Economic and Social Commission for Western Asia

THE IMPLICATIONS OF ENCRYPTION IN PUBLIC POLICIES

UNITED NATIONS

الاسكوا

ESCWA

Shared Prosperity Dignified Life

AICTO

Internet Society

ITU

AGENDA

1. We are Internet Society
2. The context
3. What is encryption?
4. How does the encryption work?
5. Why and when do we use encryption?
6. Myth busting
7. Encryption and public policies

Date

Presentation Title

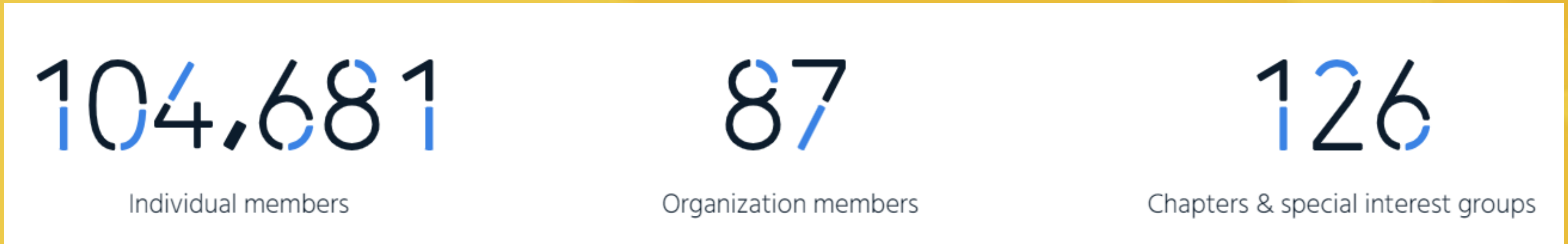
Subtitle or Supporting Information

Internet Society

Author’s Name
Title
email

Internet
Society

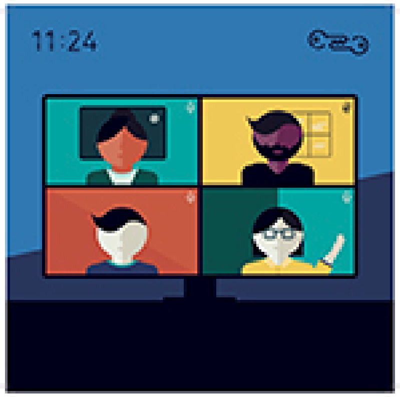
Our work ensures that the Internet thrives and that everyone can benefit from it.



104,681	87	126
Individual members	Organization members	Chapters & special interest groups

https://www.internetsociety.org/become-a-member/

The big why



17:44

Home early today - you ask your personal assistant to report on stock prices and work on your personal portfolio.

company 2.5 million.

concluded

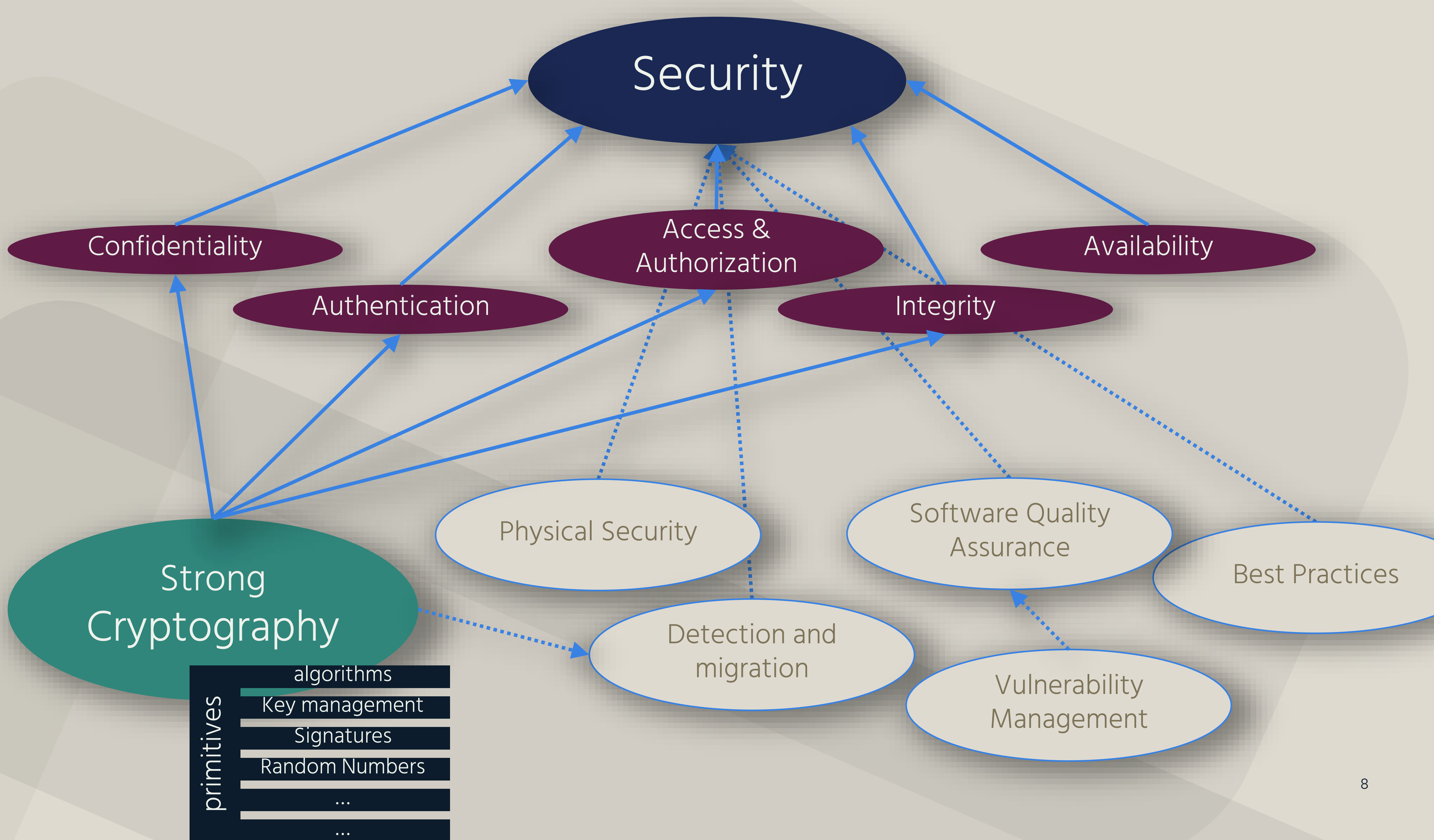
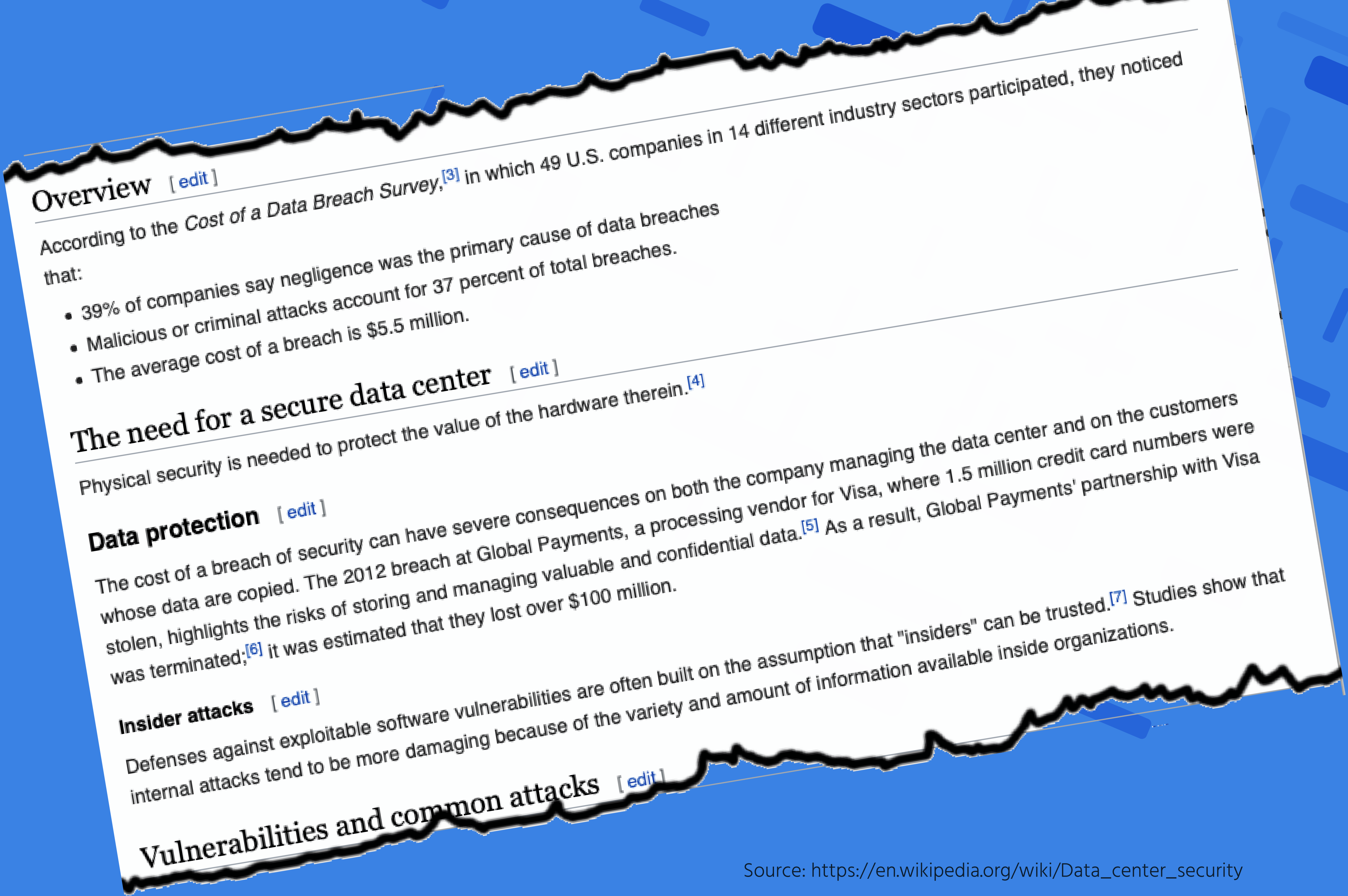

Security
Confidentiality
Authentication
Access &
Authorization
Integrity
Availability
Physical Security
Software Quality
Assurance
Best Practices
Strong
Cryptography
Detection and
migration
Vulnerability
Management
primitives
algorithms
Key management
Signatures
Random Numbers
…
…

Photo by Taylor Vick on Unsplash



Overview [edit]

According to the *Cost of a Data Breach Survey*,[3] in which 49 U.S. companies in 14 different industry sectors participated, they noticed that:

- 39% of companies say negligence was the primary cause of data breaches
- Malicious or criminal attacks account for 37 percent of total breaches.
- The average cost of a breach is $5.5 million.

