

**Assessment 1**

**Cybersecurity audit report & Cryptanalysis**

Author: Bertocco Thomas-Killian - #13758322

Lecturer: Sithira Vadivel

CP5603 Advanced E-Security | SP52 | 2019

13 September 2019

Table of Contents

[Introduction 4](#_Toc19283106)

[Security report 5](#_Toc19283107)

[[22/07/2019] IIS servers (internet): Distributed Denial of service 5](#_Toc19283108)

[Description of the attack 5](#_Toc19283109)

[Definition of the attack 5](#_Toc19283110)

[[05/08/2019] SQL server: SQL injection 7](#_Toc19283111)

[Description of the attack 7](#_Toc19283112)

[Definition of the attack 7](#_Toc19283113)

[Strategy of the attackers 7](#_Toc19283114)

[[16/08/2019] Internal network: Man in the middle 9](#_Toc19283115)

[Description of the attack 9](#_Toc19283116)

[Definition of the attack 9](#_Toc19283117)

[Strategy of the attackers 9](#_Toc19283118)

[[27/09/2019] Authentication server : Brute forcing 11](#_Toc19283119)

[Description of the attack 11](#_Toc19283120)

[Definition of the attack 11](#_Toc19283121)

[Strategy of the attackers 11](#_Toc19283122)

[Controls and countermeasures 12](#_Toc19283123)

[MySQL injection 12](#_Toc19283124)

[Filter user input in the application 12](#_Toc19283125)

[Secure web server to filter URL 12](#_Toc19283126)

[Distributed Denial of Service 12](#_Toc19283127)

[Use of a Content Delivery Network (CDN) 12](#_Toc19283128)

[Redirection via DNS protocol 13](#_Toc19283129)

[Use a firewall 13](#_Toc19283130)

[Man in the Middle (Arp poisoning) 13](#_Toc19283131)

[End-to-end encryption 13](#_Toc19283132)

[Use a packet filter 13](#_Toc19283133)

[Static ARP entries 13](#_Toc19283134)

[Brute Force 14](#_Toc19283135)

[Strict password policy 14](#_Toc19283136)

[Captcha verification 14](#_Toc19283137)

[Security recommendations 15](#_Toc19283138)

[Establish a minimum level of security throughout the entire IT infrastructure 15](#_Toc19283139)

[Ensure the security of Wi-Fi access networks and the separation of uses 15](#_Toc19283140)

[Control and protect access to server rooms and technical rooms 16](#_Toc19283141)

[Protect e-mail boxes 16](#_Toc19283142)

[Segment the network and set up a partitioning between these areas 17](#_Toc19283143)

[Encrypt sensitive data transmitted over the Internet 17](#_Toc19283144)

[Carry out regular safety checks and audits and apply the associated corrective actions 18](#_Toc19283145)

[Cryptogram for whom their Student-ID is XXXXXXX2 19](#_Toc19283146)

[Finding the Key length 19](#_Toc19283147)

[Finding the key 23](#_Toc19283148)

[Decrypt the message 25](#_Toc19283149)

[References 26](#_Toc19283150)

# Introduction

This document is the report of the tests performed on the infrastructure of XYZ Bank. It contains the findings of the investigation into the recent attacks, their descriptions, solutions to prevent their recurrence, as well as recommendations to improve the overall security of the network, computer equipment, and sensitive data.

# Security report

## [22/07/2019] IIS servers (internet): Distributed Denial of service

### Description of the attack

On July 22, 2019, many requests on IIS servers (Internet) were detected and made access to them impossible. The attack was launched by hundreds of devices from different countries and lasted 15 hours.

The attack did not cause any damage to the infrastructure.

### Definition of the attack

A denial of service attack (or DoS attack) is a computer attack designed to make a service unavailable, to prevent legitimate users of a service from using it. Currently, the vast majority of these attacks are from multiple sources, referred to as Distributed Denial of Service attacks. This may include (Wikipedia, 2019):

* the flooding of a network in order to prevent its operation
* disruption of connections between two machines, preventing access to a particular service
* obstructing access to a service for a particular person
* sending billions of bytes to an internet box

The attacker does not necessarily need sophisticated equipment. Thus, some DoS attacks can be executed with limited resources against a larger and more modern network. This type of attack is sometimes referred to as an "asymmetric attack" because of the difference in resources between the protagonists.

When several machines are involved in an attack, this is called DDoS (distributed denial of service attack). Some hackers have specialized in raising armies of "zombies" which they can then rent to other individuals or malicious groups to attack a particular target.

There are several types of DOS attacks, such as SYN Flood attack, UDP Flooding, Packet Fragment, and Smurfing.

Strategy of the attackers

The attack was carried out by a large number of devices, from different locations.

There are two possibilities:

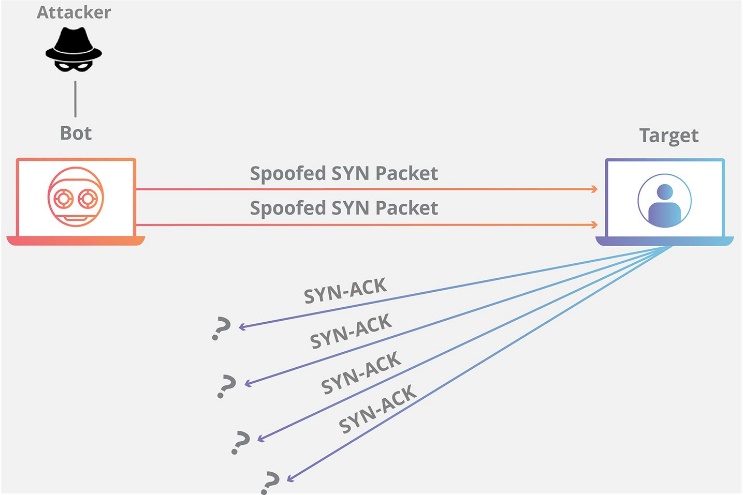
1 - the attack was launched by a group of several hundred people.

2 - the attack was launched by an attacker controlling a large number of infected machines (botnet).

