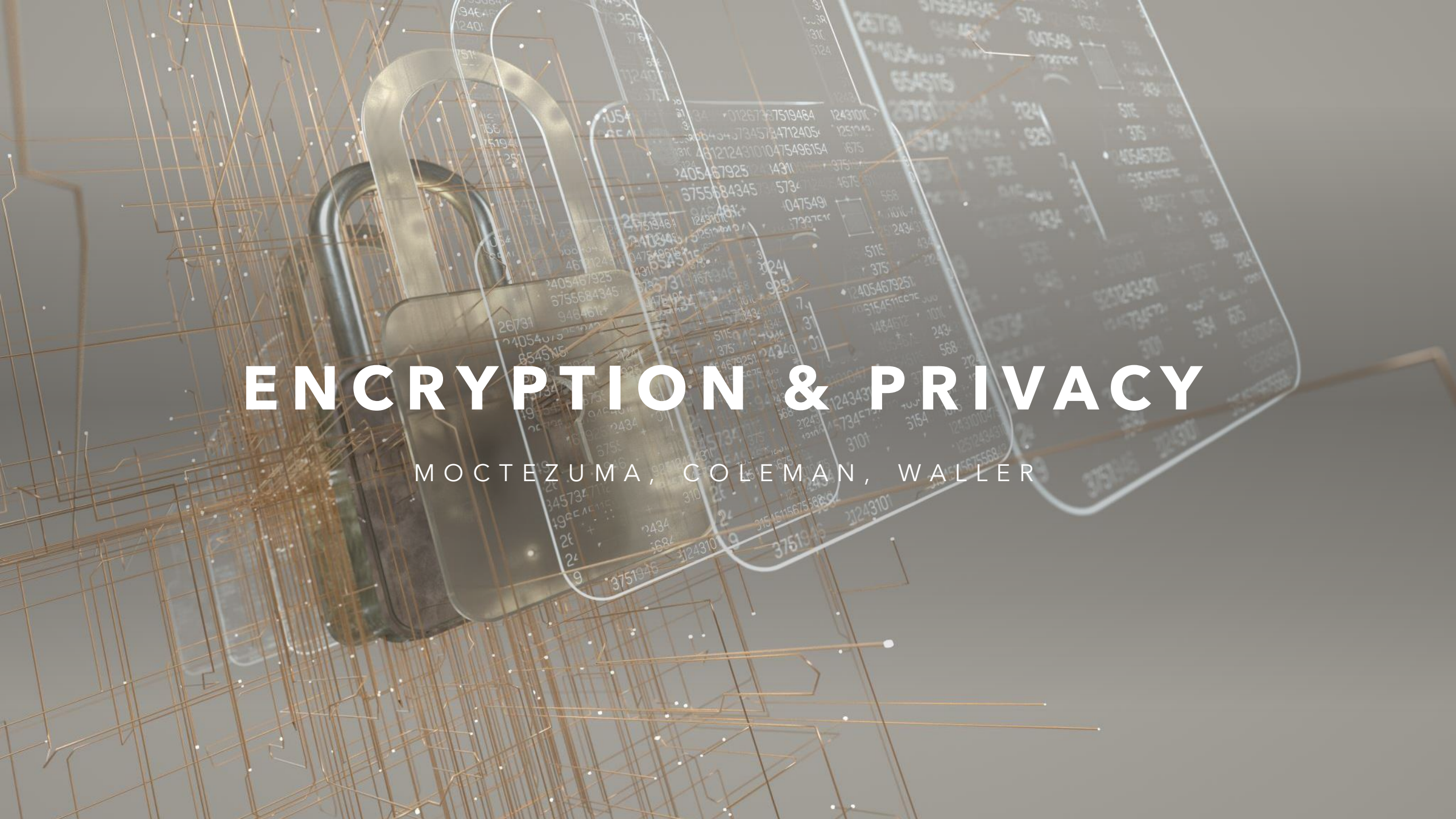


ENCRYPTION & PRIVACY

MOCTEZUMA, COLEMAN, WALLER

HOW ENCRYPTION WORKS

- The process of encoding information where only the computer or person that has the **key** can decode it to ensure security
- Computer encryption is formed from the science of cryptography
  - Biggest users were by the government, mainly military usage
  - Most forms of cryptography today are relied on computers due to human-based codes being too easy to crack (Scytale-Spartan generals used cylinder made from wood to send and receive messages)
  - Algorithms (Ciphers) are guides for encryption: Possible combinations are provided to craft a message