The need for a secure data center [edit]

Physical security is needed to protect the value of the hardware therein.[4]

Data protection [edit]

The cost of a breach of security can have severe consequences on both the company managing the data center and on the customers whose data are copied. The 2012 breach at Global Payments, a processing vendor for Visa, where 1.5 million credit card numbers were stolen, highlights the risks of storing and managing valuable and confidential data.[5] As a result, Global Payments' partnership with Visa was terminated;[6] it was estimated that they lost over $100 million.

Insider attacks [edit]

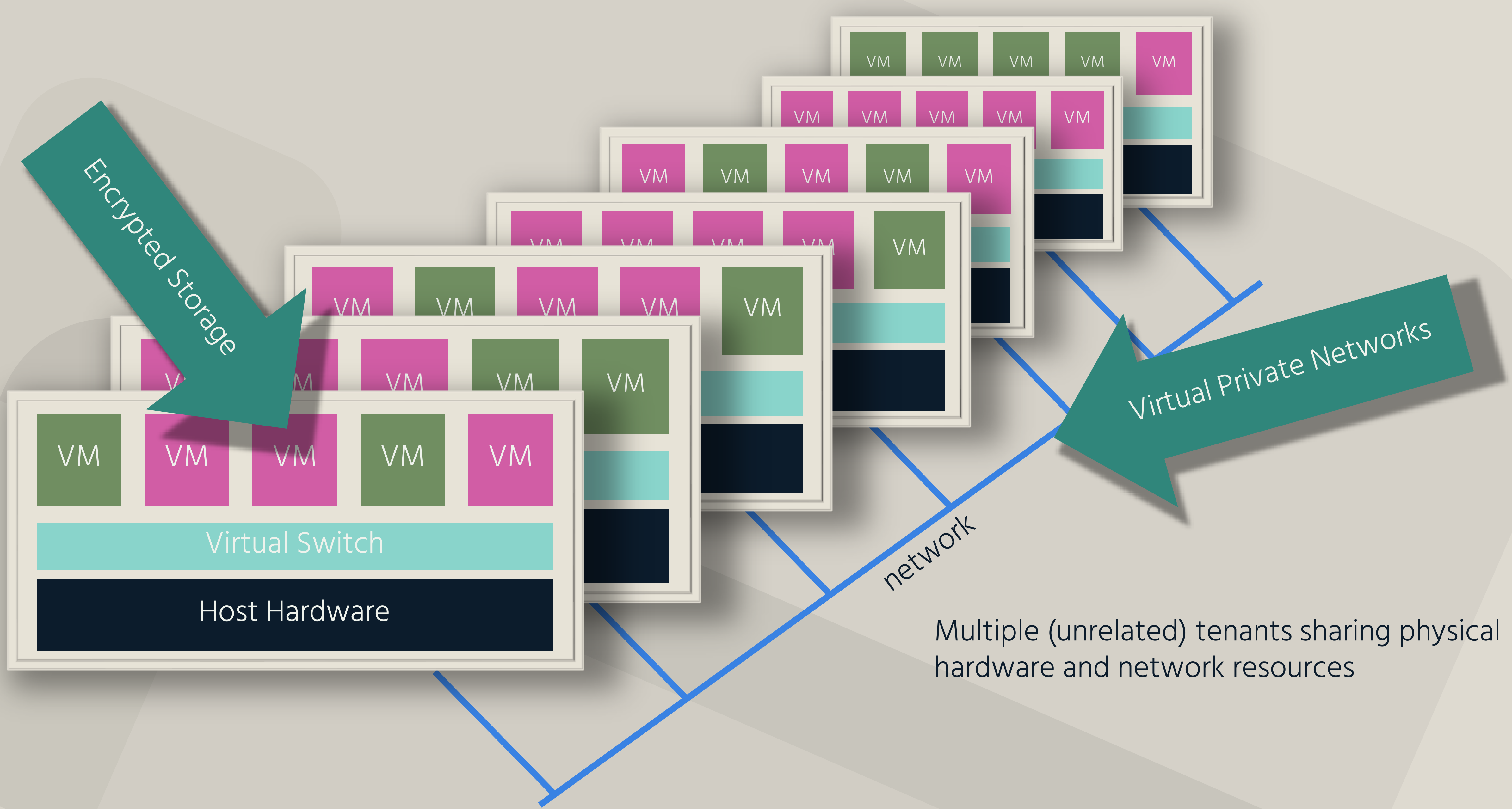
Defenses against exploitable software vulnerabilities are often built on the assumption that "insiders" can be trusted.[7] Studies show that internal attacks tend to be more damaging because of the variety and amount of information available inside organizations.

Vulnerabilities and common attacks [edit]

Source: https://en.wikipedia.org/wiki/Data_center_security

Virtualized environments exacerbate cryptographic issues by sharing of channels or resources. In particular, man- in-the-middle attacks become highly critical in virtualized environments, where messages from different tenants may share the same channel or infrastructure facilities.

ENISA 2017: Security aspects of virtualization



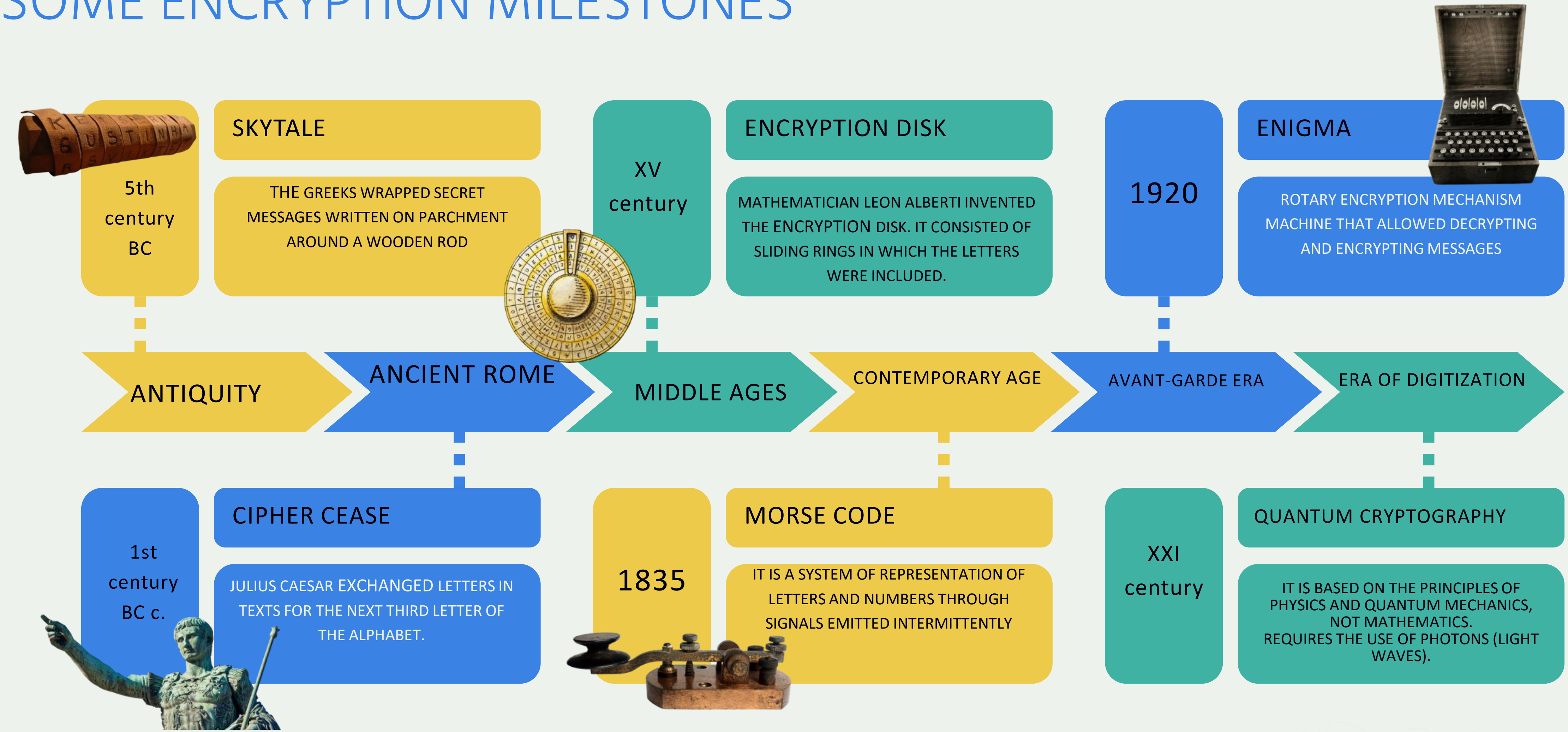
Multiple (unrelated) tenants sharing physical hardware and network resources

Zero Trust Security Design

How ‘bout the web?

WHAT IS ENCRYPTION?

