. Asymmetric encryption uses two different keys to encrypt a plain text as illustrated in the figure 2.3. The secret keys are exchanged over the Internet or large networks. It ensures that a malicious person does not take advantage of the key. It is worth noting that anyone with the secret key can decrypt the message, which is why asymmetric encryption uses two related keys to fortify security. A public key is openly available to anyone who wants to send a message. The second private key is hidden so that only the receiver knows about it.[17]. There are various symmetric key algorithms such as RSA, ElGamal, ECC, DSA and Diffie-Hellman.

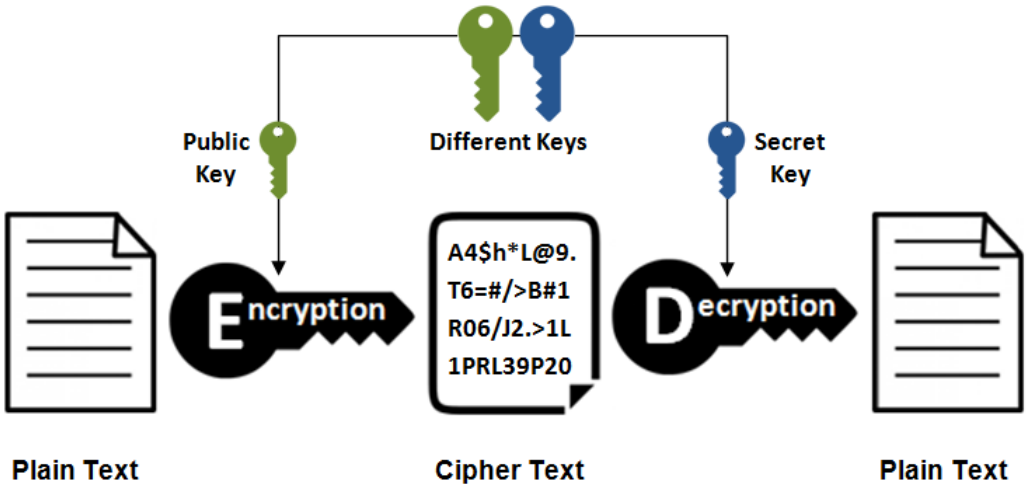


Figure 2.3: Asymmetric Encryption[17]

2.4.1 RSA

RSA stands for Rivest, Shamir and Adleman, who introduced the RSA algorithm in 1977. RSA is an asymmetric encryption algorithm that is also used for encrypting and decrypting messages. RSA is widely used to transmit keys over insecure channels. Due to the asymmetric nature, two keys are used in the algorithm. One is the public key and the second is the private key. The public key is public to everyone in the cryptosystem, while the private key is kept secret by the authorized person. RSA provides confidentiality, integrity, authenticity and non-repudiation of data. RSA is more commonly used in the electronics industry for online fund transfers. [4]

2.4.2 ElGamal

ElGamal: The ElGamal algorithm was proposed by Taher ElGamal in 1985. Proposed by Taher ElGamal, ElGamal is an asymmetric key encryption algorithm based on Diffie-Helman as an alternative to the public key RSA. ElGamal is also used in a digital signature generation algorithm called the ElGamal signature scheme. . A homomorphic algorithm called Paillier is used for its semantic security. [4]

2.4.3 ECC

ECC (Elliptic Curve Cryptography). ECC stands for Elliptic Curve Cryptography. ECC was proposed by Neal Koblitz and Victor S. Miller in 1985. ECC belongs to the category of the elliptic curve-based asymmetric schemes. applications of ECC are encryption, digital signatures and pseudo-random generators. [4]

2.5 A comparative analysis

In this section, we propose a comparative analysis of symmetric and asymmetric cryptography algorithms and their performance based on obtained researches results in [4] by using parameters such as key generation time and encryption time/decryption time. Symmetric algorithms include DES and AES, while asymmetric algorithms include RSA and ElGamal.

2.5.1 Key generation

The key generation time is the time it takes for the key generation function to generate the key. All these functions generate different times depending on the size of the text file and the length of the key in any algorithm.

The table 2.1 shows that DES with the smallest key size (56 bits) has the shortest key generation time (29ms) and as the key size gets bigger, (AES with a key size of 128 bits) key generation time increases (AES key generation time 75ms) and the algorithm with the biggest key size (RSA with 1024 bits) have the longest key generation time (287ms).
We can conclude that the key generation time increases as the key size gets bigger. We notice that due to their small key size symmetric algorithms have a smaller key generation time.

