HALFWAY WRAP-UP

Introduction to Computer and Network Security

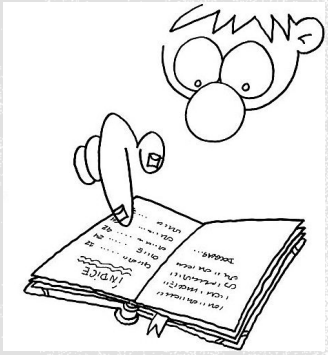
Silvio Ranise [silvio.ranise@unitn.it or *ranise@fbk.eu*]

UNIVERSITÀ DI TRENTO

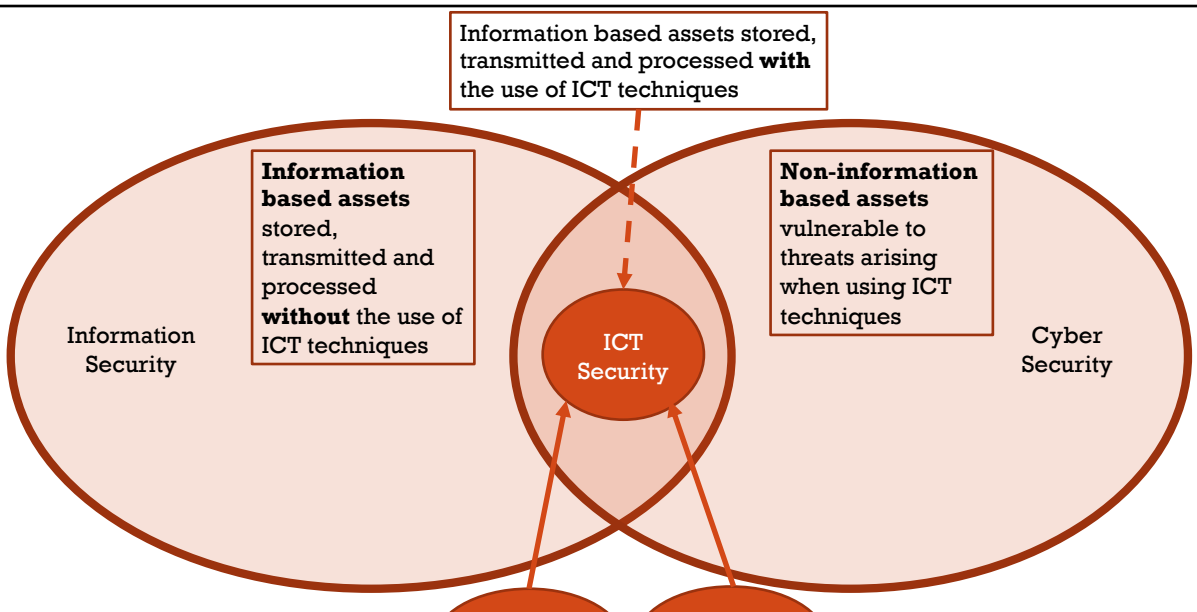
FONDAZIONE BRUNO KESSLER

CONTENTS

- Basic notions
- Authentication I
- Cryptography
- Applications of cryptography



2 BASIC NOTIONS



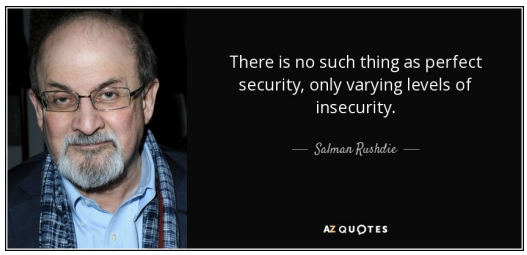
https://www.researchgate.net/publication/281107085_From_Information_Security_to_Cyber_Security_Cultures_Organizations_to_Societies

3

Potential for an attacker to successfully exploit a particular vulnerability

Any data, device, or other component of the environment that supports information-related activities

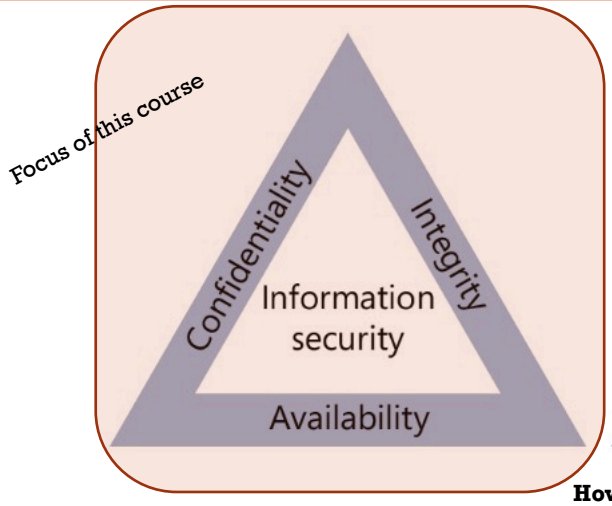
Weakness that could be exploited or triggered by an attacker