Regarding the type of attack, logs indicate that the attackers caused a denial of service by sending a large number of requests for incomplete TCP synchronization with your servers.

This attack is a SYN Flood attack.

When the attackers tried to establish a TCP connection to the servers, the clients and the server exchanged a sequence of messages. When the servers sent a SYN-ACK to the clients, the clients did not respond with a ACK message. The servers then built a data structure in their system memory that describes all connections. Because this data structure is limited in size, IIS servers have been overwhelmed by the intentional creation of too many partially open connections.



## [05/08/2019] SQL server: SQL injection

### Description of the attack

On August 05, 2019, unauthorized SQL requests were detected on the main database. The purpose of these requests was to steal sensitive information about the bank's customers.

The database was compromised, and confidential data has been stolen.

### Definition of the attack

SQL command injection attacks exploit security vulnerabilities in an application that interacts with databases. The SQL attack consists in modifying an ongoing SQL query by injecting an unplanned piece of a query, often through a form. The hacker can thus access the database, but also modify the content and thus compromise the security of the system.

There are four types of SQL injection attacks: blind based, error-based, union based, and stacked queries.

### Strategy of the attackers

After investigation, it turns out that the flaw is located on the bank's news blog. When viewing a news page, the webserver makes a request to the database. This request has been modified by the attackers to steal data.

It is probable that the attackers used a vulnerability scanner such as Nessus or Nikto to detect the vulnerability.

This is the flaw that the hackers used:

The php code on the https://blog.bank.xyz/news.php?id=1 page is vulnerable to SQL injection.

$id = $\_GET["id"]

$sql = "SELECT \* FROM news WHERE id = $id";

if ($result = $mysqli->query($sql)) {

while($obj = $result->fetch\_object()){

echo($obj->text);

}

}

The code retrieves the "id" parameter located in the url. This setting can be modified to include malicious code. For example:

https://blog.bank.xyz/news.php?id=-**1 UNION SELECT password FROM users where id=1**

This simple modification will ask the server to retrieve the passwords of all users.

This vulnerability allows to launch any type of requests and has allowed the attackers to have access to all the data present on your database.

Some powerful tools, such as Sqlmap can inject malicious code automatically and dump the database.

## [16/08/2019] Internal network: Man in the middle

### Description of the attack

On August 16, 2019, the intruder detection system detected an unknown machine on the local network, as well as suspicious arp packets from the latter. The arp tables of some machines have been modified to make the traffic pass through the intruder machine.

### Definition of the attack

The man in the middle is an attack that aims to intercept communications between two parties, without either party suspecting that the communication channel between them has been compromised. The most common channel is a connection to the Internet for the average Internet user. The attacker must first be able to observe and intercept messages from one victim to another.

There are several types of MITM attacks (Rapid7, 2019):

* Rogue Access Point
* ARP Spoofing
* mDNS Spoofing
* DNS Spoofing

### Strategy of the attackers

The attacker first attacked the wifi network, which does not have sufficient security (WPA-AES and 8 characters password).

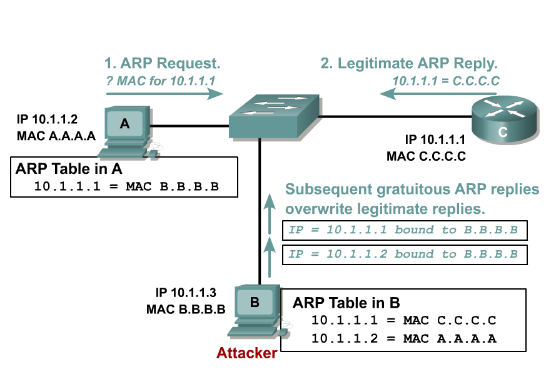
Once present on the bank's administration network, he sent malicious ARP requests to other machines to connect to the spy machine. He made an Arp poisoning attack.

To select interesting targets, he did a scan of the network with a mapping tool such as Nmap.

Technically, the machines have replaced the router's MAC address with the spy's MAC address in the ARP table.

The attacker told the other machines that the spy machine is the router.

Once the communications were redirected to the intruder, the attacker was able to sniff and capture the communications of the infected machines with Wireshark or another sniffer.



## [27/09/2019] Authentication server : Brute forcing

### Description of the attack

On September 09, 2019, a connection to the authentication server with an unknown MAC address has been detected. the attacker managed to authenticate himself and penetrate the network.

### Definition of the attack

Brute force attack is a method used in cryptanalysis to find a password or key. It is a question of testing, one by one, all possible combinations.

This method is generally considered to be the simplest conceivable. It allows any password to be broken in a finite time regardless of the protection used, but the time increases with the length of the password. In theory, the complexity of a brute force attack is an exponential function of the password length, making it impossible in principle for medium-length passwords; in practice, heuristic optimizations can give results in much shorter time frames.

This method is often combined with a dictionary and rainbow table attack to find the secret faster.

### Strategy of the attackers

The attacker tried to find the password of the admin user on the Kerberos server.

Because we can’t find any trace of brute force on the Kerberos log file, we can assume that the attacker already captured the authentication packet by sniffing the network.

The attacker might be the same as the MITM attack of the 16/08/2019.

To break the Kerberos encryption and discover the password, he may has used various strategies:

* Brute force by testing all possibilities (not probable)
* Brute force using rainbow tables
* Brute force using a dictionary

A lot of famous tools already have a configuration for Kerberos encryption. The hacker probably used Hashcat or JohnTheRipper to crack it. Depending of the force of the algorithm and the password complexity, it can be difficult or not to crack a ciphertext.

# Controls and countermeasures

## MySQL injection

### Filter user input in the application

No matter how you program, Prepared statements, and stored queries alone are not sufficient to stop injections.

It is always necessary to filter the input data of a script, shell or function in order to remove anything that a malicious user might have inserted. This filtering must be done at the server level and not at the client level to prevent the client from being disabled (e.g., javascript).

