Introduction Different audits type Deontology

Sécurité des SI - Introduction

Matthieu Keller

ECE

January 21, 2020

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Whoami

Matthieu Keller Pentester for 6 years and 9 months. Teacher (part-time) for 2 years and 11 months.

>id

uid=0(root) gid=0(root) groups=0(root)

>whoami

nt authoriy\system

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Maslow Attacks Actors Malware and vocabulary Our journey

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

TV5 monde

Introduction Different audits type Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

Introduction Different audits type Deontology

Petya, not-petya, Saint-Gobain (and others)

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

French hospitals - CHU

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

Hacktivists

Anonymous (2003 - ) L0pht (1992-2000) Lulzsec (2011 - 2011) CCC State sponsored (?) groups

Equation group (NSA?) (??) APT28 / Fancy bear (Russia?) (2004 - ) APT20 (China?) (2011 - )

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

Malware vs virus trojan Horse rootkit backdoor keylogger webshell ransomware deny of Service (DOS) DDOS phishing spear phishing APT

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

Top 10 most-clicked phishing using general email subjects

1 Change of Password Required Immediately 26% 2 Microsoft/Office 365: De-activation of Email in Process 14% 3 Password Check Required Immediately 13% 4 HR: Employees Raises 8% 5 Dropbox: Document Shared With You 8% 6 IT: Scheduled Server Maintenance – No Internet Access 7% 7 Office 365: Change Your Password Immediately 6% 8 Avertissement des RH au sujet de l’usage des ordinateurs

personnels 6% 9 Airbnb: New device login 6% 10 Slack: Password Reset for Account 6% Source: https://www.techrepublic.com/article/these-subject-lines-are-the- most-clicked-for-phishing/Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey Plan1 Introduction

Maslow Attacks Actors Malware and vocabulary Our journey

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

Introduction, OSINT Cryptography Linux Wireshark, Windows Buffer overflow Network Web application 1

Web application 2Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Maslow Attacks Actors Malware and vocabulary Our journey

Matthieu Keller Sécurité des SI - Introduction

Maslow Introduction

Attacks Different audits type

Actors Deontology

Malware and vocabulary Our journey

Exam:1h30

Only theoritical (on paper) QCM and open questions All of our journey is concerned In english for international groups. In French for French group

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Plan1 Introduction

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Security Audit

A security audit give an independent and impartial opinion about the security of the analysed perimeter.

The audit will give a vision of the perimeter exposition to risks at a time t.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Organisational and Physical security audits

Organisational and Physical security audits

This audit goal is to check that the policy and procedures defined in order to keep the <Information System (IS), appli- cation, . . . > are:

In compliance with the threat model of the auditee In compliance with the actual standards In accordance with the technical measures in place Efficiently applied

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Organisational and Physical security audits

The Organisational and Physical security audits are documentation and interviews based.

Documentation

Information Systems Security Policy (ISSP) Access control policy Risk analysis methodology Other documents regarding the IS (Information System) security and access control Interviews

CISO (Chief information security officer) The person in charge of information security in the CIO (Chief information officer) team Operator of the security solution and services (or applications) Security officer (for the physical security)

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Organisational and Physical security audits

Some example of control point for a ISO 2700x audit (not limited to):

Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization’s information security policy

All information and assets associated with information processing facilities shall be ‘owned’ by a designated part of the organization

Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.

Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Architecture audits

Architecture audits

consists of verifying the compliance of security practices rel- ative to the choice, positioning and implementation of the hardware and software devices deployed in a state-of-the-art information system. The audit can be extended to interconnections with third- party networks, in particular the Internet.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Architecture audits

The architecture security audits are documentation and interviews based.documentation (not limited to)

Technical architecture files OSI level 2 and 3 diagram Flow matrices Fire walling rules Network equipment configuration (routers, switch, firewall, load balancer) Interconnections with third-party networks or the Internet; Risk analysis Procedures and other technical documents related to the perimeter Previous architecture audit reports interviews

System and network infrastructure manager System and network administrators

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Architecture audits

Some example of control points (not limited to):

Technical architecture quality

Component scalability and sustainability Component administration and supervision Performance monitoring Incident management Security and robustness of the technical architecture Redundancy (Servers and network equipments) Auto switch in case of failure High availability mechanism for the systems Data backup (process, architecture, archivage policy) Business recovery plan

Data and process availability Continuity process Network, system and application classification regarding availability

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Vulnerability scan

Vulnerability scan

Is the use of an (automated) tool to estimate the number of vulnerability in a system at a given time.