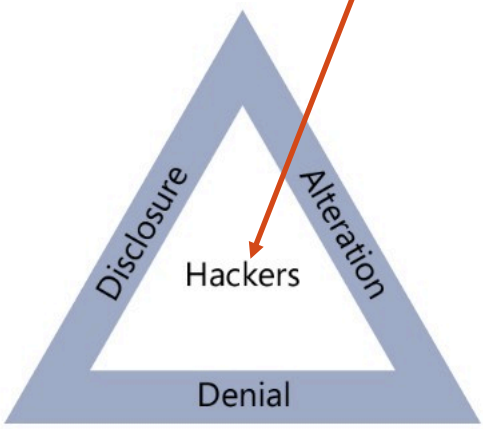


Likelihood	Severity of Impact: Negligible	Marginal	Serious	Critical	Catastrophic
Highly Probable	1x5= 5	2x5= 10	3x5= 15	4x5= 20	5x5= 25
Probable	1x4= 4	2x4= 8	3x4= 12	4x4= 16	5x4= 20
Occasional	1x3= 3	2x3= 6	3x3= 9	4x3= 12	5x3= 15
Remote	1x2= 2	2x2= 4	3x2= 6	4x2= 8	5x2= 10
Improbable	1x1= 1	2x1= 2	3x1= 3	4x1= 4	5x1= 5

- **Information** contained **in assets** can be **abused** in several different ways that can be traced back to the **three basic security properties**
- In case of **non-information based assets**, attacks can **violate properties that go beyond those of the CIA**, e.g., **safety**
  - Remember the Jeep attack in 2015

Attribution problem





How to protect from the disruptions of attackers?

5

SECURITY POLICY, SERVICE & MECHANISM

- Security **policy**
  - The rules and requirements established by an organization that governs the acceptable use of its information and services, and the level and means for protecting the confidentiality, integrity, and availability of its information

    https://csrc.nist.gov/Glossary/?term=1268#AlphaIndexDiv
- Security **mechanism**
  - A device or function designed to provide one or more security services usually rated in terms of strength of service and assurance of the design.
  - Implementation of a security policy

    https://csrc.nist.gov/Glossary/?term=1262#AlphaIndexDiv
- Security **service**
  - A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.

    https://csrc.nist.gov/Glossary/?term=1268#AlphaIndexDiv

6

BASIC NOTIONS (1)

- Define the following notions
  - Information security
  - Computer security
  - Network security
  - Cyber security
- What is the difference between
  - Cyber security
  - Cyber security readiness/posture
- What is the difference between
  - Security
  - Reliability
- Define
  - Confidentiality
  - Integrity
  - Availability
    - Authenticity
    - Non-repudiation
- Give examples for
  - Confidentiality
  - Integrity
  - Availability

7

BASIC NOTIONS (2)

- Define the notions of
  - Vulnerability
  - Threat
  - Exploit
- Give examples of
  - Vulnerability
  - Threat
- Define the attribution problem
- Define the notion of risk
- Definition the notions of
  - Likelihood
  - Impact
  - Risk matrix

8

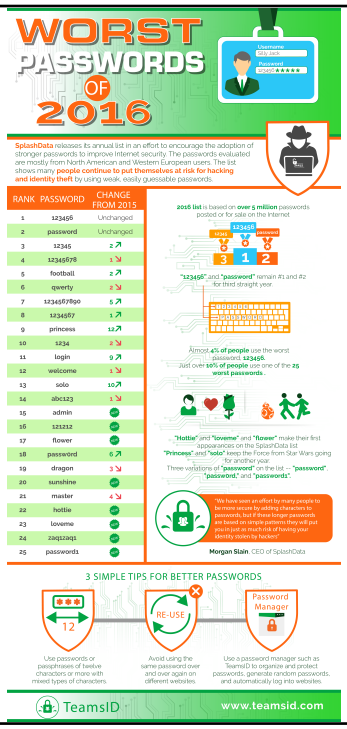
BASIC NOTIONS (3)

- What is a security policy?
- What is a security mechanism?
- What is a security service?
- How do security policies relate to Confidentiality, Integrity and Availability?
- Give examples of
  - Security policy
  - Security mechanism
  - Security service