TWO CATEGORIES OF COMPUTER ENCRYPTION SYSTEMS

- Symmetric-key encryption: one computer essentially has a secret code that is used to encrypt information and is sent to another computer, where they will both hold the same key and decode the message
- Public key encryption (asymmetric-key): uses two different keys at once- private key and public key
  - Private key is only known to your computer
  - Public key is given by your own computer that is shared to any other computer that wants to securely communicate with it

SECURE SOCKETS

http (Hypertext Transfer Protocol)- protocol that is used for viewing web pages

https (**Secure** Hypertext Transfer Protocol)- http with a security feature

Secure Sockets Layer (SSL)- internet security protocol Web servers and internet browsers to transmit important information

Transport Layer Security (TLS)- latest standard cryptographic protocol

https://www.youtube.com/watch?v=hExRDVZHhig

AUTHENTICATION

Verification that the information is coming from a trusted source

Several ways to authenticate information or a person:

Password- username and password to login

Pass cards- cards that have embedded computer chips such as credit cards

Digital Signatures- electronic documents such as e-mails and spreadsheets

Biometrics such as fingerprint scanning, face scan, and voice identification

https://www.youtube.com/watch?v=GytLOow-7OY

P = NP?

P= polynomial time and are problems that are solvable in a reasonable time

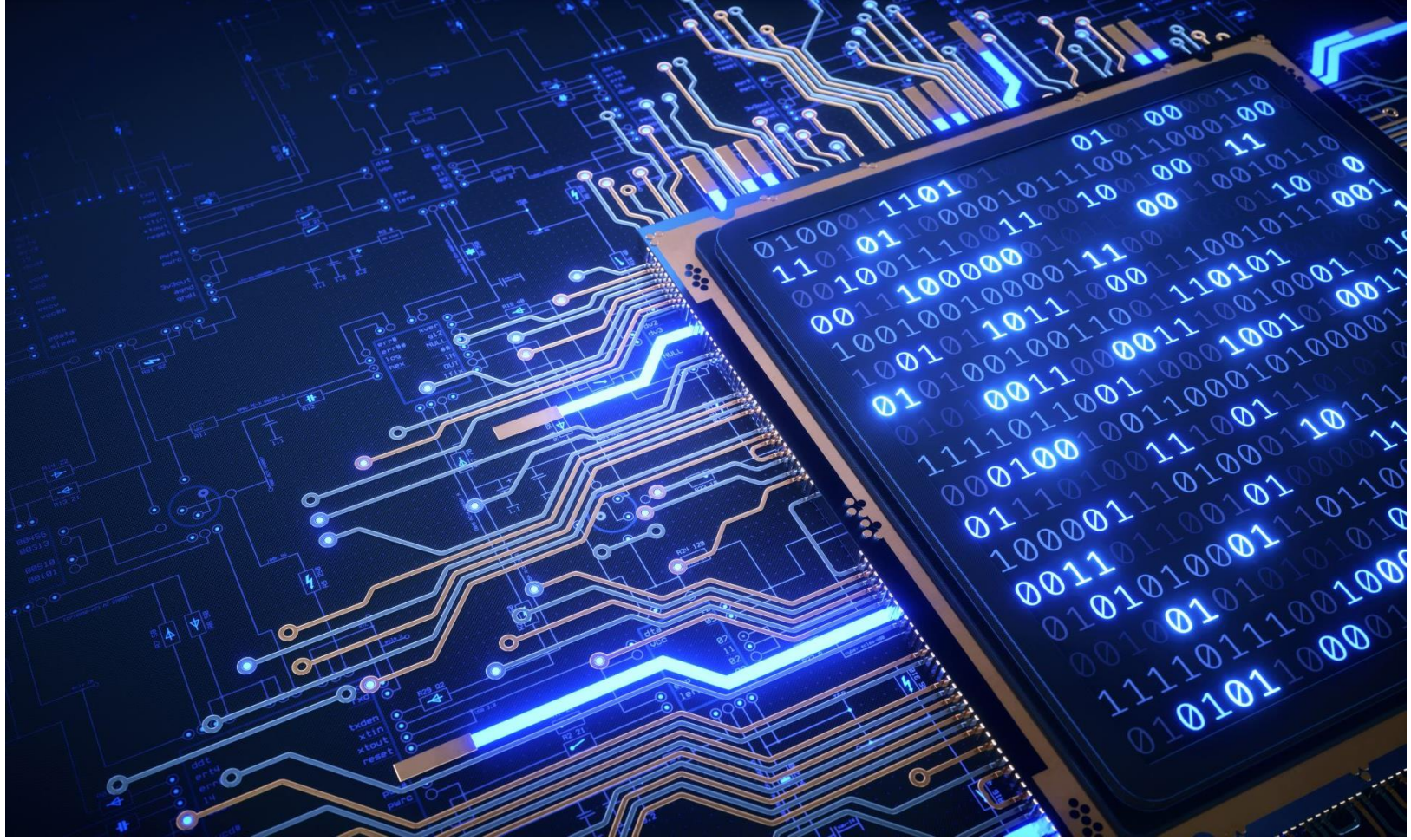
NP= nondeterministic polynomial time and these are problems that are complicated or even impossible to find a solution to