Cryptography Algorithms		Key Size (bits)	Generation Time (milliseconds)
Symmetric	DES	56	29 ms
	AES	128	75 ms
Asymmetric	RSA	1024	287 ms
	ElGamal	160	86 ms

Table 2.1: Key generation[4]

2.5.2 Encryption time/Decryption time

Encryption time is the time it takes for any encryption function to convert plain text into ciphertext. Decryption time is the time taken to convert the ciphertext to plain text again. Encryption and decryption times are shown for symmetric and asymmetric algorithms for different file sizes. [4]

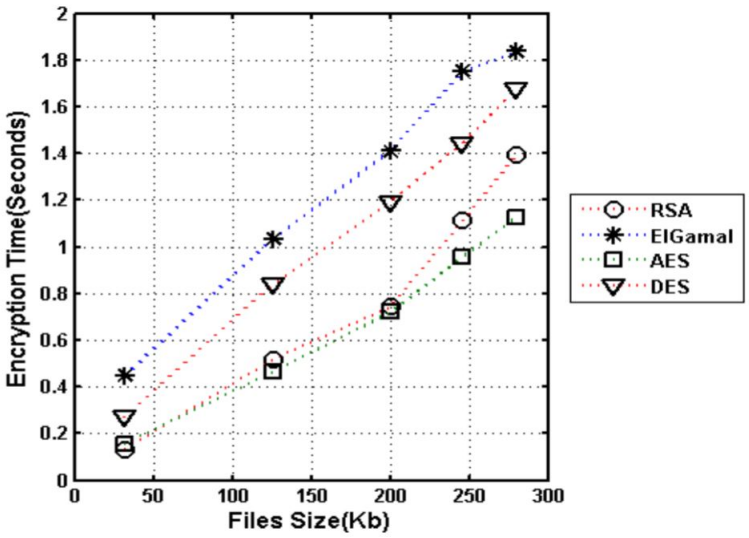


Figure 2.4: Encryption time[4]

The performance results in the table 2.2 clearly show the logical result that if we increase the size of the text file, the encryption and decryption time also Increase. Encryption and decryption times are tightly related, so to make a comparison between algorithms we are going to focus on the encryption time and we will take for reference a file size of 280 Kilo Bytes.
As shown in the table 2.1 and Despite having the smallest key size, DES ,as presented in the table 2.2 does not have the shortest encryption time (1.67 sec) but falls behind AES (1.12 sec) and RSA(1.39 sec).
In addition the type of encryption (Symmetric or Asymmetric) does not affect data encryption time as we can see in the results in the table 2.2 RSA (asymmetric (1.39 sec)) is faster than DES (Symmetric(1.67 sec)) and DES is faster than ElGamal (asymmetric(1.83 sec))
As illustrated in the graph presented in the figure 2.4 This analysis and results stay valid if we change the size of the data encrypted.
We conclude that the compute of encryption time is proportional to the nature of the algorithm.
The time difference might seem negligible (on the scale of an ms) but when projected on huge data (for example in a data center with massive hard drives storage sizes) or in a real-time secure communication where time latency should be minimal those number and the choice of the proper algorithm make a difference.

Cryptography Algorithms	File size (Kilo Bytes)	Encryption Time (seconds)	Decryption Time (seconds)
DES	32	0.27	0.44
	126	0.83	0.65
	200	1.19	0.85
	246	1.44	1.23
	280	1.67	1.45
AES	32	0.15	0.15
	126	0.46	0.44
	200	0.72	0.63
	246	0.95	0.83
	280	1.12	1.10
RSA	32	0.13	0.15
	126	0.52	0.43
	200	0.74	0.66
	246	1.11	0.93
	280	1.39	1.23
Elgamal	32	0.45	0.43
	126	1.03	0.85
	200	1.41	1.13
	246	1.75	1.30
	280	1.83	1.64

Table 2.2: Encryption time/Decryption time[4]

2.6 Cryptography-Based Cyber-Attacks

Cryptography-based cyber attacks can be defined as an attack that focuses primarily on cryptography-related crime, divided into four key groups ransomware,

cryptojacking, coin thieves and illegal money transfers . Meanwhile, dirty cryptocurrencies are investigated in these categories as a medium of exchange for cybercrime. [6]