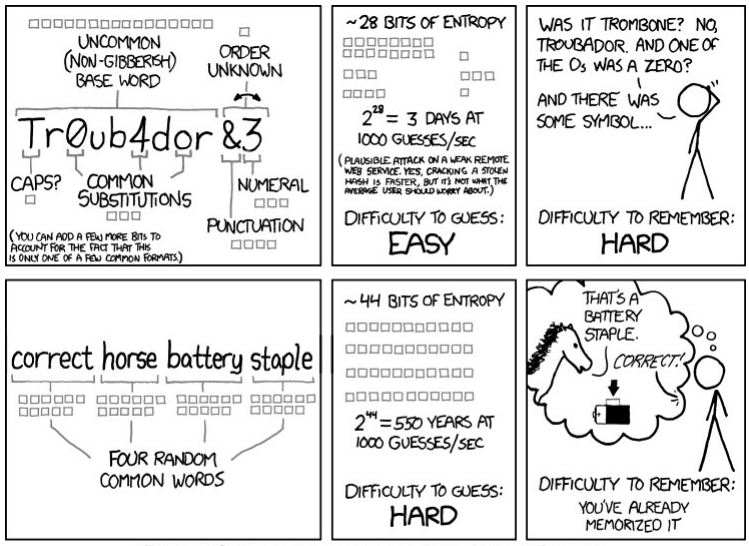
9

10

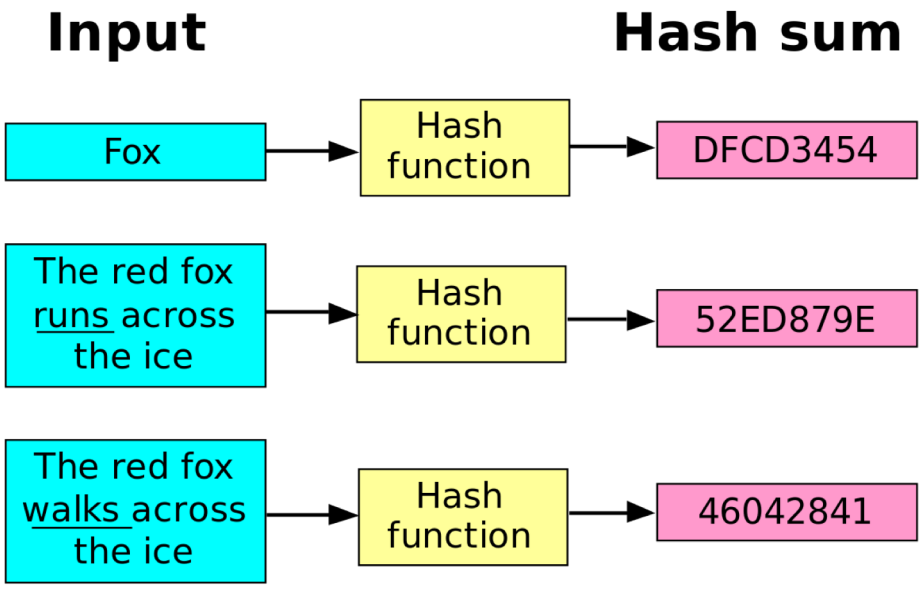
AUTHENTICATION



Issues with password based authentication deriving from a difficult trade-off between usability and security: users need to memorize a random string…

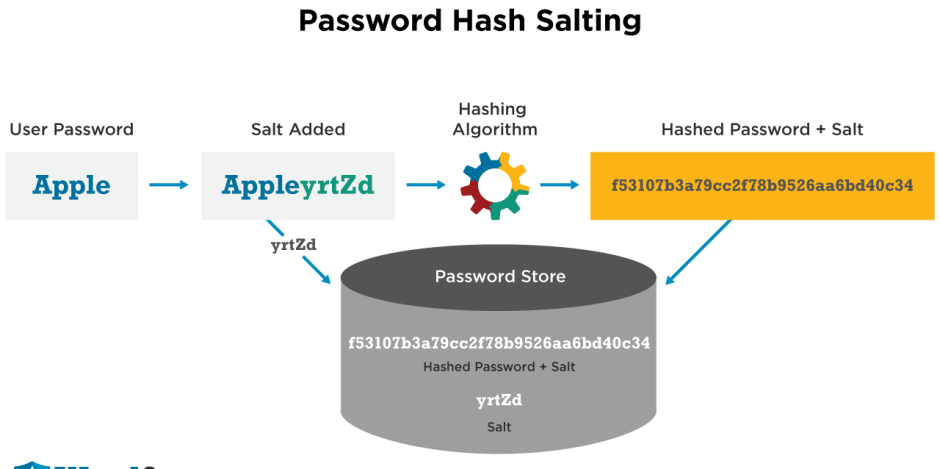


Besides these problems, passwords need to be protected when stored while allowing for easy verification… this is done by using a (keyless) cryptographic primitive to protect them!