To carry out this filtering, certain elements can be taken into consideration (Owasp, n.d.):

* deleting metacharacters
* control of the parameters passed as arguments, their value, and their name
* data length limitation
* respect of the type of data (string, date, numeric characters)

### Secure web server to filter URL

it is necessary to protect the HTTP server itself or to set up a security device external to the server.

For HTTP server security, it is possible to use the mod\_security module of the Apache server or the ISA (Internet Security and Acceleration) service for Microsoft's IIS server.

It is also possible to filter URLs using a reverse-proxy relay. Thanks to regular expressions, only specifically authorized URLs are not rejected.

It is essential to limit the scope of authorized URLs to the strict minimum.

## Distributed Denial of Service

### Use of a Content Delivery Network (CDN)

A Content Delivery Network (CDN) is an infrastructure whose objective is to replace the services of an entity in order to serve its content as close as possible to users. CDNs thus have a cache function, and in particular, make it possible to increase the availability of resources or even to increase the speed of data availability.

The distribution of the processing charge over a large number of servers can help improve resistance to some DDoS attacks (ANSSI, 2015).

### Redirection via DNS protocol

Some protection services rely on DNS redirection. The purpose is to direct traffic to a domain to the IP address of a server of the protection provider. The latter then filters the traffic and redirects it to the original destination. This model of operation is often offered by CDNs to protect their customers' web servers.

### Use a firewall

Firewalls and load balancers can help to absorb some DDoS attacks. Firewalls can be used to filter traffic based on the transport protocol and source or destination ports or to limit the number of requests per source IP address to a server.

## Man in the Middle (Arp poisoning)

### End-to-end encryption

End-to-end encryption is a communication system where only those who communicate can read the messages exchanged. In principle, it prevents wiretapping, including by telecommunications providers, Internet service providers, and even by the communication service provider. With end-to-end encryption, no one is able to access the cryptographic keys needed to decrypt the conversation.

End-to-end encryption systems are designed to resist any attempt at monitoring or falsification, as no third party can decrypt the data communicated or stored (Greenberg, 2014).

### Use a packet filter

A packet filter analyzes each packet that is sent through the network. It can filter and block malicious packets, as well as those with suspicious IP addresses. With a good configuration, it can be effective against arp poisoning attacks.

### Static ARP entries

This solution is time-consuming to implement and is only recommended for small networks. This involves adding an ARP entry for each machine on a network in each individual computer.

Mapping machines with static IP and MAC address sets prevents spoofing attacks, as machines can ignore ARP responses.

## Brute Force

### Strict password policy

The first way to protect yourself from a brute force attack is to strengthen passwords.

Several criteria can be defined and implemented in many systems to ensure password quality. These criteria are, for example:

* a predefined mandatory minimum length
* force the use of symbols
* the impossibility of reusing the last n passwords
* the number of possible attempts before account locking

### Captcha verification

This technique is very simple. It consists of inserting a verification captcha that will be displayed when a connection attempt is made.

As attacks are conducted by bots, this solution is ideal for preventing automatic attempts.

Ban IPs

This technique is more complex but much more effective. It consists in limiting the number of attempts per person per day. This method consists of recording all failed connection attempts, together with the IP addresses that made these attempts.

Beyond a certain number of attempts, IP addresses are banned and cannot attempt to connect for some time.

# Security recommendations

## Establish a minimum level of security throughout the entire IT infrastructure

The user more or less familiar with good IT security practices is, in very many cases, the first point of entry for attackers to the system. It is therefore essential to set up a minimum level of security on all the bank's IT assets (user workstations, servers, printers, telephones, USB devices, …) by implementing the following measures (ANSSI, 2017):

* limiting installed applications and optional modules of web browsers to the only necessary ones
* providing user workstations with a local firewall and anti-virus software
* encrypting partitions where user data is stored
* disabling automatic executions (autorun)
* prohibit the connection of removable media
* restrict access to websites that are not on the whitelist
* Force the use of complex passwords
* disable access to system settings

To easily apply the hardening policies of the operating system or applications, it is advisable to use a centralized management tool to standardize security policies (Active directory for a Microsoft environment).

## Ensure the security of Wi-Fi access networks and the separation of uses

If it is impossible to avoid using a wi-fi network, it is necessary to secure it.

The use of Wi-Fi in the workplace is nowadays democratized but still presents very specific security risks: low availability guarantees, no control of the coverage area that could lead to an attack outside the bank's geographical perimeter, default configuration of access points with low security, etc.

The segmentation of the network architecture must make it possible to limit the consequences of an intrusion by radio to a given perimeter of the information system. Flows from workstations connected to the Wi-Fi access network must, therefore, be filtered and restricted to the only necessary flows.

In addition, it is important to use robust encryption (WPA2 mode, CCMP AES algorithm) and centralized authentication, if possible by machine client certificates, as a priority. Otherwise, it must be complex and its renewal planned, but it must under no circumstances be distributed to unauthorized third parties.

Finally, any Wi-Fi connection of personal or visitor terminals (laptops, computers) must be separated from Wi-Fi connections of the bank's terminals (e.g., separate SSID and VLAN, dedicated Internet access).

## Control and protect access to server rooms and technical rooms

Physical security mechanisms must be an integral part of information system security and be complex to ensure that they cannot be easily bypassed by an attacker. It is, therefore, necessary to identify appropriate physical security measures and to continuously raise awareness among users of the risks involved in circumventing the rules.

Access to server rooms and technical rooms must be controlled by locks or badge access control mechanisms. Unaccompanied access by external service providers to server rooms and technical rooms should be prohibited unless it is possible to track access and limit it according to time slots. A review of access rights should be carried out regularly to identify unauthorized access.

When an employee leaves or when a service provider changes, it is necessary to remove access rights or change access codes.

Finally, network outlets in areas open to the public (meeting room, lobby, hallways, closets, etc.) must be restricted or disabled to prevent an attacker from easily gaining access to the company's network.

## Protect e-mail boxes

Messaging is the primary vehicle for desktop infection, whether it is opening attachments containing malicious code or inadvertently clicking on a link that redirects to a site that is itself malicious.

Users must be particularly aware of this issue.