It is a operation to do regularly (low cost). Some tools: Nessus Nmap Qualys MBSA

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Configuration audit

Configuration audit

Aim to verify that configuration of device implement the secu- rity practices in accordance with state of the art and internal audit rules.

These devices can notably be:

Network equipements OS (workstation or server) Application (apache, MySQL, . . . ) Security product (Firewall, IPS, IDS, . . . )

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Source code audit

Source code audit

Consists of analyzing all or part of the source code or the compilation conditions of an application in order to discover vulnerabilities linked to poor programming practices or logic errors, that could have an impact on security.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Source code audit

This audit require the source code of the application, its documentation and interviews with the developers (optional). It can be automated with tools (checkmarx, fortify, PMD). But mostly is manual.Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

PentestPenstest

Its goal is to emulate an attacker and discover vulnerability on the target, And verify their exploitability and impact in real conditions.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Pentest

The target can take many forms:

Web extern (ip) internal black box gray box white box

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Pentest vs vulnerability scan

Vulnerability scan is List-Oriented Peneration tests are Goal-Oriented

The vulnerability scan is :

More complete regarding attack surface

Less complete regarding depth of attack (privesc, bounce)

"Dumber"

link to the port scan’s quality and exhaustivity

only testing known vulnerabilities

authentication can be a pain

might need some attention from an experimented pentester

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Other (exotic) audits

Physical audit (lock picking) Active Directory audit Passwords audit SCADA audit VOIP audit Wifi audit Badges audits Thick client audit hardware audit Firmware audit Social engineering Red team

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Plan1 Introduction

2 Different audits type

3 Deontology

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

French law

Article 323-1

Le fait d’accéder ou de se maintenir, frauduleusement, dans tout ou partie d’un système de traitement automatisé de données est puni de deux ans d’emprisonnement et de 30 000 euros d’amende.

Lorsqu’il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d’emprisonnement et de 45 000 euros d’amende.

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Other considerations

Confidential documents (company) Ability to transfer money Company’s client’s data Users’ passwords Personal documents

Matthieu Keller Sécurité des SI - Introduction

Introduction Different audits type Deontology

Tools

A local network connection (usb to ethernet adapter) I strongly recommend a Kali Linux (VM)

a Web browser: Firefox a (script) programming language: python a password cracker: John (or hashcat) a port scanner: nmap the ability to connect using SSH: Linux or putty a packet analyzer: Wireshark a online bruteforcer: hydra, patator a MitM proxy: Burp Suite, ZAP Proxy a directory brute forcer: dirb, gobuster, dirbuster Automatic scanner: Nikto, Nessus SQLi scanner: sqlmap, sqlninja

Matthieu Keller Sécurité des SI - Introduction

WHOIS Information DNS Records Internet Searches

Sécurité des SI - OSINT

Matthieu Keller

ECE

January 17, 2020

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches Definition

OSINT

Open Source INtelligence is produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.

(source: DOD)

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches Plan1 WHOIS Information

2 DNS Records

3 Internet Searches

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches Whois

whois zonetransfer .me

host zonetransfer .me

whois 5.196.105.14

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches Plan1 WHOIS Information

2 DNS Records

3 Internet Searches

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches DNSDo you know about DNS records?

A: Maps hostname to IP addresses AAAA: Maps hostname to IPv6 addresses AXFR: Transfers all information about a domain CNAM: Alias of one hostname to another MX: Points to a mail transfer agent for a domain NS: Points to a DNS server for a domain PTR: Maps an IP address to a hostname (reverse of A record) SOA: Contains authoritative information (primary NS, serial number, caching information) about a domain SRV: Service location record (usually only used internally by Active Directory) TXT: Record which contains human-readable text

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches DNSdig zonetransfer .me

dig zonetransfer .me ANY

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches DNS Zonetransfer

dig axfr @nsztm1.digi.ninja zonetransfer.me

https://digi.ninja/projects/zonetransferme.php

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

Plan1 WHOIS Information

2 DNS Records

3 Internet Searches

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

Google Dorks

Google dorks: involves using advanced operators in the Google search engine to locate specific strings of text within search results.