SOME ENCRYPTION MILESTONES



ANTIQUITY

5th century BC

SKYTALE

THE GREEKS WRAPPED SECRET MESSAGES WRITTEN ON PARCHMENT AROUND A WOODEN ROD

ANCIENT ROME

1st century BC c.

CIPHER CEASE

JULIUS CAESAR EXCHANGED LETTERS IN TEXTS FOR THE NEXT THIRD LETTER OF THE ALPHABET.

MIDDLE AGES

XV century

ENCRYPTION DISK

MATHEMATICIAN LEON ALBERTI INVENTED THE ENCRYPTION DISK. IT CONSISTED OF SLIDING RINGS IN WHICH THE LETTERS WERE INCLUDED.

CONTEMPORARY AGE

1835

MORSE CODE

IT IS A SYSTEM OF REPRESENTATION OF LETTERS AND NUMBERS THROUGH SIGNALS EMITTED INTERMITTENTLY

AVANT-GARDE ERA

1920

ENIGMA

ROTARY ENCRYPTION MECHANISM MACHINE THAT ALLOWED DECRYPTING AND ENCRYPTING MESSAGES

ERA OF DIGITIZATION

XXI century

QUANTUM CRYPTOGRAPHY

IT IS BASED ON THE PRINCIPLES OF PHYSICS AND QUANTUM MECHANICS, NOT MATHEMATICS.
REQUIRES THE USE OF PHOTONS (LIGHT WAVES).

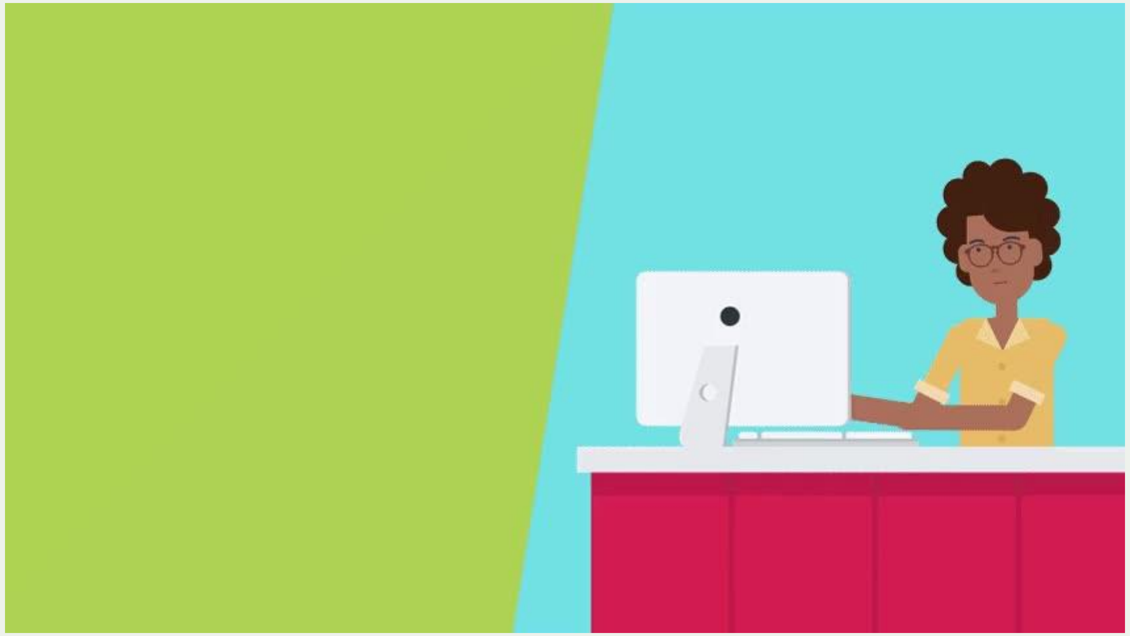
WHAT IS ENCRYPTION?

It is the process of encoding or encrypting data so that it can only be read by someone who has the means to return it to its original state.

It is a crucial feature of a secure, reliable Internet and helps ensure the safety of sensitive data.

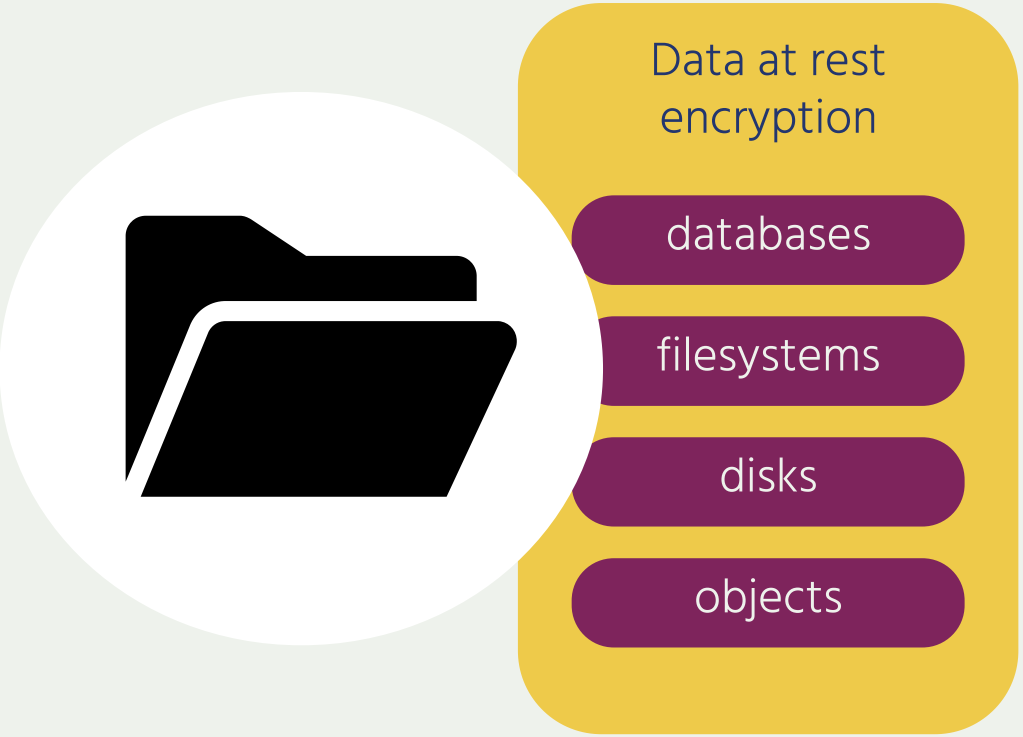
WHAT IS ENCRYPTION?

Encrypts the data, using an encryption key. It requires the correct key to convert the encrypted data back to the original "decrypt" format.



DATA-AT-REST ENCRYPTION

Data “*at rest*” is data that is stored somewhere—on a mobile device, laptop, server, or external hard drive, for example. When data is at rest, it doesn't move from one place to another. But needs protection anyway.



Data at rest encryption

databases

filesystems

disks

objects

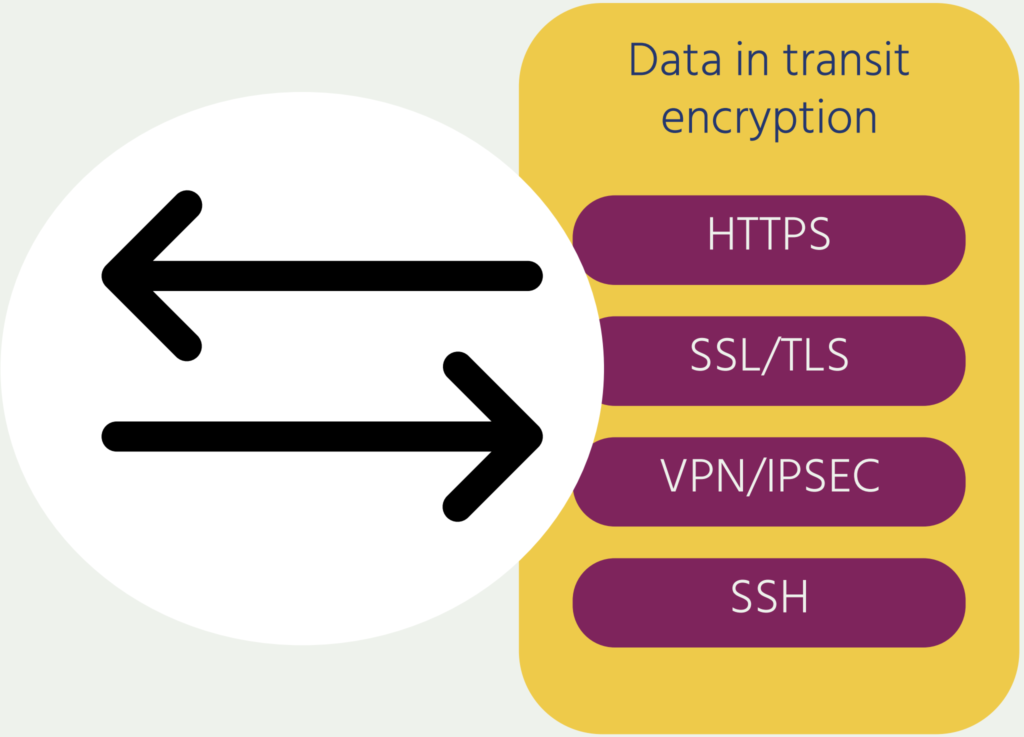
DATA-AT-REST ENCRYPTION

An example of a form of encryption that protects data at rest is "*full disk*" encryption.

Enabling Full Disk Encryption encrypts all information stored on a device and protects the information with a passphrase or other authentication method. On a mobile or laptop device, this often resembles a typical device lock screen, requiring a passkey, passphrase, or fingerprint.

ENCRYPTION OF DATA IN TRANSIT

Data *"in transit"* is the information that is moving through the network from one place to another. When you send a message using a messaging app, for example, that message moves from your device, to the app company's servers, to your recipient's device. Another example is web browsing: when you go to a website, data from that web page travels from the website's servers to your browser.