2.6.1 Ransomware

Ransomware is a type of malware that uses encryption technology to blackmail victims into paying money for their information. A hacker gets access to a person or organization's critical data and then encrypts it, making them unable to access their files, databases or software. A ransom is then demanded to decrypt their data. Ransomware is a type of virus often designed to spread across networks and target important databases and server files, so it can quickly cripple entire organizations. It is a growing threat, resulting in billions of dollars in payments to cybercriminals and massive losses and high costs to businesses and government organizations. [22] Ransomware has gradually risen year after year since 2013 and peaked in 2016, with 1,271 detections per day in 2016. Secondly, ransomware can be classified according to three criteria - the target of the cyberattack, the technology of the cyber attack and the level of damage.[6]

2.6.2 Cryptojacking

Cryptocurrency hijacking has many interchangeable names such as coin mining, coin miner. crypto miner, and cryptocurrency miner. it employs two techniques - file-based cryptojacking (by downloading and running malicious files on any device, such as computers, servers, and networks) and browser-based cryptojacking or stowaway mining (by embedding malicious code for mining in any attacked website) [6]

2.6.3 Coin thieves

The coin thieves are carried out by malware and crimeware as a service (CaaS). Two examples of coin theft The malware is OSX.Stealbit.A and OSX.Stealbit.B. They are both two Trojans designed to open backdoors and steal credentials from major bitcoin sites by capturing the victim's login information.[6]

2.6.4 Illegal money transfers

The price of money transfer services for stolen funds in 2018 was the same as in 2016, as a percentage of the total amount.10 For example, $100 of bitcoin for 1{,}000$ of cash (Symantec 2017, 2019). In addition, Bytecoin, Verge, Zcash, Zcoin, Monero, MoneroC, Monero Gold, MoneroV, Monero-Classic, Monero 0, are examples of

privacy-based cryptocurrencies. Privacy-based cryptocurrencies are used for money laundering.[6]

2.7 Techniques of cryptography in CyberSecurity

2.7.1 Limitations

DES used to be a major symmetric key algorithm (Standard. 2018).DES worked on equal block sizes and used both algorithms for confusion and diffusion. However, due to its small key length, DES was considered insecure. In 1999, the Electronic Frontier Foundation worked with distributed.net to exploit the DES key in less than 24 hours. using a brute force attack to crack the DES key in less than 24 hours . There are various other attacks that can crack DES with less time complexity than brute force. As a result, triple DES is extended to decryption-encryption (EDE) mode, so the size of the key is 168 bits (Bhanot and Hans, 2015). However, a new attack has been introduced, the meet-in-the-middle attack, which challenges 3DES. The middle attack, challenged 3DES.
As a result, in 2001, NIST (Diehl and Laws, 2016) announced and chose a new cipher, AES. invented by Rijmen and Daemen.AES is applicable to different lengths of keys 128, 192 and 256 bits. The higher the number of bits of the key, the more secure the transmission. the more secure the transmission. Although there are many attacks on AES (recovery attacks and side-channel attacks), it has not been breached so far. Despite the many attacks on AES (recovery attacks and side-channel attacks), it has so far not been breached and is considered secure. Blowfish (Bhanot and Hans, 2015; Schneier. 1993) was designed by Bruce Schneier and has a key length between 32 bits and up to 448 bits, with a block size of 64 bits. This algorithm is vulnerable to birthday attacks due to its block size. [10]

2.7.2 Research

Chowhan and Jaju (2015) introduced an improved RSA public key encryption algorithm and performed a comparison based on security and time complexity by manipulating data of different sizes. According to the authors, the algorithm works as follows with three prime numbers and two other constraints to make the system more stable. The algorithm becomes more efficient as the security level and the speed of key generation increase. However, the results of the study show that RSA is still better in terms of the speed of encrypting and decrypting text and the overall execution time.[10]

Thangarasu and Selvakumar (2018) propose an enhanced cryptography technique on sensor-cloud architectures for securing session keys between hosts while leveraging reliable services. To enhance the authentication of sensor nodes in the network, the technique uses a modified elliptic curve cryptography (ECC) algorithm and removes the complexity associated with finding intruders in Abelian groups' network theory.[10]