Example is prime factorization

There are currently no algorithms that can change NP problems to P problems

QUANTUM COMPUTING AND ENCRYPTION

- Quantum computers test and solve complicated problems through multiple combinations all happening at once
- This can possibly doom encryption as code breaking is a NP problem
- https://www.youtube.com/watch?v=dDOn_n7tNyo



HISTORY OF ENCRYPTION

- **Ancient Methods:**
  - Encryption traces back to ancient civilizations, where methods such as substitution ciphers and transposition ciphers were used to conceal messages.
  - Examples include the Caesar cipher, used by Julius Caesar to communicate securely with his generals, and the scytale, a cryptographic tool employed by the Spartans.
- **Medieval Cipher Systems:**
  - During the Middle Ages, more sophisticated cipher systems emerged, such as the Vigenère cipher, which used a keyword to encrypt plaintext messages.
  - Cryptanalysis, the art of breaking codes, also began to develop during this period, with cryptanalysts devising methods to crack encrypted messages.
- **Rise of Modern Cryptography:**
  - The Renaissance witnessed advancements in cryptography, including the invention of polyalphabetic ciphers and the publication of seminal works like Johannes Trithemius' "Polygraphiae."
  - In the 20th century, the invention of electromechanical cipher machines, such as the Enigma machine used by the German military during World War II, revolutionized encryption technology.

•Public Key Cryptography:

•The advent of public key cryptography in the 1970s marked a significant milestone in encryption history.

•Whitfield Diffie and Martin Hellman's groundbreaking paper on "New Directions in Cryptography" introduced the concept of asymmetric encryption, enabling secure communication over insecure channels.

HISTORY OF ENCRYPTION CONT.

THE HISTORY OF ENCRYPTION

FILE ENCRYPTION

File encryption involves the process of encoding data in a way that only authorized users can access it. It transforms plaintext data into ciphertext using encryption algorithms, making it unreadable without the decryption key.

The primary purpose of file encryption is to prevent unauthorized access to sensitive information, such as personal documents, financial records, or confidential business data. By encrypting files, even if an unauthorized party gains access to the device or file storage, they cannot view the contents without the decryption key.

VPN (VIRTUAL PRIVATE NETWORK)

A Virtual Private Network (VPN) is a technology that establishes a secure, encrypted connection over a public network, such as the internet. It creates a private network from a public internet connection, enabling users to access the internet securely and anonymously.

When a user connects to a VPN server, their internet traffic is encrypted before being transmitted over the network. This encryption ensures that sensitive information, such as browsing activity, passwords, and personal data, remains protected from eavesdroppers and cyber threats.