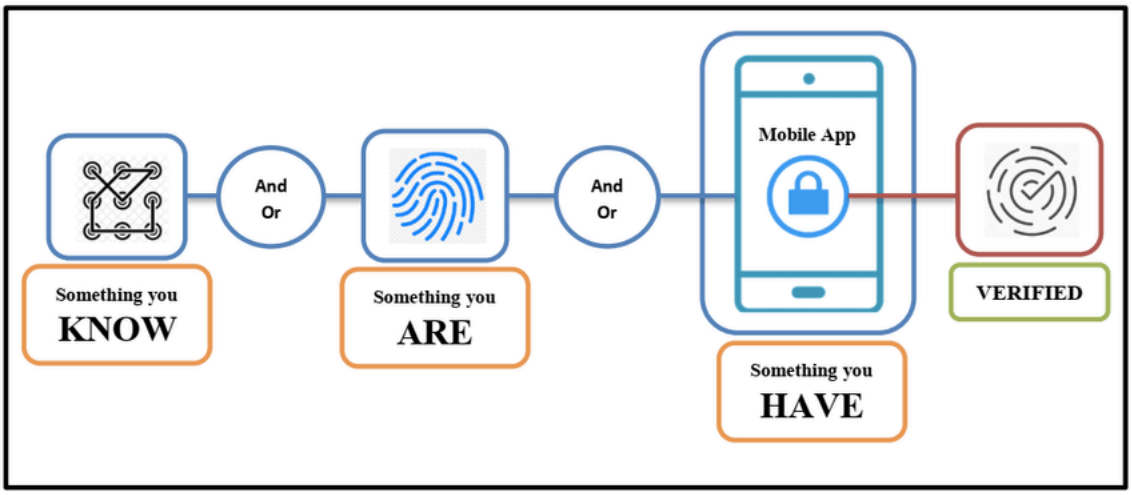
12

Unfortunately, hashing is not enough to protect from certain (typically offline) attacks (e.g., those based on rainbow tables (i.e. data structures storing large amounts of precomputed digests for most commonly used passwords). This is where salting comes in place but notice that it mitigates the attack (i.e. makes it very computationally expensive as it requires to recompute a table for every salt) without preventing it



13

Going beyond password based authentication… Multi Factor Authentication (MFA)



14

AUTHENTICATION (1)

- Define the notions of user
  - Authentication
  - Identification
    - (On-boarding/bootstrapping)
- In the context of password based authentication, describe how it is possible to perform a guessing attack; in particular
  - Brute force
  - Dictionary
- Define the three types of authentication factors and give examples
- In the context of password management, describe
  - Spoofing
  - Phishing
- Describe countermeasures to
  - Spoofing
  - Phishing

15

AUTHENTICATION (2)

- Define the notion of hash function and its main properties
  - Ease of computation
  - Compression
  - One-way
  - Weak collision resistance
  - Strong collision resistance
- Give an example of a weak and an example of a strong hash function available
- How do you protect a password file with hashing and salting
  - Explain what is salting and why it is needed besides hashing
  - Describe the structure of a password file
    - Can salts be stored in clear?
- Describe a credential stuffing attack
  - How organizations can mitigate this attack?

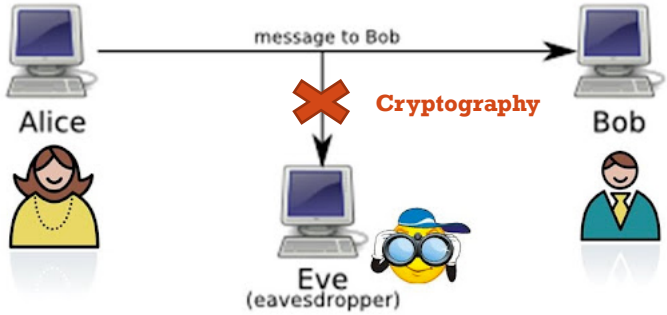
16

AUTHENTICATION (3)

- What is Multi Factor Authentication?
- How does Time-Based One-Time Password work?
- What is an authenticator?
- Describe the three assurance level for authentication
- What is a Single Sign On Experience?
- What are the pros and cons of Single Sign On?