To protect against scams (e.g., fraudulent transfer requests, probably from a manager), organizational measures must be strictly applied.

In addition, the redirection of professional messages to a personal message is to be prohibited because it constitutes an irremediable leak of information from the bank. If necessary, controlled and secure means for remote access to professional messaging must be provided.

The bank must insure itself:

* to have an antivirus scanning system upstream of users' e-mail boxes to prevent the reception of infected files
* the activation of TLS encryption of exchanges between mail servers as well as between user workstations and servers hosting e-mail boxes.

It is advisable not to expose e-mail box servers directly to the Internet. In this case, a relay server dedicated to sending and receiving messages must be set up.

While spam - malicious or not - constitutes the majority of emails exchanged on the Internet, the deployment of an anti-spam service should eliminate this source of risk.

Finally, the email administrator will ensure that mechanisms are in place to verify the authenticity and correct configuration of public DNS records related to his email infrastructure.

## Segment the network and set up a partitioning between these areas

When the network is "flat" without any partitioning mechanism, each machine in the network can access any other machine. The compromise of one of them then jeopardizes all the connected machines. An attacker can thus compromise a user workstation and then "bounce" to critical servers.

It is therefore important to reason by segmentation into zones composed of systems with homogeneous security needs. For example, infrastructure servers, business servers, user workstations, administrator workstations, IP telephony workstations, etc. can be grouped separately.

An area is then characterized by dedicated VLANs and IP subnets or even dedicated infrastructures depending on its criticality. Thus, partitioning measures such as IP filtering using a firewall can be implemented between the different zones. Particular attention should be paid to compartmentalizing as much as possible the equipment and flows associated with administrative tasks.

## Encrypt sensitive data transmitted over the Internet

The Internet is a network on which it is almost impossible to obtain guarantees on the route that the data sent to it will take. It is therefore quite possible that an attacker may be on the data path between two correspondents.

All data sent by email or transmitted using online (cloud) hosting tools are therefore vulnerable. It is, therefore, necessary to systematically encrypt them before sending them to a correspondent or hosting them.

The transmission of the secret (password, key, etc.) then allowing the data to be decrypted, if necessary, must be carried out via a trusted channel or, if not possible, a channel separate from the data transmission channel.

## Carry out regular safety checks and audits and apply the associated corrective actions

Regular audits (at least once a year) of the information system are essential because they make it possible to evaluate the effectiveness of the measures implemented and their sustainability in practice. These controls and audits also make it possible to measure the differences that may persist between the rule and practice.

They may be carried out by possible internal audit teams or by specialized external companies. Depending on the scope to be controlled, technical, and/or organizational audits will be carried out by the professionals involved. These audits are all the more necessary as the bank must comply with regulations and legal obligations directly related to its activities.

At the end of these audits, corrective actions must be identified, their application planned and follow-up points organized at regular intervals.

# Cryptogram for whom their Student-ID is XXXXXXX2

fhwvseoehmswyudmmcqvwesitiwkeiohaveceeukikehskmeswslgfzsawiiqdtrwvhejtprgtzhvjeewysiqxsftcqsztqzdkgmlrdiamsrzduaeizekllryijlyxsekmwktalmliqszhpueczxqvefgklzqrskgyucsekiauhlgrzbwkirxirxhskgaomesmgkijtajxwkahazlvdlwoicbajmmtupsgxjwolaeiucggwzpejxhyuejtvttiutpktrwllfxdkvlvyekbrntiuaejumheikunamliqszhpueczxqvusslwfoismiuiilaxyqilapvhedhjryudmmcqvwekiauhmlvabnbsledjtasmcchjktiklscgtahrzetztxzfdgxweathksmudwvseoujkieoysfsesdayjvdefmpvhedlswtiwkeiohavecsrgntjutgwmjoukliueeukikehskmesfgkkvzejtprocwlwjfrmvxldektrubrgoiufhsmimqrqtgtqsklxigclnvvoafuiiqadbdvpbqttvdfwvxjqcjxxjtajbrxeczxqvfhwfezzdjtasmcchjkteakwtteexmjfhsmxyqmgkigdinbpvsevieifiubtrztktvvmskbkeqddhrxqrkaeiqskbqdankiszztwwslftztxktekhplfiggwwarkxgiqtkaeiunybrdgllbpvhedzvfgpkivfbokxhskeskpzqrsnxyarktvvzolxjwucaxrkteknkxqslxhvrfavmvztyxsdqtjbgrxswvvvfsztvzzgkvlvyekpmkttzxvvcuakiubrgiiifiwllfienxvyuskhplfiggmjmphemtmbdxsexylhegmrlbglxajvejqoxfycfidxzvxgjhygemgkigdeubwvxyzxhzecmlwvpswvvvfsztvzzgagqlxtaeimqlykslbsobxybajmmtglsketoeklwkduumyiqstkmtwedewkgdaxhxqnwkeceeukikehskmesiffycfidxzvxgjhygeafwtiavwwxymtammjboklmsxelhgfzslkytfivxeceeukikehskmessuaidqsxhvrzyenpkulwoicmcuxwjetjngkgrwbrsdiudicxsnxgkarkietqcggwkduummfztzxpfiejuslzdggxyqsasifrtzxqfpudnwgeirxswfhwymvxdagayuczmlvoadvycmtahrjmrwuizzgvhrvusuhrjudwkesxydtvxqifmlzeswvxzanoxtiqswgxrzexymtuefmwfxulbserojlitdelllrdifzmeyudmmcqvwekiauhlsldsuaidqikuejqdggxyqsztqzdsuaidqafwmjbejyitfafwmuqadbrfgrkvlvyelaicawwkffgnvhrkteehhlxukbwjugfbjzoafmppemsepvdtztrzzbjbgbqldlwtteexmepewwxyqcgghzfiggtzegjxekqrlaeezakbrjtaebvjarazmemlkvlvyealwlrfavmvztlhmdblwfiefomktiapgliueczxqv

Because the key is a “meaningful English word” it is very easy to retrieve the original plaintext with a dictionary attack. However, brute-forcing is not a solution for complex keys and take a lot of time to proceed. There are 3 famous ways to crack Vigenere: the Friedman test, the Kasiski Method, and the Kerckhoffs’ method.