site: site :ece. fr filetype: filetype :pdf inurl: inurl :ece. fr /ecole-ingenieur intext: intext: secret intitle: intitle : confidentiel ”: intitle :"index of /" filetype :mkv <whatever> +/ -: filetype :. config+"password="

https://www.exploit-db.com/google-hacking-database

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

The Harvester

theHarvester -d ece.fr -b google

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

Shodan

demo

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

Plan1 WHOIS Information

2 DNS Records

3 Internet Searches

Social networks

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

twint

twint -u ingenieursece -o out.csv

twint -s "IngenieursECE"

twint -u ingenieursece --email

Matthieu Keller Sécurité des SI - OSINT

Social networks

Tweet-analyzer

WHOIS Information DNS Records Internet Searches

Matthieu Keller Sécurité des SI - OSINT

WHOIS Information DNS Records Internet Searches

Social networks

Sources"Méthodologie d’OSINT orientée réseaux sociaux" - Brian

Nicolas-Nelson, MISC 104. https://www.andreafortuna.org/2017/03/20/open-source- intelligence-tools-for-social-media-my-own-list/ https://github.com/twintproject/twint https://github.com/x0rz/tweets\_analyzer

Matthieu Keller Sécurité des SI - OSINT

Vocabulary Some history Modern cryptography Conclusion

Cryptography

Matthieu Keller

ECE

January 26, 2020

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion Plan1 Vocabulary

2 Some history

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

cryptography: is the practice of coding an information in order that anyone accessing it without knowing the key (and cipher) will not be able to retrieve it. Guvf grkg vf na rknzcyr bs n (onfvp) plcure.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

cryptography: is the practice of coding an information in order that anyone accessing it without knowing the key (and cipher) will not be able to retrieve it. This text is an example of a (basic) cypher.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

cryptography: is the practice of coding an information in order that anyone accessing it without knowing the key (and cipher) will not be able to retrieve it. This text is an example of a (basic) cypher. Cryptanalysis: is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

cryptography: is the practice of coding an information in order that anyone accessing it without knowing the key (and cipher) will not be able to retrieve it. This text is an example of a (basic) cypher. Cryptanalysis: is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. Steganography: is the practice of hiding some information within some genuine support. We will not speak about that in this course. This white text is a (basic) example of steganography.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

cryptography: is the practice of coding an information in order that anyone accessing it without knowing the key (and cipher) will not be able to retrieve it. This text is an example of a (basic) cypher. Cryptanalysis: is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. Steganography: is the practice of hiding some information within some genuine support. We will not speak about that in this course. This [white] text is a (basic) example of steganography.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution Plan1 Vocabulary

2 Some history

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution Plan1 Vocabulary

2 Some history

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

In -600, Nabuchodonosor, King of Babylone, wrote messages on his slave’s shaved head, waited for their hairs to grow and send the slave to his generals.

In -400 the first (known) usage of cryptography with a Scytale: a cylinder with a strip of parchment wound around it on which is written a message. The recipient just need a rod of the same diameter on which the parchment is wrapped to read the message.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution Plan1 Vocabulary

2 Some history

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

In -200 Julius Caesar, used the "Caesar cipher". A simple substitution cipher where a character is simply replace by another with a fix shift.

Plaintext : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG Ciphertext : QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

This cipher can be break either by frequency analysis or by simple brute force as there is only 25 possible shift (in English using only letters).

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

In -150 appear the Polybius square, another substitution method. Wake up time: 32 51 13 13 43 25 43 24 13 41

Matthieu Keller Cryptography

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vocabulary Some history Modern cryptography Conclusion

This method is quit useful as you can transmit the information over long distance using torches or flags.

In order to have some encryption you just need to change the letter order. Moreover you can enlarge the square to include numbers an symbols (space).