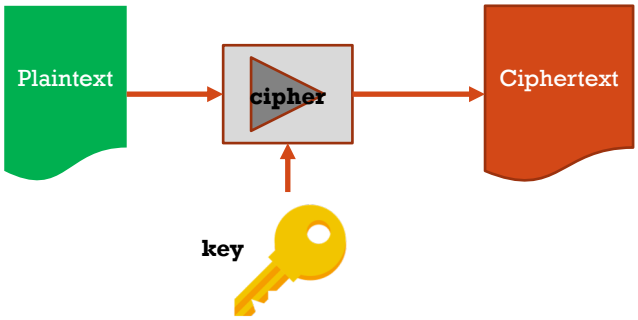
17

18 CRYPTOGRAPHY



Kerchhoff's principle

A cryptographic system should be secure even if everything about the system except the encryption key is public knowledge

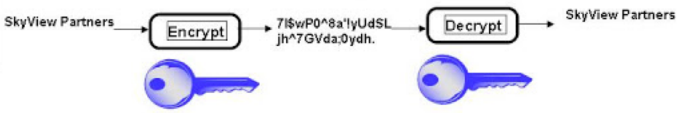


19

DES
TripleDES
AES
RC5

Symmetric Keys

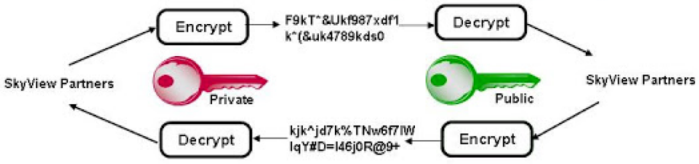
- Encryption and decryption use the **same key**.



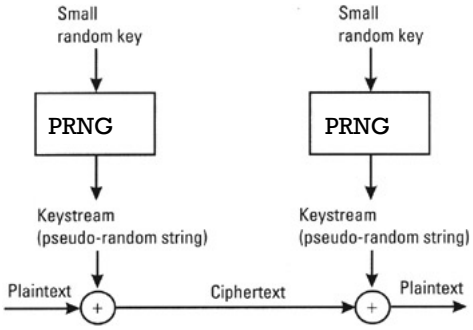
RSA
Elliptic Curve

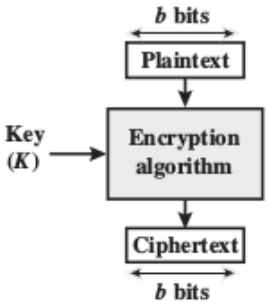
Asymmetric keys

- Encryption and decryption use different keys, a **public key** and a **private key**.



20

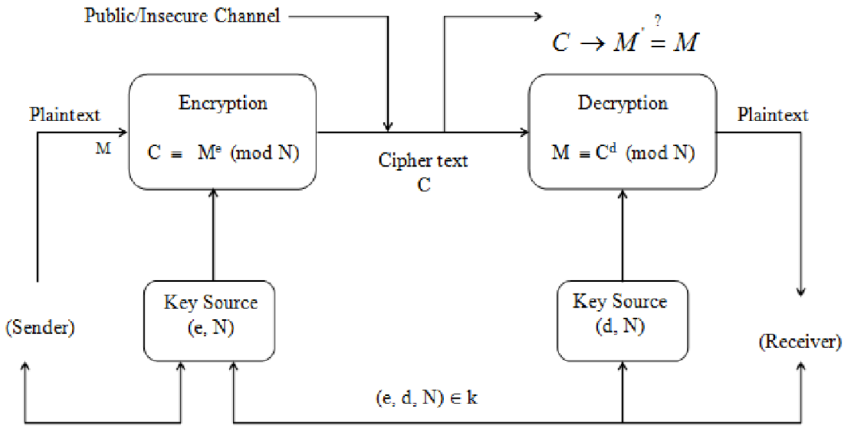




SYMMETRIC CIPHERS

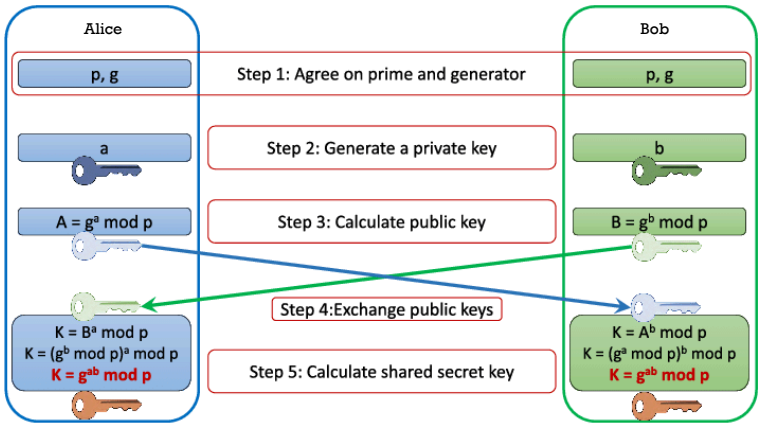
21

ASYMMETRIC CIPHERS: RSA



22

ASYMMETRIC CIPHERS: DH



23

CRYPTOGRAPHY (1)