For this exercise, I will only use the Kasiski method.

I suppose that the dictionary used is "abcdefghijklmnopqrstuvwxyz."

Finding the Key length

The Kasiski examination method will look for repetitions of a group of letters in the ciphertext.

It will then look at the distance between every similar repetition and take the intersection of every set of distances.

Example with one repetition:

rsscikyrioc**tskcxipo**xmweryizyerpmqrqckx**tskcxipo**

Distance between the two “o” is 27, so the key length can be 1,3,9, or 27.

Example with two or more repetitions:

rsscikyrioc**tskcxipo**xmweryizyer**pmqr**qckx**tskcxipo**gfsgiorabexifpoei**pmqr**

Tskcxipo distance is 27, and pmqr distance is 33

The key length is a factor of 27 and 33

Factors of 27 are **1**, **3**, 9, 27

Factors of 33 are **1**, **3**, 11, 33

In this example, we can deduce that the key length is 1 or 3.

I use a script to find repetitions of groups of 3 and 4 letters (trigraphs and quadrigraphs) and find the greatest common divider between the 6 most common distances. These parameters are optimal to find the key size.



List of every similarities found in the ciphertext:

QSZ | SEK | IRX | HSK | SKG | MES | AEI | EJT | TRW | TIU | UAE | MLI | LIQ IQS | QSZ | SZH | ZHP | HPU | PUE | UEC | ECZ | CZX | ZXQ | XQV | ILA | VHE YUD | UDM | DMM | MMC | MCQ | CQV | QVW | VWE | EKI | KIA | IAU | AUH | JTA WVS | VSE | SEO | PVH | VHE | HED | TIW | IWK | WKE | KEI | EIO | IOH | OHA HAV | AVE | VEC | EEU | EUK | UKI | KIK | IKE | KEH | EHS | HSK | SKM | KME MES | FGK | EJT | JTP | TPR | KTR | SMI | UII | IIQ | JTA | TAJ | ECZ | CZX ZXQ | XQV | FHW | DJT | JTA | TAS | ASM | SMC | MCC | CCH | CHJ | HJK | JKT FHS | HSM | XYQ | MGK | GKI | VSE | AEI | IQS | QSK | SKB | WSL | TZT | ZTX KTE | GGW | KAE | AEI | EIU | BPV | PVH | VHE | HED | XHS | HSK | ZQR | QRS ARK | KTV | TVV | XJW | RKT | KTE | TEK | YXS | SZT | KVL | VLV | LVY | VYE YEK | IUB | UBR | BRG | IFI | WLL | LLF | LFI | KHP | HPL | PLF | LFI | FIG IGG | XSE | MGK | GKI | KIG | IGD | WVX | SWV | WVV | VVV | VVF | VFS | FSZ SZT | ZTV | TVZ | VZZ | ZZG | AEI | IMQ | BAJ | AJM | JMM | MMT | SKE | EKL IQS | WKE | ECE | CEE | EEU | EUK | UKI | KIK | IKE | KEH | EHS | HSK | SKM KME | MES | ESI | FYC | YCF | CFI | FID | IDX | DXZ | XZV | ZVX | VXG | XGJ GJH | JHY | HYG | YGE | WTI | BOK | GFZ | FZS | XEC | ECE | CEE | EEU | EUK UKI | KIK | IKE | KEH | EHS | HSK | SKM | KME | MES | XHV | HVR | LWO | WOI OIC | SNX | ARK | KIE | CGG | GGW | WKD | KDU | DUU | UUM | TZX | FIE | EJU XYQ | SIF | TZX | ZXQ | IRX | RXS | XSW | FHW | MVX | YUC | MLV | VOA | MTA TAH | AHR | ZZG | VUS | HRJ | UDW | WKE | KES | ESW | SWV | WVX | IQS | RZE EXY | XYM | YMT | MTU | EFM | LBS | LLR | LRD | RDI | YUD | UDM | DMM | MMC MCQ | CQV | QVW | VWE | WEK | EKI | KIA | IAU | AUH | UHL | SUA | UAI | AID IDQ | IKU | UEJ | EJQ | DGG | GGX | GXY | XYQ | YQS | QSZ | SZT | ZTQ | TQZ QZD | DSU | SUA | UAI | AID | IDQ | AFW | WMJ | MJB | AFW | FWM | QAD | ADB KVL | VLV | LVY | VYE | VHR | RKT | KTE | TEE | OAF | FMP | TZT | TRZ | JBG DLW | WTT | TTE | TEE | EEX | EXM | WWX | WXY | XYQ | QCG | CGG | FIG | IGG GTZ | LAE | KBR | JTA | TAE | ZME | KVL | VLV | LVY | VYE | RFA | FAV | AVM VMV | MVZ | VZT | LWF | FIE | MKT | KTI | TIA | LIU | IUE | UEC | ECZ | CZX