Katz and Vaikuntanathan (2013) describe a system for building cryptography-based protocols that authorize clients to restart vulnerable shared keys as cryptographic keys and authenticated key exchange protocols, enabling parties to securely share secret keys over uncertain networks. This new system is handled by clients sending messages to each other simultaneously. To make the key exchange protocol protected, the protocol applies a hash function and a secure encryption scheme (Gen, Enc, Dec).[10]

Wang et Al. (2018) introduce a new quantum algorithm to break the RSA cryptosystem in polynomial time by computing the order g of the RSA public key (x, s = pq) 2 Mxg M(mod s) using the quantum inverse Fourier transform and phase estimation. This is because, when g is found, the plaintext P of RSA can be easily obtained by computing P Mxg-1(mod s). Thus, an attack is proposed that only targets the ciphertext, while Ariffin et al. (2014) propose an attack on RSA in which the decryption indices p1 and p2 share their most significant bits, related to prime numbers x and y, which share their least significant bit of information. The scheme is presented in such a way that the RSA is made insecure by improving the previous bounds of the attack.[10]

Marzan and Sison proposed an algorithm to handle plaintexts containing letters, numbers and special characters. This study improves the Playfair cipher through a key encryption and decryption process which will guide the difficulty of key security without negotiating its runtime operation. The runtime performance of this system exceeds that of the encryption and decryption methods in the study by Amalia et al. Again, in this technique, the key security algorithm demonstrates a powerful avalanche effect. Limitations in adaptability are the weakness of the Pryfel cipher. By eliminating the letter j from the ciphertext, it eradicates uncertainty and makes

the cipher text vulnerable to frequent attacks. attacks. Therefore, the Playfair cipher algorithm should be made into a 5x19 key matrix that can accommodate 95 characters of any type. By modifying the Playfair cipher to a 5x19 matrix, its weaknesses can be overcome and strong encryption can be achieved.[11]

2.7.3 Algorithms development

We list the commonly used security standards and their advantages and disadvantages. Recently, cyber security has reached a new level of being translated into the primacy of digital business. However, a number of new methods and tools are being introduced in line with the rate of digital growth and, on the other hand, hackers are trying out new tools and techniques to challenge the security framework. As a result, many other efforts have arisen. This paper reviews the new developments in security standards for symmetric and asymmetric algorithms developed by different researchers over time with the help of new algorithms, procedures and frameworks.[10]

Basic algorithms

RSA starts with a one-way function and a factorization problem. Unfortunately, instead of using one-way functions to protect data, the researchers used prime numbers and developed an improved RSA algorithm to solve the factorization problem with the help of cyclic integers. The authors also propose techniques to merge DES and RSA in order to achieve good confidentiality and minimal overhead. Similarly, all other recent advances in RSA algorithms are described in detail and various key management schemes and their advantages and disadvantages are fully discussed in this paper. In addition, the symmetric encryption standard uses XOR as its main feature to transfer bits to classical and dangerous channels. [10]

New Approach

Recently, another interesting cryptographic technique is being prominently developed, called quantum cryptography based on the laws of physics. This technique uses Qubits to provide more secure new algorithms where cryptanalysis is not an easy task for Qubits. Quantum computers present challenges and produce disruptive results against classical asymmetric encryption algorithms. Side-channel attack algorithms include RSA, ECC, ElGamal, as well as symmetric encryption algorithms such as DES, Ericsson, etc. for many years, A great deal of research is being done in quantum computing, and quantum computers can completely break

existing standards when they come into real-time implementation. In addition, Hardware implementations of security algorithms are being developed by various researchers along with software implementations to achieve the goals of speed, complexity and correctness, but researchers need to be careful to avoid side-channel attacks that contain timing attacks, caching attacks, scan-based attacks, faults and differential-based attacks. There are many practical experiments that can break AES and RSA through timing attacks, while symmetric ciphers are vulnerable to scan-based attacks.[10]

Conclusion

We have presented the different encryption algorithms and we have compared their performances. We have also enumerated the advantages and the disadvantages of each algorithm. In addition, we have given an overview about their security development to be used nowadays safely and certainly.