Data in transit encryption

HTTPS

SSL/TLS

VPN/IPSEC

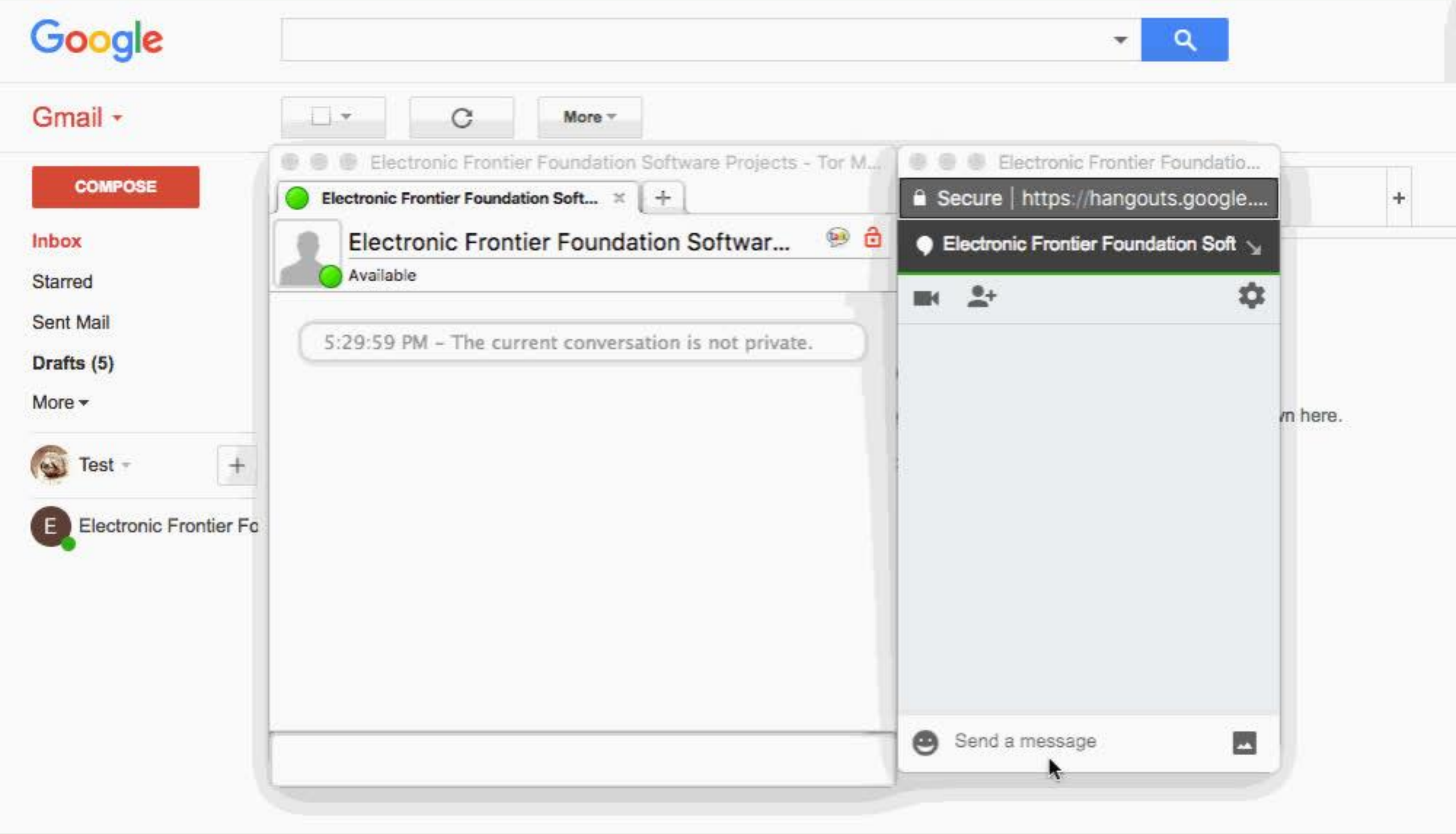
SSH

END-TO-END ENCRYPTION

Protect messages in transit from sender to receiver. It ensures that the information is converted into a secret message by its original sender (the first "end") and that it is only decrypted by its final recipient (the second "end").

No one, including the app you are using, can "listen" and access your activity.

END-TO-END ENCRYPTION


Google
Gmail
COMPOSE
Inbox
Starred
Sent Mail
Drafts (5)
More
Test
Electronic Frontier Fo
More
Electronic Frontier Foundation Software Projects - Tor M...
Electronic Frontier Foundation Soft...
Electronic Frontier Foundation Softwar...
Available
Electronic Frontier Foundatio...
Secure | https://hangouts.google....
Electronic Frontier Foundation Soft
Send a message
n here.

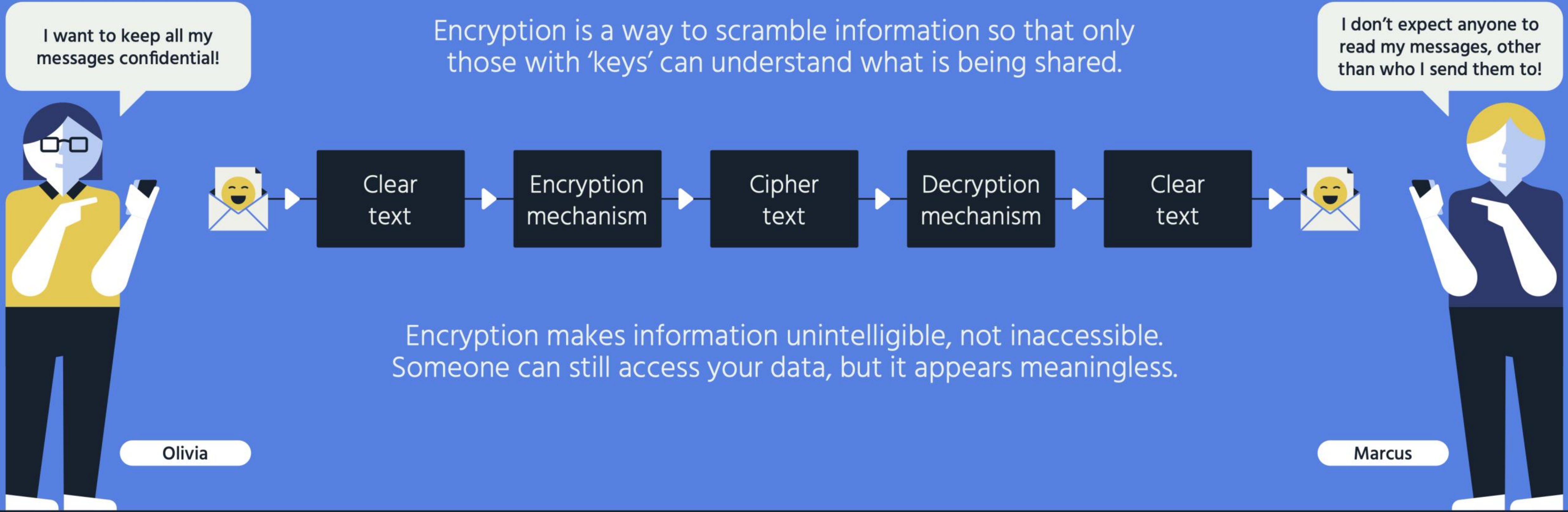
5:29:59 PM – The current conversation is not private.

HOW DOES THE ENCRYPTION WORK?

01 What is encryption?

Internet Society

Encryption is a way to scramble information so that only those with ‘keys’ can understand what is being shared.


I want to keep all my messages confidential!
I don’t expect anyone to read my messages, other than who I send them to!
Olivia
Marcus

Clear text → Encryption mechanism → Cipher text → Decryption mechanism → Clear text

Encryption makes information unintelligible, not inaccessible. Someone can still access your data, but it appears meaningless.

The importance of encryption

In our increasingly digital lives, the role of encryption has never been more essential.

Encryption is a crucial feature of a safe Internet. It ensures your private messages stay private.

From video calls to air traffic control and e-voting, encryption is vital for securing all aspects of our lives.

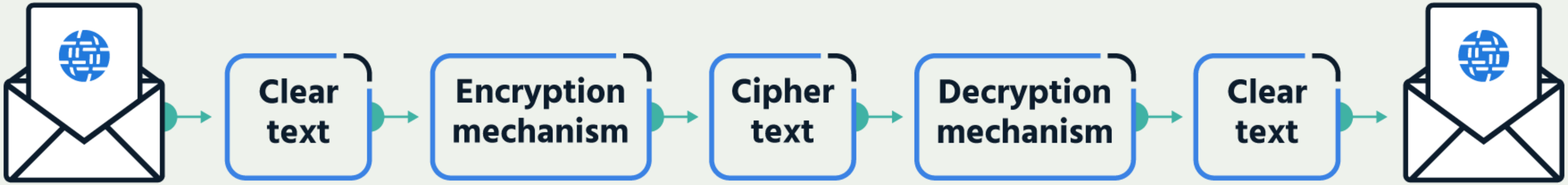
It keeps your identity safe and stops people from impersonating you, or the people that you trust.

It is critical to national security, protecting society from terrorists, criminals, and hostile governments.

Personal security depends on encryption. It keeps your confidential data out of the hands of criminals.

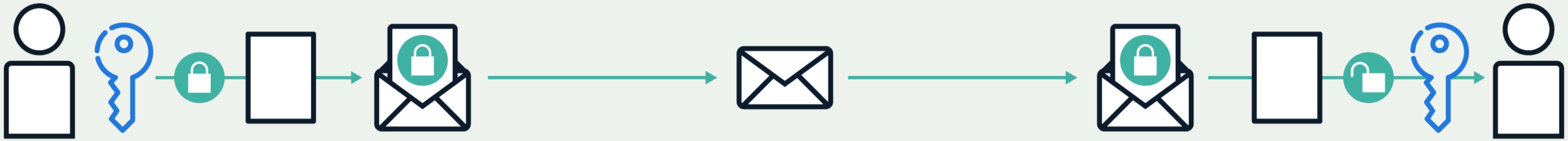
What is Encryption?