MLIQ | LIQS | IQSZ | QSZH | SZHP | ZHPU | HPUE | PUEC | UECZ | ECZX | CZXQ ZXQV | YUDM | UDMM | DMMC | MMCQ | MCQV | CQVW | QVWE | EKIA | KIAU | IAUH WVSE | VSEO | PVHE | VHED | TIWK | IWKE | WKEI | KEIO | EIOH | IOHA | OHAV HAVE | AVEC | EEUK | EUKI | UKIK | KIKE | IKEH | KEHS | EHSK | HSKM | SKME KMES | EJTP | JTPR | JTAJ | ECZX | CZXQ | ZXQV | DJTA | JTAS | TASM | ASMC SMCC | MCCH | CCHJ | CHJK | HJKT | FHSM | MGKI | TZTX | KAEI | AEIU | PVHE VHED | XHSK | ZQRS | KTVV | KTEK | KVLV | VLVY | LVYE | VYEK | UBRG | WLLF KHPL | HPLF | PLFI | LFIG | FIGG | MGKI | GKIG | KIGD | SWVV | WVVV | VVVF VVFS | VFSZ | FSZT | SZTV | ZTVZ | TVZZ | VZZG | BAJM | AJMM | JMMT | ECEE CEEU | EEUK | EUKI | UKIK | KIKE | IKEH | KEHS | EHSK | HSKM | SKME | KMES FYCF | YCFI | CFID | FIDX | IDXZ | DXZV | XZVX | ZVXG | VXGJ | XGJH | GJHY JHYG | HYGE | GFZS | ECEE | CEEU | EEUK | EUKI | UKIK | KIKE | IKEH | KEHS EHSK | HSKM | SKME | KMES | XHVR | LWOI | WOIC | CGGW | WKDU | KDUU | DUUM RXSW | TAHR | XYMT | LRDI | YUDM | UDMM | DMMC | MMCQ | MCQV | CQVW | QVWE VWEK | WEKI | EKIA | KIAU | IAUH | AUHL | SUAI | UAID | AIDQ | DGGX | GGXY GXYQ | XYQS | QSZT | SZTQ | ZTQZ | TQZD | DSUA | SUAI | UAID | AIDQ | AFWM QADB | KVLV | VLVY | LVYE | RKTE | WTTE | TTEE | TEEX | EEXM | WWXY | QCGG FIGG | KVLV | VLVY | LVYE | RFAV | FAVM | AVMV | VMVZ | MVZT | LIUE | UECZ ECZX

List of every distances:

[48, 38, 3, 141, 27, 144, 120, 180, 196, 24, 168, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 6, 264, 324, 324, 324, 324, 324, 324, 324, 324, 180, 180, 180, 180, 165, 402, 402, 402, 102, 102, 102, 414, 414, 414, 414, 414, 414, 414, 414, 414, 414, 432, 432, 432, 432, 432, 432, 432, 291, 432, 432, 288, 330, 240, 420, 420, 249, 204, 226, 486, 207, 372, 276, 276, 276, 276, 582, 228, 21, 228, 228, 228, 228, 228, 228, 228, 228, 96, 96, 294, 426, 426, 224, 432, 372, 138, 18, 632, 300, 300, 90, 462, 48, 48, 480, 96, 294, 294, 294, 558, 267, 594, 594, 54, 114, 114, 539, 15, 84, 84, 670, 720, 552, 552, 552, 552, 552, 201, 330, 330, 210, 588, 588, 155, 168, 168, 168, 13, 168, 168, 754, 300, 300, 300, 300, 368, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 251, 444, 762, 762, 762, 762, 243, 876, 336, 582, 990, 990, 558, 558, 558, 558, 558, 558, 558, 291, 558, 558, 558, 1016, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 622, 336, 1032, 1032, 520, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 335, 335, 918, 918, 918, 407, 408, 755, 936, 474, 180, 180, 180, 180, 354, 336, 909, 582, 165, 24, 630, 1038, 417, 417, 642, 728, 1074, 888, 702, 180, 870, 870, 306, 960, 18, 870, 252, 531, 1243, 348, 364, 300, 925, 428, 244, 244, 1092, 888, 351, 1218, 1236, 1236, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1188, 252, 252, 252, 252, 1083, 1125, 474, 180, 180, 180, 180, 180, 1086, 432, 1290, 1290, 1290, 24, 24, 24, 24, 24, 336, 936, 324, 12, 12, 864, 864, 600, 600, 600, 600, 174, 666, 666, 834, 918, 1032, 786, 833, 678, 1274, 882, 882, 48, 882, 882, 432, 432, 120, 330, 330, 642, 642, 1437, 1290, 1254, 939, 569, 198, 126, 126, 126, 126, 768, 768, 768, 768, 768, 768, 1258, 382, 748, 1204, 516, 1116, 1116, 1284, 1008, 1008, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 156, 324, 324, 324, 324, 324, 324, 324, 180, 180, 180, 402, 402, 102, 102, 414, 414, 414, 414, 414, 414, 414, 414, 414, 432, 432, 432, 432, 432, 432, 432, 432, 432, 432, 420, 420, 372, 276, 276, 276, 228, 228, 228, 228, 228, 228, 228, 228, 228, 96, 426, 300, 48, 480, 294, 294, 558, 594, 114, 84, 552, 552, 552, 552, 330, 588, 168, 168, 168, 168, 168, 300, 300, 300, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 762, 762, 762, 990, 990, 558, 558, 558, 558, 558, 558, 558, 558, 558, 558, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 138, 1032, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 72, 335, 918, 918, 936, 180, 180, 180, 417, 870, 244, 1236, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1008, 1188, 252, 252, 252, 180, 180, 180, 180, 1290, 1290, 1290, 1290, 24, 24, 24, 24, 12, 864, 600, 600, 600, 666, 882, 882, 882, 882, 432, 330, 642, 126, 126, 126, 768, 768, 768, 768, 768, 1116, 1284, 1008]

The six most common distances are:

138 (x49), 1008 (x28), 180 (x25), 156 (x25), 72 (x25) 432 (x24)

The GCD of these numbers is 6. The key length is probably 6.

## Finding the key

Now that we know the key length, we can separate the ciphertext in 6 (key length) parts.