- What are the properties that cryptography aim to guarantee and how?
  - Data confidentiality
  - Data integrity
  - Data origin authentication
- Define the notion of cryptosystem
- Explain the notion of computational difficulty in the context of cryptography
- Describe the Kerckhoffs principle
- What is the purpose of key management?
- Give an example of a substitution cipher
- Give an example of a transposition cipher

24

CRYPTOGRAPHY (2)

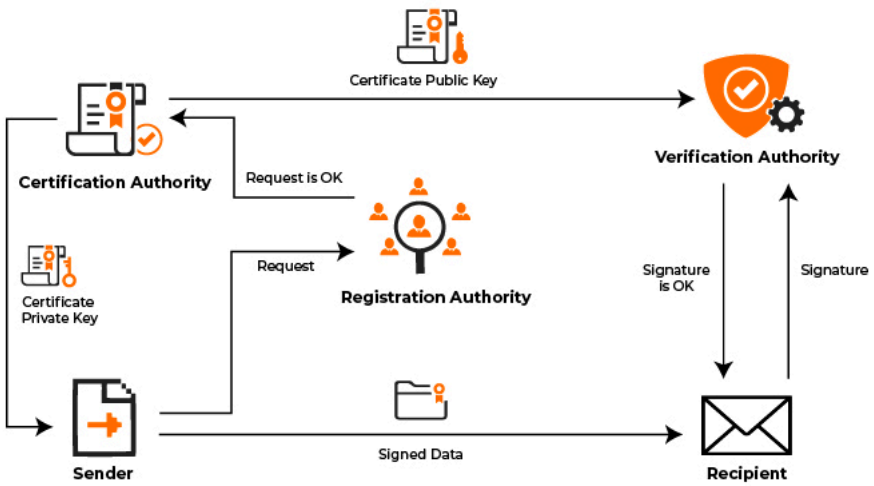
- Define the notion of symmetric key cryptography
- Describe two types of symmetric key cryptography:
  - Stream ciphers
  - Block ciphers
- What is DES? What is AES? How are they related?
- Define the notion of asymmetric or public key cryptography (PKC)
- Give two examples of PKC and on which mathematical problems they are based
- Describe the Diffie-Hellman key exchange protocol
- Describe the Men-In-the-Middle attack to the Diffie-Hellman protocol