VPNs utilize encryption protocols, such as OpenVPN, IPSec, and L2TP/IPSec, to secure data transmission between the user's device and the VPN server. This encryption prevents unauthorized access and interception of data packets, enhancing privacy and confidentiality.

VPN

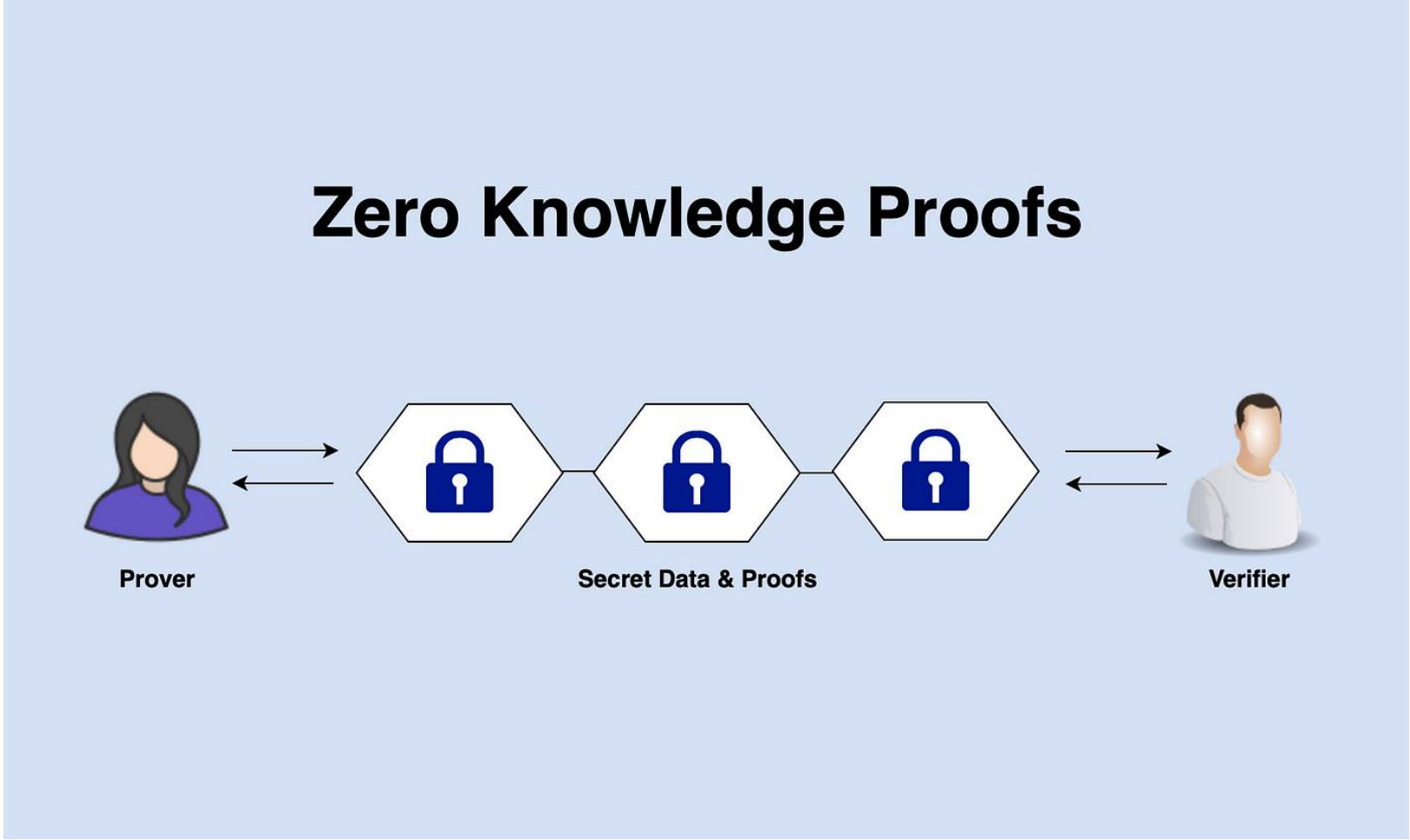
DISK ENCRYPTION

Disk encryption is the process of encrypting data stored on a hard drive or other storage device, rendering it inaccessible to unauthorized users without the appropriate decryption key.