The first array contains every 1 + (6\*i) letters of the ciphertext, the second: 2 + (6\*i), etc.…

FOYQTOEESZQHGEQQDDZZYSTQEEQUAZXKSTADBUWUPUTTXYTUUQEUOIQHYQAAEMTGEFAUOOSDHTOSUOEESZOFDBFQQGOQPDQTEFZMTTFQDSFZMQQQAZFTFAQUGHGBKQAZUTQRZQXFZYTCBFIUFMMXMXQFXEDXEPFZXQBBGODQWGQEESFXEAMBXZFEESQZUMEGDXAQDZIZQRPEFXUOMMZUUXQEAQZUXRDDYQADQQQDQBFQGYAGTXUOEDZQTPQFEQZTAMYRZBFAE

HEUVIHEHWSDETEXSKIDEIEASCFRCUBIGMAHLAPOCEEIRDEIMNSCSIIIEUVUBDCITTDTDUYDEEIHRTUEHFECRERHRSCAABFCACHDCEEHMIEITSDRSNTTEIRTNLEPOERROCESFTTSSGETURIESIPBYRAOIGMEYCSSGTLSALEUSEDNEHIIGAVTOESIEHSSYLCTRISRCUTEDSTUIHDCATRGSDYISNSEEUOEIUVUSIDSSAEAAREWNEUGAMTBLEECIGRAARLEFTLOPC

WHDWWAUSSATJZWSZGAUKJKLZZGSSHWRAGJAWJSLGJJUWKKUHAZZSSLLDDWHNJCKAZGHWJSAFDWAGGKUSGJWMKGSQKLFDQWJJZWJCAESGNVUKKDKKKWZKGKKYLDKKSSKLAKLAYJWZKKZAGWNKGHDLLJXDJGUZMWZAAYOJSKUTDAWUSFDJFWAKLLVUSUXEWUJWUNKGUZJGAZDRWAZDAWVUWDFWOWXFLJLFDWHUKGZUFJFDKLWVEKFFSZJDEWGGJLKEAKAALWMGZ

VMMEKVKKLWRTHYFTMMALLMMHXKKELKXOKXZOMGAGXTTLVBAEMHXLMAAHMEMBTHLHTXKVKFYMLKVNWLKKKTLVTOMTLNUBTVXBXFTHKXMKBIBTBHABIWTHGXABBZIXKNTXXNXVXBVTVPXKILXHGEXHBVFXHKBXLVTGEKBMKLMKEXKKKFXHWWMLHKXKKAHNOXNBDXIGMXUGSXNXYGMVHUHHKTMVXGYMBLLZMELAUGTAWYWBVAKHHBBMETBLXWGGXABBZVLVHFKLX

SSMSEEIMGIWPVSTQLSELYWLPQLGKGIHMIWLIMXEWHVPLLREILPQWIXPJMKLSAJSRXWSSISJPSEETMIIMKPWXRIIGXVIDTXXRQEAJWMXIPETVKREQSSXPWGERPVVHPXVJRKHMSGVVLMVIILVPMMSEGEYZYIWHWVVQISXMEWYMWHEIMYZYTXMMGYEIMIVPIWGRIGEWMPSXIQWSMALYRIRREVLXTXMWSILMMKSIEXQIMIMRLIFRHWJPPRGWMXHTEERVMLWMMITIQ

EWCIICKEFIVRJICZRRIRXKIUVZYIRRSEJKVCTJIZYTKFVNJKIUVFUYVRCIVLSKCZZEMEEEVVWICJJUKEVRJLUUMTIVIVVJJXVZSKTJYGVIRVEXIDZLKLWIIDVFFSZYVWKXVVDRVZVKVUIFYLJTEGLJCVGGVZVVZLMLYTTKITKXCKECVGIYJSFTCKEDRKCJKSCKTKFFLYFFGWVYVCJZVJSXZZIRTFETRECILDJYZDJTUFVCFKLJZPVZBTEYZZKEJJEVLVDEIUV

The next step is to do a frequency analysis on each ciphertext fragments.

I compare the frequency of letters from millions of English words, with the frequency of letters in fragments.

We use these values for the frequencies of letters in the English language (source: https://norvig.com/mayzner.html):

A = .0804 | B = .0148 | C = .0334 | D = .0382 | E = .1249 | F = .0240 | G = .0187 | H = .0505 |

I = .0757 | J = .0016 | K = .0054 | L = .0407 | M = .0251 | N = .0723 | O = .0764 | P = .0214 |

Q = .0012 | R = .0628 | S = .0651 | T = .0928 | U = .0273 | V = .0105 | W = .0168 | X = .0023 |

Y = .0166 | Z = .0009

After comparing the frequency, I rotate my array (the 1st value become the last) of the fragment letter frequency, and I do comparison again. I rotate it and do the comparison 26 times. (numbers of letters in our alpha).

[264.2504, 264.2672, 264.37140000000005, 264.33, 264.27799999999996, 264.4412, 264.2684, 264.507, 264.29879999999997, 264.5278, 264.1894, 264.2717999999999, **264.0394**, 264.37919999999997, 264.1286, 264.159, 264.25939999999997, 264.4684, 264.40880000000004, 264.25419999999997, 264.38379999999995, 264.44640000000004, 264.315, 264.2388, 264.27359999999993, 264.2476]

[**264.0076**, 264.2276, 264.25859999999994, 264.21579999999994, 264.1194, 264.38599999999997, 264.273, 264.20039999999995, 264.30679999999995, 264.26439999999997, 264.0822, 264.2342, 264.3992, 264.1604, 264.16940000000005, 264.0952, 264.3498, 264.2836, 264.26, 264.04459999999995, 264.12459999999993, 264.42379999999997, 264.2758, 264.3028, 264.24139999999994, 264.2974]

[264.22399999999993, 264.41479999999996, 264.18399999999997, 264.13159999999993, 264.336, 264.121, 264.09119999999996, 264.2358, 264.4476, 264.1696, 264.207, 264.25699999999995, 264.15299999999996, 264.24080000000004, 264.229, 264.39680000000004, 264.2136, 264.1698, **264.0104**, 264.22799999999995, 264.275, 264.2368, 264.28400000000005, 264.4616, 264.21299999999997, 264.07259999999997]

[264.07259999999997, 264.224, 264.41479999999996, 264.184, 264.13159999999993, 264.3359999999999, 264.121, 264.09119999999996, 264.2358, 264.4476, 264.16959999999995, 264.207, 264.25699999999995, 264.15299999999996, 264.24080000000004, 264.229, 264.39680000000004, 264.2136, 264.16979999999995, **264.0104**, 264.22799999999995, 264.275, 264.2368, 264.28400000000005, 264.4616, 264.21299999999997]

[264.4486, 264.571, 264.4246, 264.253, **264.0544**, 264.2357999999999, 264.46, 264.35880000000003, 264.376, 264.6952, 264.593, 264.2746, 264.2932, 264.4872, 264.49760000000003, 264.27799999999996, 264.4194, 264.20699999999994, 264.13559999999995, 264.26, 264.65360000000004, 264.4562, 264.37460000000004, 264.4306, 264.4052, 264.36]

[264.4172, 264.2268, 264.2844, 264.4806, 264.17119999999994, 264.1726, 264.2466, 264.4508, 264.32099999999997, 264.308, 264.2944, 264.20099999999996, 264.49060000000003, 264.30539999999996, 264.46360000000004, 264.2432, 264.3306, **264.01220000000006**, 264.2612, 264.2796, 264.2704, 264.30500000000006, 264.51619999999997, 264.3986, 264.20279999999997, 264.3496]

We now have arrays of 26 results of comparisons for each fragment. I look at the position of the lowest value, look at the same place in the alphabet, and add the character to the Key.