25

26

APPLICATIONS OF CRYPTOGRAPHY

Public Key Infrastructure



27

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Aug  1 00:00:00 1996 GMT
            Not After : Dec 31 23:59:59 2020 GMT
        Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                 OU=Certification Services Division,
                 CN=Thawte Server CA/Email=server-certs@thawte.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d3:a4:50:6e:c0:ff:56:6b:e6:cf:5d:b6:ea:0c:
                    68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                    85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                    6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                    6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                    29:b6:2f:49:c0:3b:d4:27:04:25:10:97:2f:e7:90:
                    6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                    5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                    3a:c2:b5:66:22:12:d6:87:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8c:ca:d9:
        a0:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c0:40:
        3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
        4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
        8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
        e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
        b2:75:1b:f6:42:f2:cf:c7:f2:18:f9:89:bc:a3:ff:8a:23:2c:
        70:47
```


IMPORTANCE OF CERTIFICATES IN THE WEB: LET'S ENCRYPT (1)

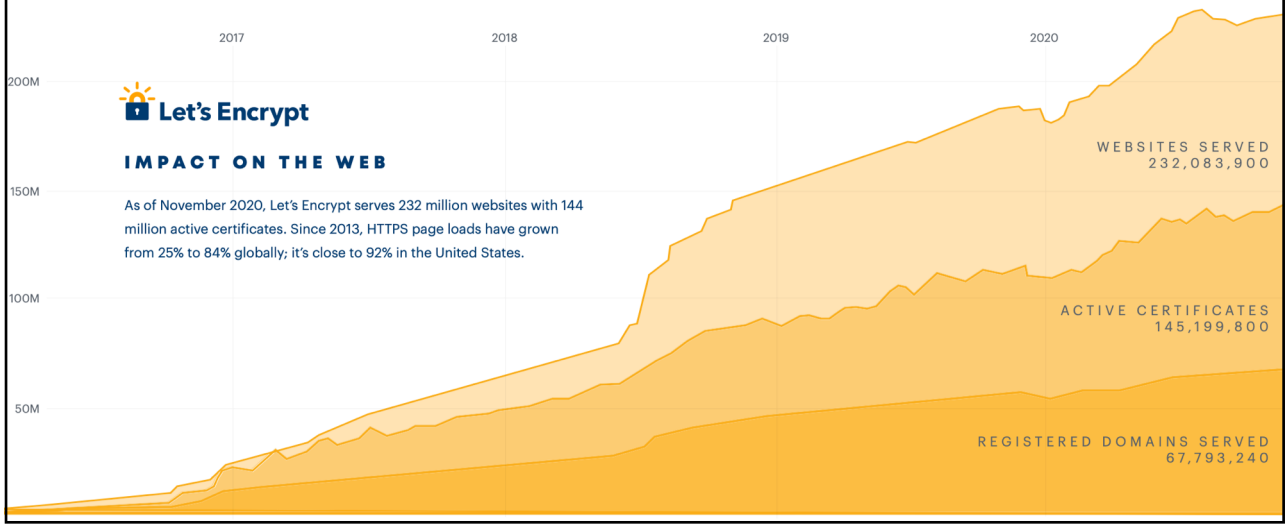
https://letsencrypt.org/

- Taken from https://www.abetterinternet.org/documents/2020-ISRG-Annual-Report.pdf

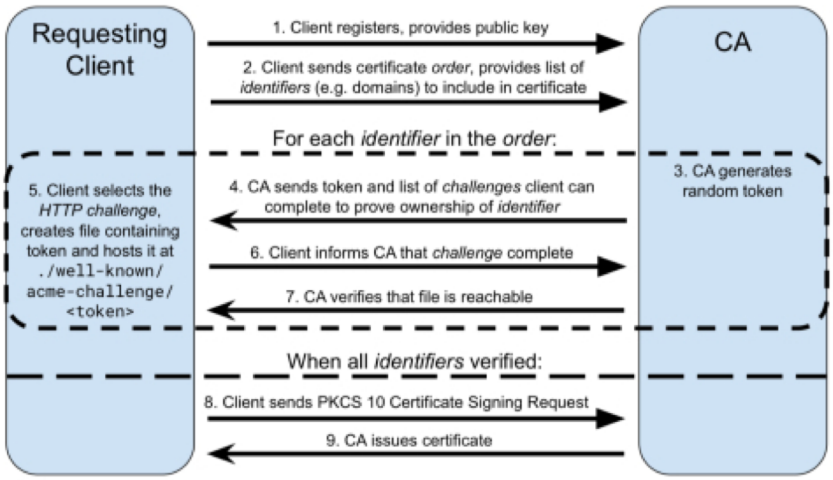
HTTPS has been around since the mid-90s but uptake was abysmally slow because SSL/TLS certificates weren't easy to get or manage. Let's Encrypt made getting and managing certificates easy and as a result HTTPS adoption rates shot up. Critically, the answer wasn't to get people to think more about their certificates—we needed to make it possible for people to spend much less time thinking about certificates. Ideally we'd be invisible—server software should just get and manage certificates automatically.

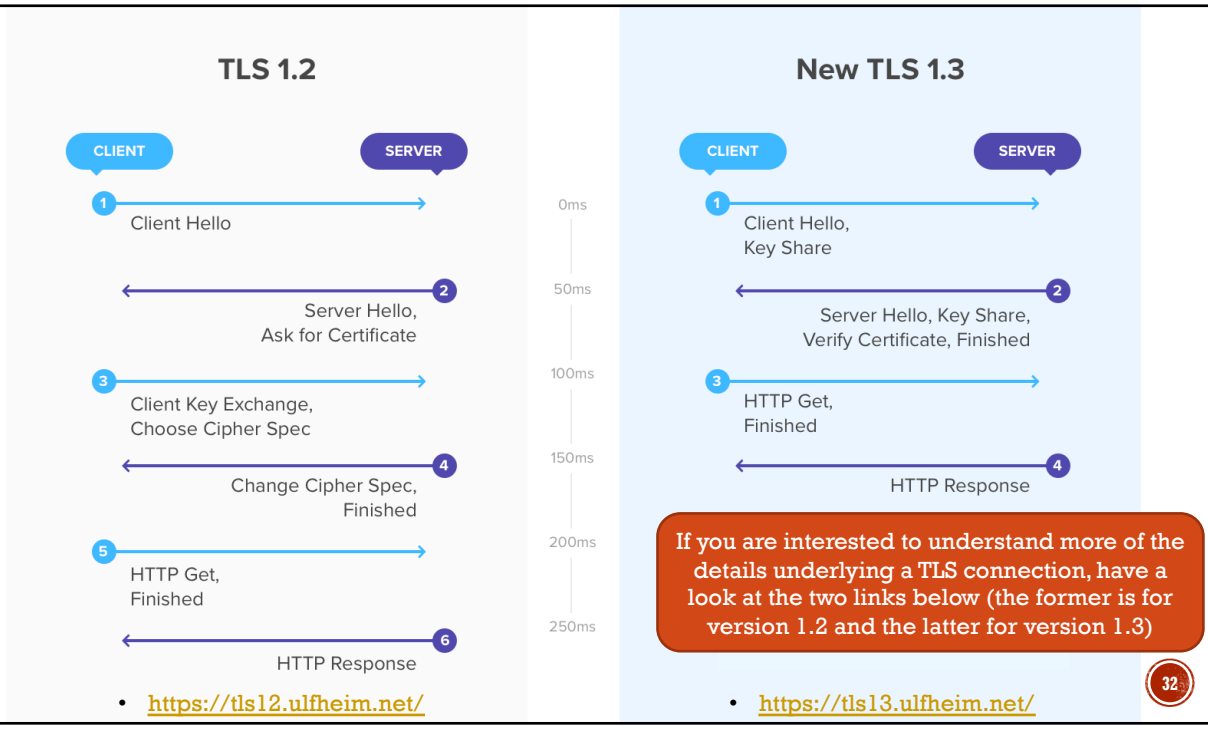
IMPORTANCE OF CERTIFICATES IN THE WEB: LET'S ENCRYPT (2)

https://letsencrypt.org/



HOW TO OBTAIN A CERTIFICATE: DOMAIN VALIDATION





- https://tls12.ulfheim.net/
- https://tls13.ulfheim.net/

APPLICATIONS OF CRYPTOGRAPHY (1)

- With Public Key Cryptography, how can data confidentiality, data integrity, and data origin authenticity be guaranteed?
- What is a digital certificate and what are its main components?