Encryption is a way to scramble information so that only those with “keys” can understand what is being shared.

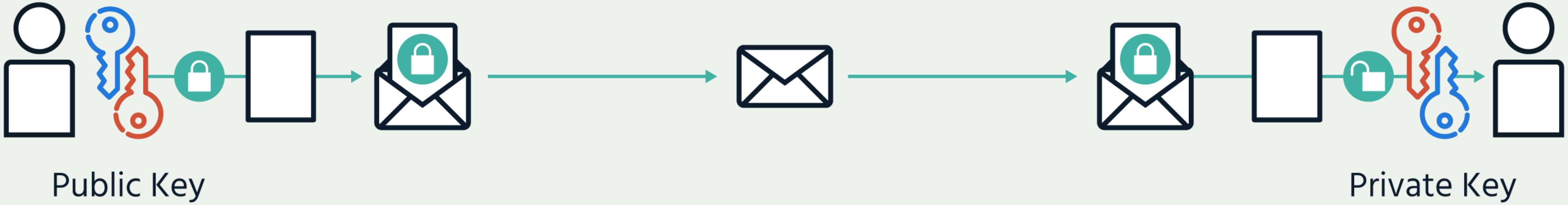


Encryption makes information unintelligible, not inaccessible. Someone can still access your data, but it appears meaningless.

Symmetric Encryption



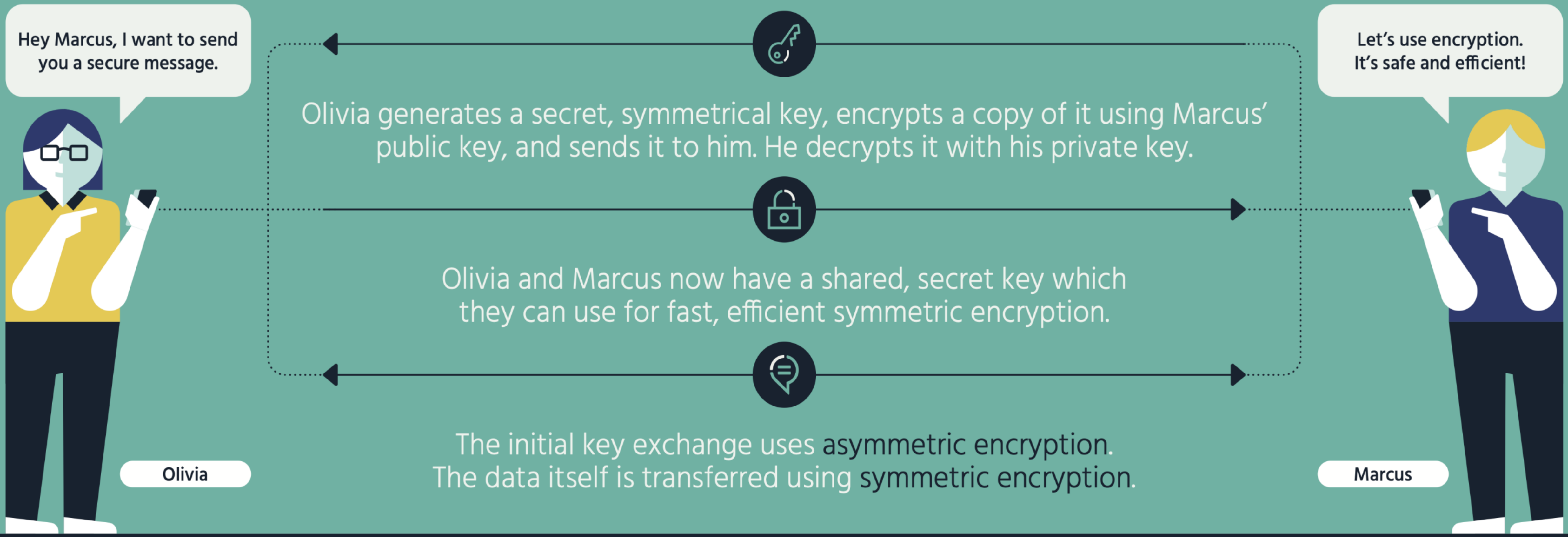
Asymmetric Encryption



In both cases, encryption is a reversible process, but in the case of symmetric encryption, it is reversible using the same key.
With asymmetric encryption, reversing the process with the same key does not produce the clear text.

02 How does encryption work?

Internet Society


Hey Marcus, I want to send you a secure message.
Let's use encryption. It's safe and efficient!
Olivia
Marcus

Each user has two keys: a public one and private one. Olivia finds Marcus' public key and copies it to her device.

Olivia generates a secret, symmetrical key, encrypts a copy of it using Marcus' public key, and sends it to him. He decrypts it with his private key.

Olivia and Marcus now have a shared, secret key which they can use for fast, efficient symmetric encryption.

The initial key exchange uses asymmetric encryption. The data itself is transferred using symmetric encryption.

Different types of encryption

Not all encryption is equal. The best systems balance safety and efficiency.

Symmetric encryption is like a cash box, where all users have the same secret key to see what's inside.

✓ Fast and efficient

✗ Vulnerable to interception

With asymmetric encryption each user has their own public and private keys, providing additional security.

✓ Safe and secure

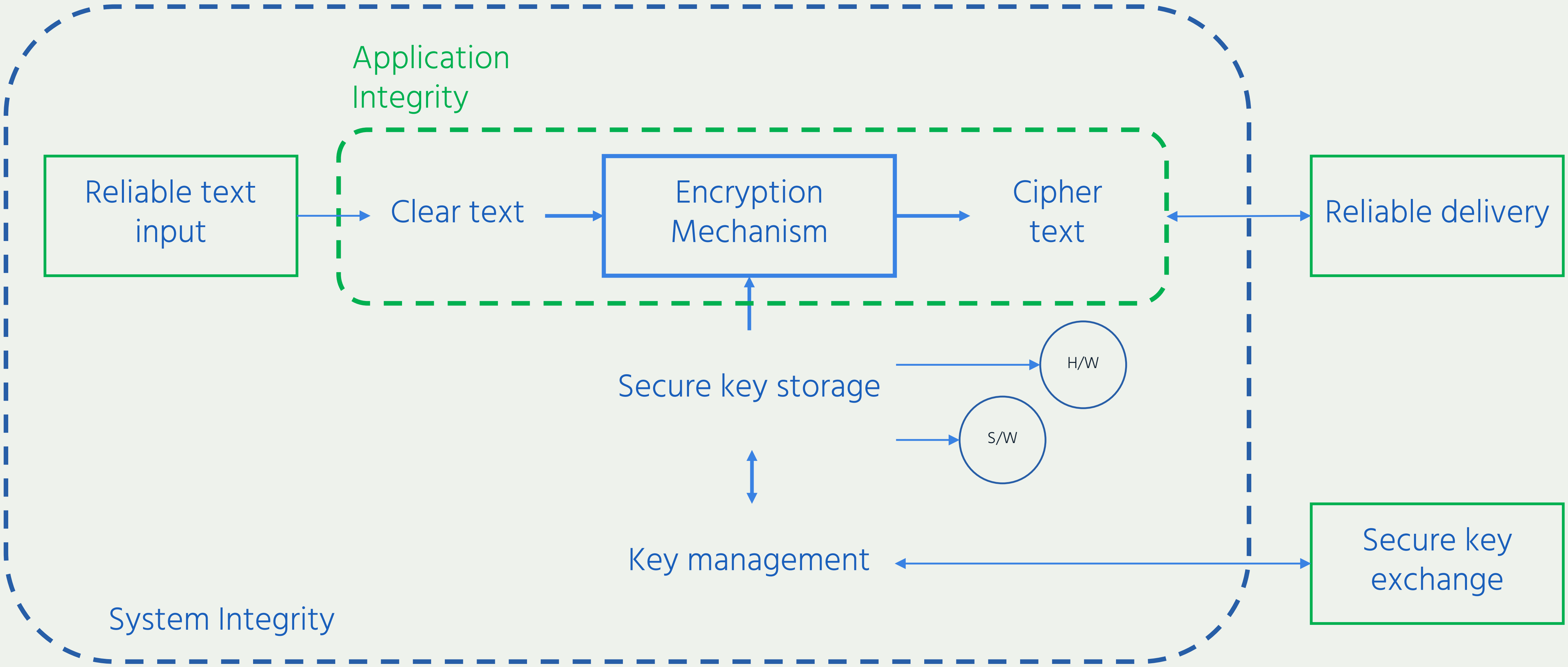
✗ Complexity means less efficiency

In hybrid systems, a mixture of encryption processes provides the best of both worlds. Asymmetric encryption is used for a secure key exchange, with the more efficient system of symmetric encryption used to transfer the data itself.