Unlike file encryption, which encrypts individual files or folders, disk encryption encrypts entire disk volumes, including the operating system, applications, and user data.

Zero-Knowledge Proof (ZKP) is a cryptographic protocol that allows one party (the prover) to demonstrate to another party (the verifier) that a statement is true without revealing any additional information beyond the validity of the statement itself.

In a Zero-Knowledge Proof, the prover convinces the verifier of the truthfulness of a statement without disclosing any knowledge or details that could compromise the privacy or confidentiality of the underlying data or information.



ZERO KNOWLEDGE PROOF

HOMOMORPHIC ENCRYPTION

Homomorphic Encryption is a cryptographic scheme that enables computations to be performed directly on encrypted data, yielding an encrypted result that, when decrypted, matches the result of the operations performed on the plaintext data.

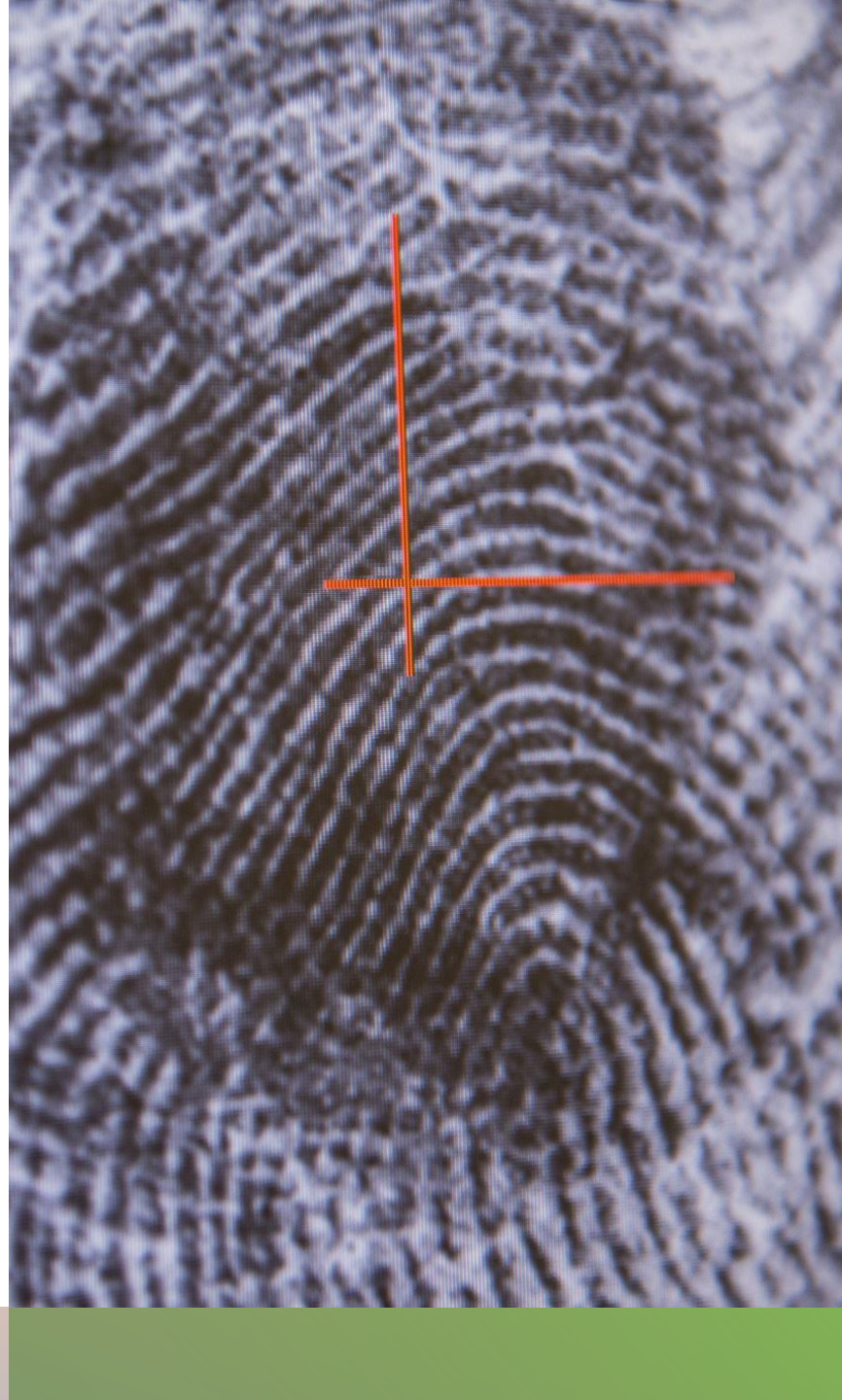
Unlike traditional encryption methods, which require decryption before performing computations, Homomorphic Encryption allows data to remain encrypted throughout the computation process, preserving privacy and confidentiality.