- Describe the purpose and main components of a Public Key Infrastructure (PKI)
  - Describe the process of obtaining a certificate
- What is the main purpose of TLS?
- How are SSL and TLS related?
- Give a high level characterization of the protocols composing TLS?

33

APPLICATIONS OF CRYPTOGRAPHY (2)

- Describe the TLS 1.2 handshake protocol by drawing a message sequence chart and giving a brief description of each step
- How does TLS provide
  - Authentication
  - Confidentiality
  - Integrity ?
- Give two examples of TLS vulnerabilities
- Describe how TLS 1.2 and TLS 1.3 differ in particular concerning
  - Handshake
  - Cipher suites

FINAL REMARK

- Passwords and TLS are crucial pre-requisite in many use case scenarios and in particular in web services and applications
- TLS secures the exchange between a client and a server, in addition it authenticates the server to the client but not *vice versa*
- At that point, for the service to authenticate the user, it asks for providing credentials (passwords plus possibly other authentication procedure) and goes through an authentication process
- The client enters user name and credentials in the client that sends them (passwords are hashed and salted) to the server over the secure TLS channel
  - If a TLS channel is not in place, it would be like not having a password protecting the account
- The server gets such an information and uses it as discussed (retrieving the salt and digest with the user name from the database and then comparing them with the received information)

A RECENT AND TIMELY NEWS (1)

- To whom is associated the Greenpass QR code on the right?
  - *Adolf Hitler…*
- Have a look at the news if you have not yet read it, e.g., at

https://www.ansa.it/english/news/general_news/2021/10/27/eu-green-pass-generation-keys-stolen-sources_e231d1e5-8eab-429b-ae6d-c70991469d41.html

- It seems that the private keys used to sign the QR codes have been stolen (from authorities in France and Poland) but there are other possibilities such as the template code for the EU Digital COVID Certificate Issuance Web Frontend contains default authentication credentials that some Member State deploying it has not changed in operation…
- Do you think this can be considered only a joke or is it something to take seriously?
- What should be done?
- What are the potential consequences of the mitigations (if any)?

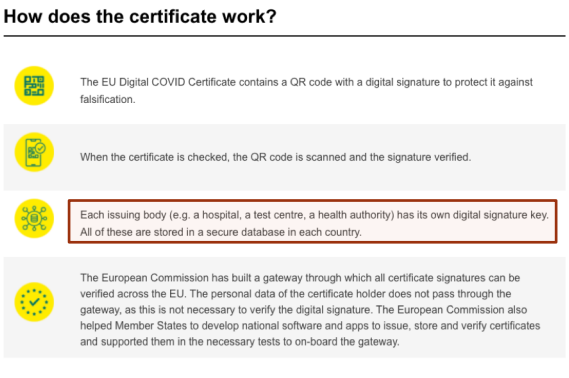
36

A RECENT AND TIMELY NEWS (2)

- If you want to read more about the European Greenpass

https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

- For more technical documents, see
  - https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v1_en.pdf
  - https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v2_en.pdf



37