For example, in the 1st fragment, the lowest value of the comparison is at the 12th position (start from zero), so the 1st letter of the key is M.

Fragment 1: M

Fragment 2: A

Fragment 3: S

Fragment 4: T

Fragment 5: E

Fragment 6: R

The key is MASTER.

## Decrypt the message

To decrypt the ciphertext, subtract the value of letters in the ciphertext, with the value of letters in the key. The key is smaller than the ciphertext, so when we arrive at the last character, we start over.

Let’s do the beginning:

F – M = 5 – 12 = -7 (negative result, so we add 26) = 19 = T

H – A = 7 – 0 = 7 = H

W – S = 22 – 18 = 4 = E

V – T = 21 – 19 = 2 = C

S – E = 18 – 4 = 14 = O

E – R = 4 – 17 = -13 (+26) = 13 = N

O – M = 14 – 12 = 2 = C

E – A = 4 – 0 = 4 = E

H – S = 7 – 18 = -11 (+26) = 15 = P

**The full plaintext:**

THECONCEPTOFMULTILEVELORHIERARCHICALSECRETSHARINGWASCONSIDEREDBYSEVERALAUTHORSSEEFOREXAMPLESHAMIRKOTHARIITOANDCHARNESSHAMIRSUGGESTSTHATTHRESHOLDSCHEMESFORHIERARCHICALGROUPSCANBEREALIZEDBYGIVINGMORESHARESTOHIGHERLEVELPARTICIPANTSKOTHARICONSIDEREDHIERARCHICALTHRESHOLDSCHEMESINWHICHASIMPLETINITHRESHOLDSCHEMEISASSOCIATEDWITHTHEITHLEVELOFAMULTILEVELGROUPTHEOBVIOUSDRAWBACKOFTHISSOLUTIONISTHATITDOESNOTPROVIDECONCURRENCYAMONGDIFFERENTLEVELSOFHIERARCHICALGROUPSITODISCUSSEDSECRETSHARINGFORGENERALACCESSSTRUCTURESANDPROVEDTHATEVERYACCESSSTRUCTURECANBEREALIZEDBYAPERFECTSECRETSHARINGSCHEMETHEMAINDRAWBACKOFTHEIRSCHEMEISTHATTHEMOREPRIVILEGEDPARTICIPANTSAREASSIGNEDLONGERSHARESSIMMONSPOINTEDOUTTHATTHESOLUTIONSFORSECRETSHARINGINMULTILEVELGROUPSPROPOSEDBYEARLIERAUTHORSARENOTEFFICIENTHESUGGESTEDEFFICIENTGEOMETRICALSECRETSHARINGSCHEMESWITHTHEREQUIREDPROPERTIESHOWEVERHISSOLUTIONISAPPLICABLEONLYTOAPARTICULARCASEOFMULTILEVELGROUPSMOREPRECISELYHEDISCUSSEDSECRETSHARINGINMULTILEVELGROUPSWITHPARTICULARACCESSSTRUCTURESBRICKELLSTUDIEDGENERALSECRETSHARINGINMULTILEVELGROUPSANDPROVEDTHATITISPOSSIBLETOCONSTRUCTIDEALSECRETSHARINGSCHEMESFORANYMULTILEVELACCESSSTRUCTUREINBRICKELLSVECTORSPACECONSTRUCTIONTHELOWERBOUNDONTHESIZEOFTHEMODULUSPSIZEOFTHEFIELDINWHICHTHECALCULATIONSAREBEINGDONEISCONSIDERABLYLARGEINTHISSECTIONWEPRESENTANEFFICIENTSOLUTIONFORSECRETSHARINGINMULTILEVELGROUPSOURSCHEMEISBASEDONTHESHAMIRSCHEMEANDISPERFECTANDIDEALINOURSCHEMETHELOWERBOUNDONTHEMODULUSISSIGNIFICANTLYSMALLERTHANINBRICKELLSSCHEMEINDEEDTHECONDITIONPISGREATERTHANNASINSHAMIRSORIGINALSCHEMEISSUFFICIENTTOIMPLEMENTOURPROPOSEDSCHEME

# References

ANSSI. (2013, 08 13). *ssi.gouv.fr.* Retrieved from Recommandations pour la sécurisation des sites web: https://www.ssi.gouv.fr/uploads/IMG/pdf/NP\_Securite\_Web\_NoteTech.pdf

ANSSI. (2017). *Guide d’hygiène informatique.* Retrieved from ssi.gouv.fr: https://www.ssi.gouv.fr/uploads/2017/01/guide\_hygiene\_informatique\_anssi.pdf

Greenberg, A. (2014, November 25). *Hacker Lexicon: What Is End-to-End Encryption?* Retrieved from Wired.com: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/

Owasp. (n.d.). *SQL Injection Prevention Cheat Sheet*. Retrieved from Owasp.org: https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html

Rapid7. (2019). *Brute-Force and Dictionary Attacks*. Retrieved from rapid7.com: https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/

Rapid7. (2019). *Man-in-the-Middle (MITM) Attacks*. Retrieved from Rapid7.com: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Wikipedia. (2019). *Denial of service attack*. Retrieved from Wikipedia.org: https://en.wikipedia.org/wiki/Denial-of-service\_attack