General Conclusion

In this report, we mainly presented the complementarity between cybersecurity which is the protection of hardware, software and data connected to the internet and that by using cryptography to make the data circulating on the web encrypted in a secret way to deny access to any person wishing to miss-use it. This interconnection provides security and minimizes the many dangers faced while surfing the internet.

This report has been an overview of those two important subjects that are constantly evolving to ensure our data security, defined and explained their most notable characteristics and how they can be effective against the presented common threats, starting from the most simple solutions, comparing them and having an in-depth analysis of their advantages and disadvantages and how each method evolved to be more efficient.

Bibliography and netography

[1] Aishah Abdullah et al. "CyberSecurity: a review of internet of things (IoT) security issues, challenges and techniques". In: *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE. 2019, pp. 1–6.

[2] Tony M. Damico. *A Brief History of Cryptography*. `http://www.inquiriesjournal.com/articles/1698/a-brief-history-of-cryptography`. Last accessed 2 April 2022. 2009.

[3] *Data Loss Prevention*. `https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/`.

[4] Muhammad Ahmed Faiqa Maqsood. "Cryptography: A Comparative Analysis for Modern Techniques". In: *International Journal of Advanced Computer Science and Applications* 8.6 (2017), pp. 442–448.

[5] JAKE FRANKENFIELD. *A Brief History of Cryptography*. `https://www.investopedia.com/terms/d/denial-service-attack-dos.asptoc-distributed-denial-of-service-ddos-attack`. 2022.

[6] Srirath Gohwong. "The State of the Art of Cryptography-Based Cyber-Attacks". In: *International Journal of Crime, Law and Social Issues* (2019).

[7] Saeed Al-Haj and Ehab Al-Shaer. "Measuring firewall security". In: *2011 4th Symposium on Configuration Analytics and Automation (SAFECONFIG)*. IEEE. 2011, pp. 1–4.

[8] Mamoona Humayun et al. "Cyber security threats and vulnerabilities: a systematic mapping study". In: *Arabian Journal for Science and Engineering* 45.4 (2020), pp. 3171–3189.

[9] Federal Information. "ADVANCED ENCRYPTION STANDARD". In: *Processing Standards Publication 197* (2001), pp. 1–51.

[10] R. Ramkumar Jagpreet KaurK. "The recent trends in cyber security: A review". In: *Journal of King Saud University* (2021).

[11] Kshiteesh R Bharadwaj Kshiteesh R Bharadwaj. “A Review on Challenges and Latest Trends on Cyber Security Using Text Cryptography”. In: *Atlantis Highlights in Computer Sciences* (2021).

[12] Nilesh A Lal, Salendra Prasad, and Mohammed Farik. “A review of authentication methods”. In: *vol* 5 (2016), pp. 246–249.

[13] Pradeep Mishra Monika Agrawal. “A Comparative Survey on Symmetric Key Encryption Techniques”. In: *International Journal of Advanced Computer Science and Applications* 4.6 (2012), pp. 877–882.

[14] Hamid R Nemati and Li Yang. *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering: Information Encryption and Cyphering*. IGI Global, 2010.

[15] Les Olson. *What is Firewall ? How You Can Protect Your Sensitive Computer Data Using Software or Hardware Firewalls*. `https://ksltv.com/403051/what-is-a-firewall/`. 2020.

[16] Dipnarayan Das Sumit Gupta. “Some potential remedial measures to counter popular cyber attacks”. In: *International journal of innovative knowledge concepts* 7.1 (2019), pp. 143–149.

[17] *Symmetric vs. Asymmetric Encryption – What are differences?* `https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences`. Last accessed 8 April 2022.

[18] Mariarosaria Taddeo. “Three ethical challenges of applications of artificial intelligence in cybersecurity”. In: *Minds and Machines* 29.2 (2019), pp. 187–191.

[19] *The Digital Arms Race between Black-Hat and White-Hat Hackers*. `https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/`.

[20] Dobromir Todorov. *Mechanics of user identification and authentication: Fundamentals of identity management*. Auerbach Publications, 2007.

[21] Lionel Sujay Vailshery. *Number of IoT connected devices worldwide 2019-2030, by vertical*. 2022.

[22] *What Is Ransomware?* `https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware.html?fbclid=IwAR2gZzDePbrdm3-7dEGEBePpr0Xcc4BZ6RX1By51dCfNl6Mssr3CVsL3xa8`. 2020.