PRIVACY

There are several privacy issues facing people today including the following:

- biometrics: fingerprints, facial recognition, iris recognition
- video surveillance: cameras in public and private places
- online privacy: ensuring your browser history is not known
- wireless tracking: using cell towers to locate a phone
- identity theft: assuming someone else's online identity and exploiting it
- medical records: ensuring their privacy
- wiretapping: usually requires warrant, some states (i.e., Georgia) allow phone user to tap own line without permission
- RFID: radio frequency identification can be used to steal encrypted information from credit cards

There other issues not listed here, but can be researched at privacyrights.org



ELECTRONIC FREEDOM FOUNDATION

- The Electronic Freedom Foundation is an organization that strives for protecting individual rights related to electronic technology
- You can get more information about your rights and protection of your privacy on their page Electronic Freedom Foundation

They even talk about privacy on campuses from campus security technology including:

- Body Worn Cameras
- Drones
- Automated License Plate Readers
- Social Media Monitoring
- Biometric Identification
- Gunshot Detection
- Video Analytics

DIGITAL RIGHTS AND POLICE

- E911 allows authorities to track cell phones during 911 calls
- The law does not allow GPS tracking in non-emergency situations
- The 4th Amendment protects people from unreasonable governmental search and seizures unless given consent
- If officers suspect an electronic device with important evidence is going to be destroyed, they may enter anyway
- Always ask for a warrant!!!

EVENT DATA RECORDERS

- Popularly known as "black boxes," event data recorders (EDRs) have helped investigators solve the mysteries of airplane crashes for decades. Now they've become standard in almost every new car sold.
- Event data recorders track vehicle data such as speed, acceleration, braking, steering, and air-bag deployment before, during, and after a crash.

- The newest EVRs record:
  - The forward and lateral crash force.
  - The crash event duration.
  - Indicated vehicle speed.
  - Accelerator position.
  - Engine rpm.
  - Brake application and antilock brake activation.
  - Steering wheel angle.
  - Stability control engagement.
  - Vehicle roll angle, in case of a rollover.
  - Number of times the vehicle has been started.
  - Driver and front-passenger safety belt engagement, and pretensioner or force limiter engagement.
  - Air bag deployment, speed, and faults for all air bags.
  - Front seat positions.
  - Occupant size.
  - Number of crashes

WHAT ABOUT INSURANCE TRACKING DEVICES?

Car insurance tracking devices are either plugged into your car's onboard diagnostics or downloaded as an app on your smartphone.

These devices monitor your speed, acceleration, braking, and other details each time you drive and report the information to the insurance company.

Car insurance companies use the data they gather from the tracking device to adjust your premium or offer a discount.

Even though discounts on insurance may be great, the biggest con to having insurance tracking devices means you have no more privacy on your whereabouts and your personal information

CYBERSECURITY INFORMATION SHARING ACT (CISA)

- "CISA is responsible for protecting the Nation’s critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations."
- CISA functions:
  - Comprehensive Cyber Protection
  - Infrastructure Resilience
  - Emergency Communication
  - National Risk Management Center

CITATIONS:

- https://privacyrights.org/resources/privacy-today-review-current-issues
- https://www.eff.org/issues/security
- https://www.usnews.com/insurance/auto/how-do-those-car-insurance-tracking-devices-work