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution Plan1 Vocabulary

2 Some history

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vocabulary Some history Modern cryptography Conclusion

In 800 Al-Kindi (Alkindus) wrote the first book about breaking codes Deciphering Cryptographic Messages introducing several new methods of breaking ciphers, notably frequency analysis.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution Plan1 Vocabulary

2 Some history

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

3 Modern cryptography

4 Conclusion

Matthieu Keller Cryptography

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vocabulary Some history Modern cryptography Conclusion

In 1467 Leon Battista Alberti invented the premiss of the polyalphabetic substitution.

Matthieu Keller Cryptography

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vocabulary Some history Modern cryptography Conclusion

In 1553 Giovan Battista Bellaso will describe the Vigenere cipher (misattribution in the 19th century). Lvymi wyypcijp qmnipx gpitrykpklni mq msksre. Key is the key.

Matthieu Keller Cryptography

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vocabulary Some history Modern cryptography Conclusion

In 1553 Giovan Battista Bellaso will describe the Vigenere cipher (misattribution in the 19th century). Brace yourself modern cryptography is coming. Key is the key.

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

Vigenere Cryptanalysis (text is in French)

MUKS RVUV QRRV LLVR EDHS RZVG QMCV ICDB GLNL TRTY QRIL VIMC MRZL SVAY MBBX RVCE ECRU EMMN BAFV EVBQ QPHL SJMF OAZS AXVR ELHL AGXN DAVV SVVG YOAR TFVR EEGD TKZV ETNQ TVAC QKNQ GUMQ MITQ ERCW AUEG HLQY QSOH ALBR EDRO AEIG GRRO EJKU MMCV VVZQ AYNQ TJTN RRNL CYMH DDRV LRKF XOZE RVLR EBBL SKWH RFHV NVAN GRNL EEBY QCUD RDME BOHU LLQY QSSO ELZF EAPU EVAQ GLVV OEBC QRQX LVCE BAEI UDTR ESBQ SAWL QUKG EJNY GTRV RRXC QLNQ TCWQ QKBX AEBF QURW LRDB UXCO AZVG UVRG ECWV EENX JRCA QLRW RFCI QNGH GRTR YEAW IEAR ZSVE LVTB DSDX ICWS RRRV ECWA XEFU IKMF PEFV ATZV RIPH SRAR EAAF EKZR EDNQ SCMG QMCO EDMZ QPRN AEOF ANTH EEKB DERW DVAV DE

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

First we need the key length. We found the 3 characters (or more) repetitions.

MUKS RVUV QRRV LLVR EDHS RZVG QMCV ICDB GLNL TRTY QRIL VIMC MRZL SVAY MBBX RVCE ECRU EMMN BAFV EVBQ QPHL SJMF OAZS AXVR ELHL AGXN DAVV SVVG YOAR TFVR EEGD TKZV ETNQ TVAC QKNQ GUMQ MITQ ERCW AUEG HLQY QSOH ALBR EDRO AEIG GRRO EJKU MMCV VVZQ AYNQ TJTN RRNL CYMH DDRV LRKF XOZE RVLR EBBL SKWH RFHV NVAN GRNL EEBY QCUD RDME BOHU LLQY QSSO ELZF EAPU EVAQ GLVV OEBC QRQX LVCE BAEI UDTR ESBQ SAWL QUKG EJNY GTRV RRXC QLNQ TCWQ QKBX AEBF QURW LRDB UXCO AZVG UVRG ECWV EENX JRCA QLRW RFCI QNGH GRTR YEAW IEAR ZSVE LVTB DSDX ICWS RRRV ECWA XEFU IKMF PEFV ATZV RIPH SRAR EAAF EKZR EDNQ SCMG QMCO EDMZ QPRN AEOF ANTH EEKB DERW DVAV DE

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

We look at the distance between each repetitions:

Sequence distance RVL 200 VRE 80 HSR 425 ZVG 336 QMC 445 VCE 223 NQT 64 CWA 271

Matthieu Keller Cryptography

Vocabulary Some history Modern cryptography Conclusion

An hairs and rod story Substitution ciphers The beginning of Cryptanalysis polyalphabetic substitution

We decompose them into prime factor:

sequence prime factors RVL 200 = 23x52 VRE 80 = 24x5 HSR 425 = 52x17 ZVG 336 = 24x3x7 QMC 440 = 23x5x11 VCE 232 = 23x29 NQT 64 = 26 CWA 271 = 271 The common factor seems to be 23 = 8

Matthieu Keller Cryptography