✓ Safe and secure

✓ Fast and efficient

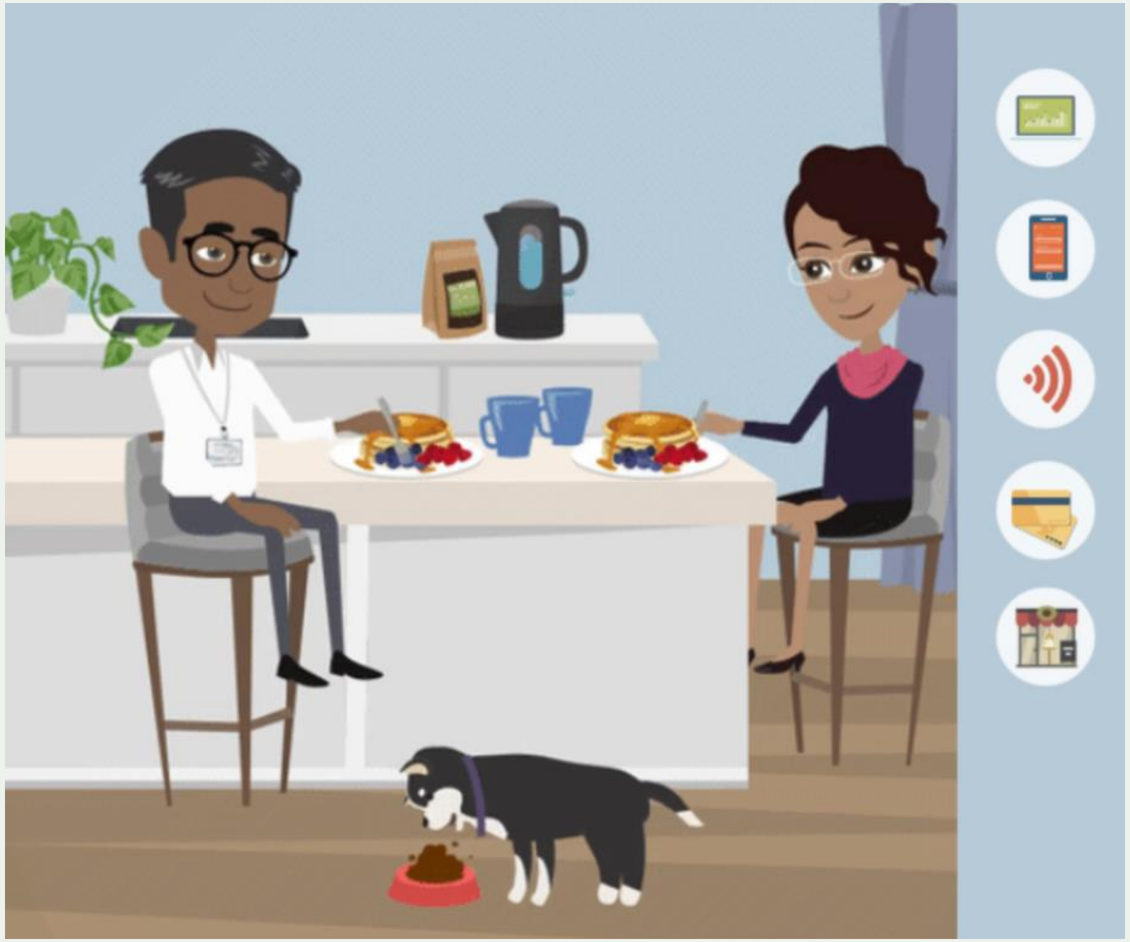
Thinking of Encryption as a System



And now… a game

WHY AND WHEN DO WE USE ENCRYPTION?

ENCRYPTION EVERY DAY



- Leila starts the day by checking a news website for the traffic report. There is a lock icon in the search bar indicating that the site uses HTTPS, a type of security encryption.

- Next, Leila uses Signal to send a text message to her friend, and they choose a place to eat. By using Signal, Leila knows that her messages are "end-to-end" encrypted, meaning only she and her friend can read them.

- While having lunch, Leila connects to her private hotspot to check her email. Luckily, your access point is encrypted, which prevents others from using it as well.

- Leila pays for lunch with her credit card, which has three encryption points: the card's chip, the credit card reader, and while the credit card information was being transmitted to authorize the purchase.

- Gerald on the other hand, orders dinner using one of the apps on his phone. Good thing the transaction data used to pay online is protected by encryption.

WHEN DO WE USE ENCRYPTION?

It is commonly used to protect data stored on systems and data transmitted over computer networks, including the Internet. Financial transactions and private messaging communications that use encryption to increase security.

WHY DO WE USE ENCRYPTION?

The Roman emperor Julius Caesar used it to hide his war secrets, he made them so that each unencrypted letter was moved three letters later; this is what is known as *Caesar cipher*.

Plain text
Asterix and Obelix are hiding behind the bushes

Encrypted Text
Dvwhula dqg Rehola duh klglqj ehklqg wl
exvkhv

WHY DO WE USE ENCRYPTION?

Through encryption we take care of our content, from photos, videos, text messages, chat conversations, documents, contacts, bank transactions, payments and more.

The amount of information we store on our devices is increasing, and it is also becoming more sensitive. Therefore, it becomes an essential task to protect it from the various risks that exist.

Myth busting

MYTHS ABOUT ENCRYPTION AND PRIVACY

WHO IS GOING TO WANT TO ATTACK ME?

Sometimes users do not encrypt their data because they have read on the Internet about the weaknesses of using such encryption. Sometimes these weaknesses are myths, or simply no longer true with the advancement of technology.

Let's review some of the most well-known myths about data encryption.

MYTHS ABOUT ENCRYPTION AND PRIVACY

Data encryption reduces speed: this myth is one of the most widespread, it is true that if we have old hardware we will notice that the reading and writing speed is slower than if the data were not encrypted.

Data encryption increases the load on equipment and servers: if we have updated hardware, we will see that the load is exactly the same as if the data did not travel encrypted.

MYTHS ABOUT ENCRYPTION AND PRIVACY

Using encryption on websites (HTTPS) slows down browsing.

The first time we access a web page, it is true that it is somewhat slower, around 10%, since the TLS protocol must "agree" the encryption parameters with the browser, but once the page has loaded for the first time, subsequent requests to the same website will be as fast as HTTP.

MYTHS ABOUT ENCRYPTION AND PRIVACY

Mobile phones don't need antivirus:

There are dozens of reasons to install a good security solution on your smartphone or tablet (the data and information you store on these devices is usually particularly sensitive), but the proliferation of threats for Android and iOS , an inevitable consequence of its popularity, is the most forceful. To prevent your mobile from being hijacked by the dreaded ransomware, for example, your best ally will be an antivirus.

MYTHS ABOUT ENCRYPTION AND PRIVACY

If I use an encryption tool, I am exempt from any risk:

Although encryption tools protect our data, they do not have super powers, and if our equipment lacks other protections, what we take care of with encryption can be lost due to other weaknesses. For example, I use a tool like E2E (end to end encryption) on my mobile phone but no I have no screen saver or tool to lock my screen and anyone can read my chats if I'm not close to him.

ENCRYPTION AND PUBLIC POLICIES

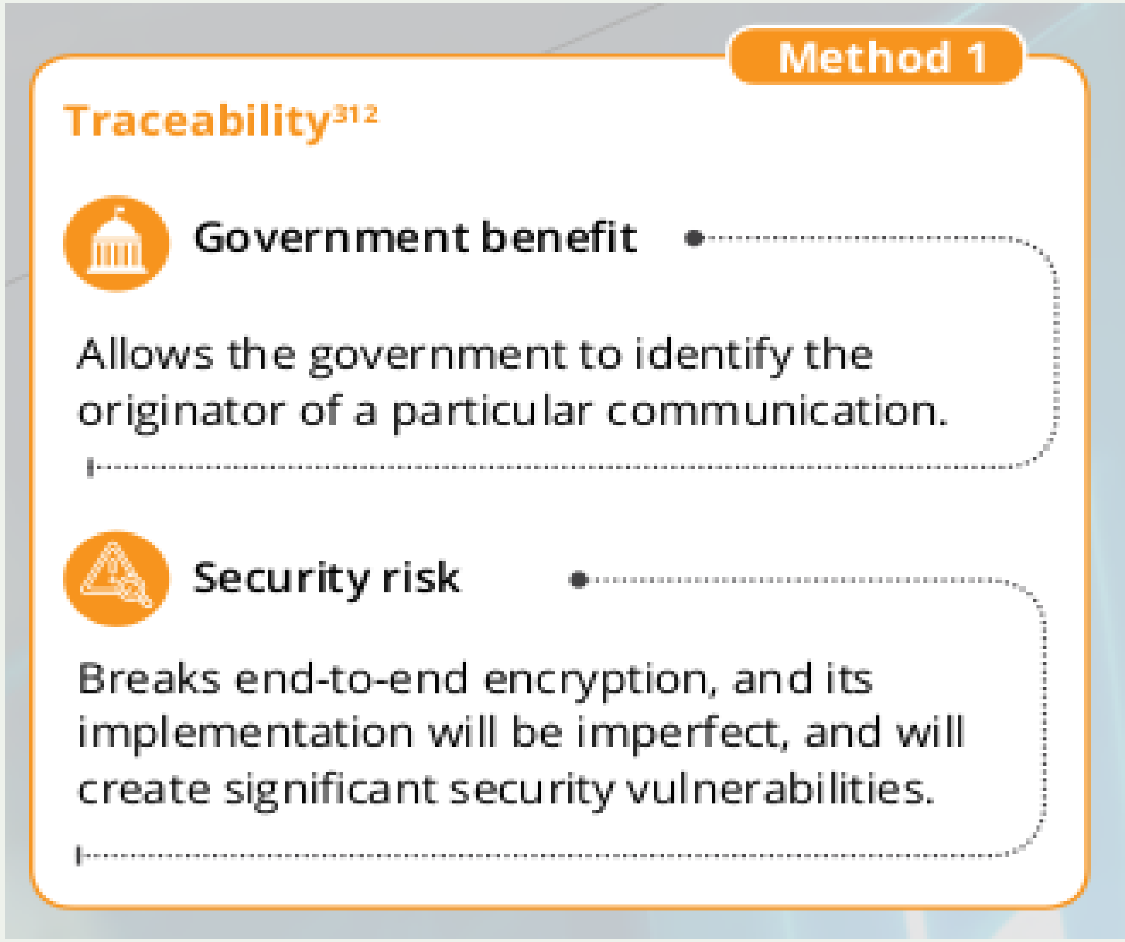
Encryption protects all people – The math is the same

Law enforcement wants access to devices and online platforms to stop the spread of child abuse and terroristic content

There are many cases of legislators, politicians and government entities, whose devices and online platforms have been hacked and monitored by external actors.

Although we all want to prevent crime on the Internet, there is simply no magic key that gives the "good guys" access without making sensitive user data available to anyone who wants it, including criminals

ENCRYPTION DEBATE



Method 1

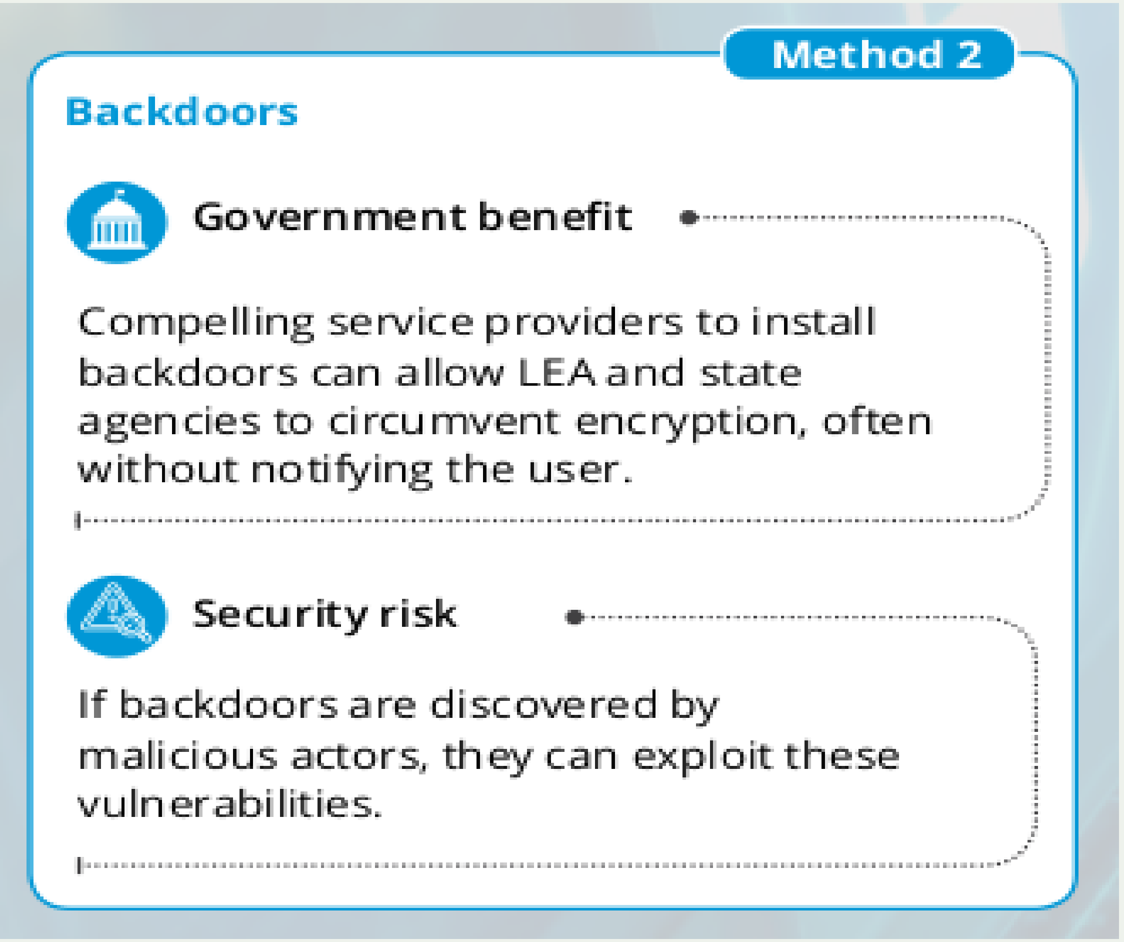
Traceability[312]

Government benefit

Allows the government to identify the originator of a particular communication.

Security risk

Breaks end-to-end encryption, and its implementation will be imperfect, and will create significant security vulnerabilities.



Method 2

Backdoors

Government benefit

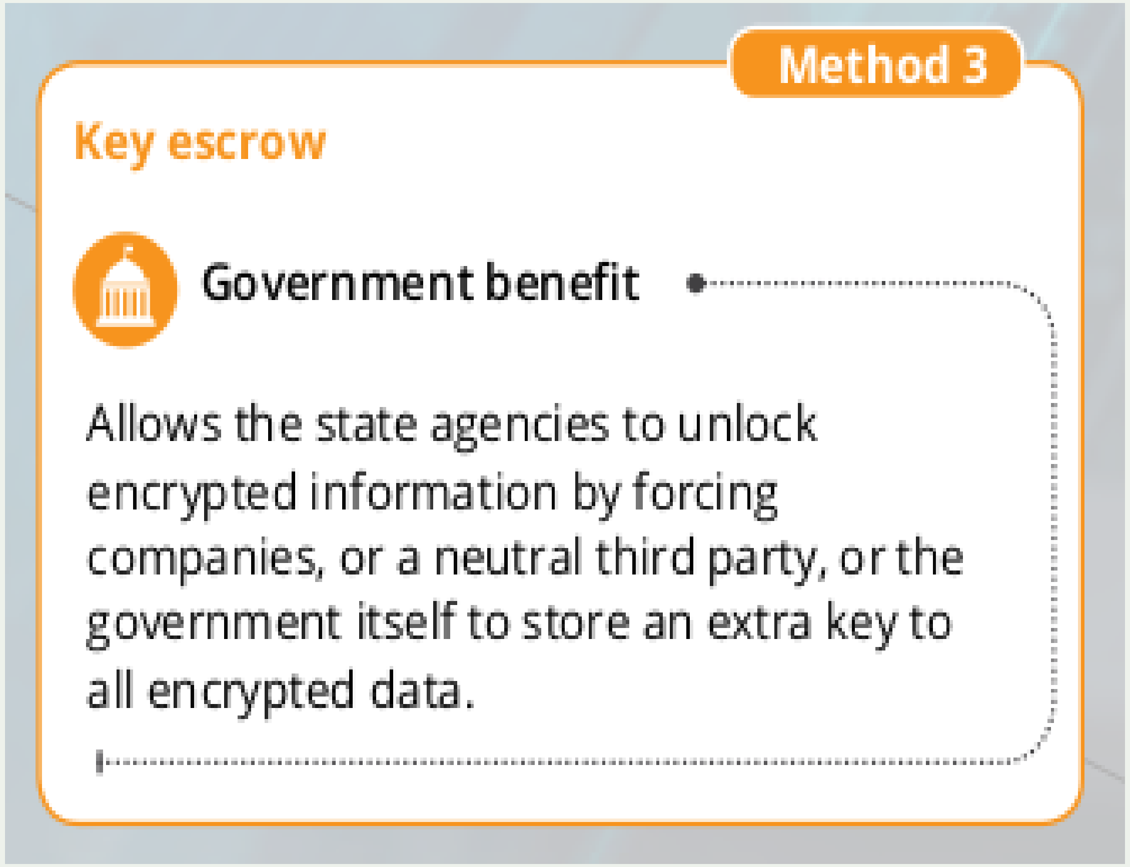
Compelling service providers to install backdoors can allow LEA and state agencies to circumvent encryption, often without notifying the user.

Security risk

If backdoors are discovered by malicious actors, they can exploit these vulnerabilities.

Source: https://ac-lac.org/wp-content/uploads/2022/05/Encryption-and-the-Digital-Economy.pdf

ENCRYPTION DEBATE

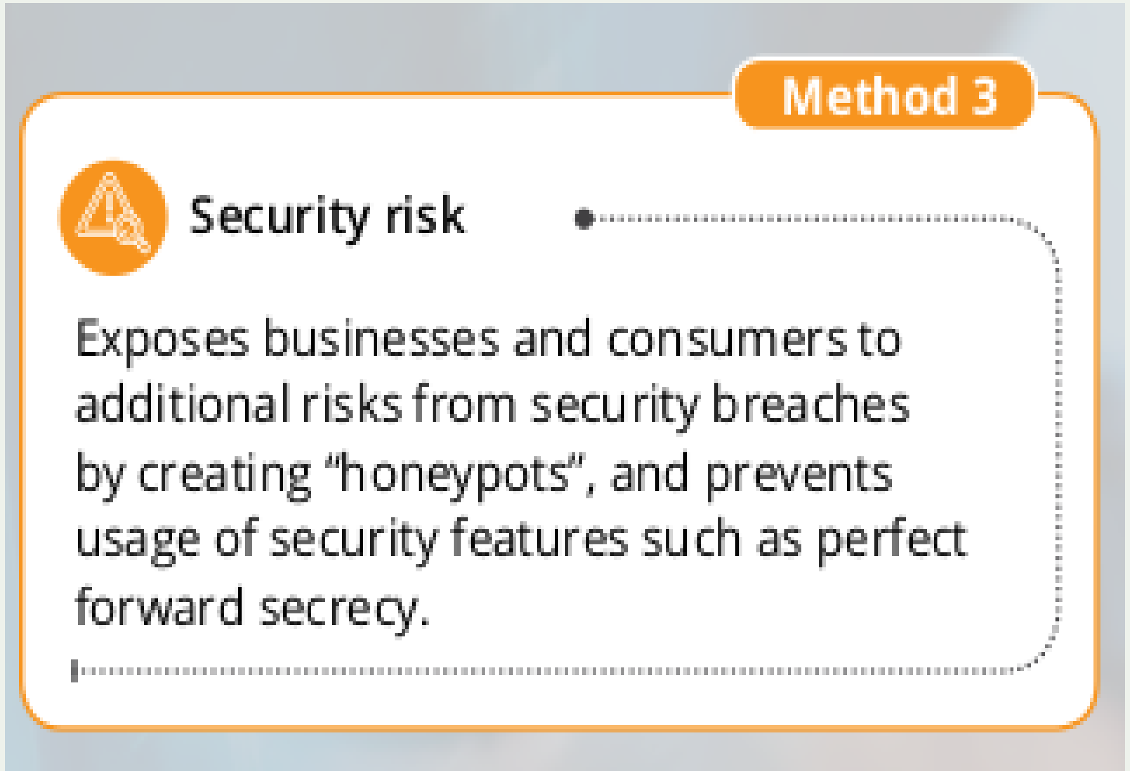


Method 3

Key escrow

Government benefit

Allows the state agencies to unlock encrypted information by forcing companies, or a neutral third party, or the government itself to store an extra key to all encrypted data.



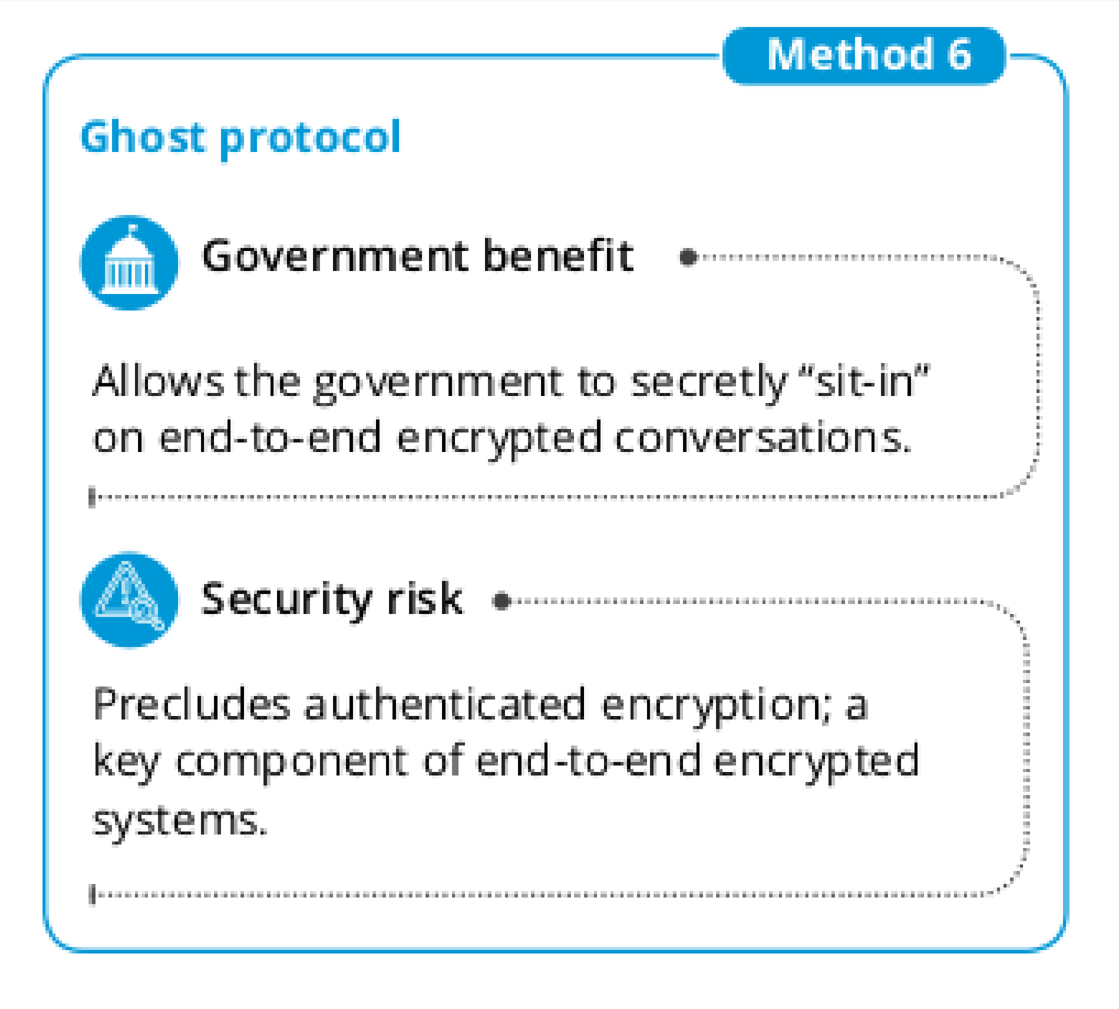
Method 3

Security risk

Exposes businesses and consumers to additional risks from security breaches by creating "honeypots", and prevents usage of security features such as perfect forward secrecy.

Source: https://ac-lac.org/wp-content/uploads/2022/05/Encryption-and-the-Digital-Economy.pdf

ENCRYPTION DEBATE



Method 6

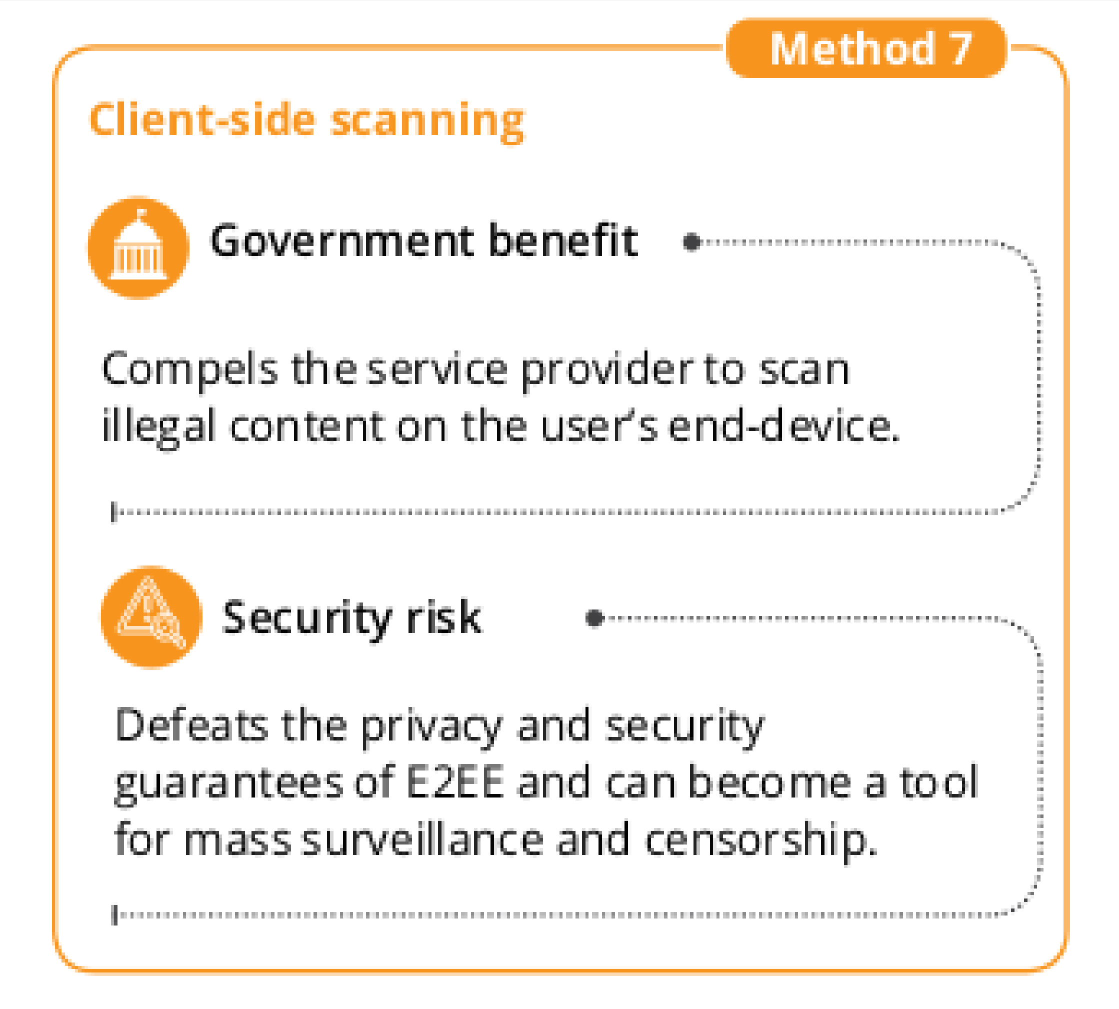
Ghost protocol

Government benefit

Allows the government to secretly "sit-in" on end-to-end encrypted conversations.

Security risk

Precludes authenticated encryption; a key component of end-to-end encrypted systems.



Method 7

Client-side scanning

Government benefit

Compels the service provider to scan illegal content on the user's end-device.

Security risk

Defeats the privacy and security guarantees of E2EE and can become a tool for mass surveillance and censorship.

Source: https://ac-lac.org/wp-content/uploads/2022/05/Encryption-and-the-Digital-Economy.pdf

RELEVANT CONSIDERATIONS

Encryption is not simply a tool used by criminals. It keeps data secure and communications private,

The absence of safeguards in frameworks that limit encryption and its security properties, either by enabling access through backdoors or demanding technical assistance from intermediaries, can trigger human rights related harms.

Source: https://ac-lac.org/wp-content/uploads/2022/05/Encryption-and-the-Digital-Economy.pdf

RELEVANT CONSIDERATIONS

At the Internet Society, as part of our public policy advisory efforts for Internet security, we provide technical assistance in the field of cryptography, a fundamental discipline for ensuring the confidentiality and integrity of online data.

We can provide detailed and specific technical material in accessible and easy-to-understand language, as well as expert guidance to help you understand and address information security challenges in your particular context.

STRONG ENCRYPTION AND RELATED SECURITY PRACTICES

- Use messaging apps that offer end-to-end encryption by default.
- Whenever available, use encryption on your devices or services. Some devices or services will offer encryption, but do not set it as the default.
- Use strong passwords. Do not use default passwords or passwords that include personal information.
- Keep security updates up to date. No system is totally secure.
- Security vulnerabilities are discovered all the time and fixed with updates. That's why it's so important to keep updates to your apps, devices, and services up to date.
- Whenever available, turn on two-factor authentication. Two-factor authentication adds another factor to your normal login process, making it harder for criminals to gain access to your data. This additional factor could be a free on-board security, an authenticator app, or simply receiving a text message with a security pin on your phone.
- Enable data wipe options to protect your data. Some smartphones and services have an option that will wipe your data after 3 or 10 failed attempts.

Donate

Olaf Kolkman
kolkman@isoc.org

Rue Vallin 2
CH-1201 Geneva
Switzerland

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

Science Park 400
1098 XH Amsterdam
Netherlands

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

66 Centrepoint Drive
Nepean, Ontario, K2G 6J5
Canada

6 Battery Road #38-04
Singapore 049909

internetsociety.org
@internetsociety