E-business

E-business security

SILESIAN UNIVERSITY
SCHOOL OF BUSINESS ADMINISTRATION IN KARVINA

Petr Suchánek

E-business

Outline of the lecture

- **Cyber security**
- **Electronic and digital signature.**

Cyber security*

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.*
- Cyber security may also be referred to as information technology security.*
- Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.**
- These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.**

*https://digitalguardian.com/blog/what-cyber-security

**https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cyber security*

- A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe.
- In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.
- A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions:
  - detection;
  - investigation;
  - remediation.

* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cyber security*

- People
  - ➢ Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.
- Processes
  - Organizations must have a framework for how they deal with both attempted and successful cyber attacks.
  - One well-respected framework can guide you.
  - It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cyber security*

- Technology
  - Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks.
  - Three main entities must be protected:
    - endpoint devices (computers, smart devices, routers, etc.);
    - networks;
    - cloud.
  - Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cyber security

- https://study.com/academy/lesson/what-is-cybersecurity-definition-principles.html
- https://arch.simplicable.com/arch/new/the-8-principles-of-web-security
- https://www.iotsecurityfoundation.org/access-and-control-of-device/
- https://www.neosit.com/en/contenthub/blog-post-19.html
- https://blackpointcyber.com/blog/12-cyber-security-principles/
- https://www.accaglobal.com/ie/en/member/discover/cpd-articles/audit-assurance/the-key-cybersecurity-principles.html

Digital signature

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.*

- As the digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.*

- Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

*https://searchsecurity.techtarget.com/definition/digital-signature

Digital signature vs. electronic signature

- While digital signature is a technical term, defining the result of a cryptographic process that can be used to authenticate a sequence of data, the term electronic signature - or e-signature - is a legal term that is defined legislatively.
- This means that a digital signature -- which can be expressed digitally in electronic form and associated with the representation of a record - can be a type of electronic signature.
- More generally, though, an electronic signature can be as simple as the signer's name being entered on a form on a webpage.

*https://searchsecurity.techtarget.com/definition/digital-signature

Certification authority

- A certificate authority or certification authority (CA) is an entity that issues digital certificates.*
- A digital certificate certifies the ownership of a public key by the named subject of the certificate.*
- This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key.*
- A CA acts as a trusted third party - trusted both by the subject (owner) of the certificate and by the party relying upon the certificate.*

*https://en.wikipedia.org/wiki/Certificate_authority

Cryptography

- Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.*

- The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing.„*

- In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher.*

- These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.*

*https://searchsecurity.techtarget.com/definition/cryptography

Cryptography

- Confidentiality
  - ➢ the information cannot be understood by anyone for whom it was unintended;
- Integrity
  - ➢ the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected;
- Non-repudiation
  - ➢ the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information;
- Authentication
  - ➢ the sender and receiver can confirm each other's identity and the origin/destination of the information.

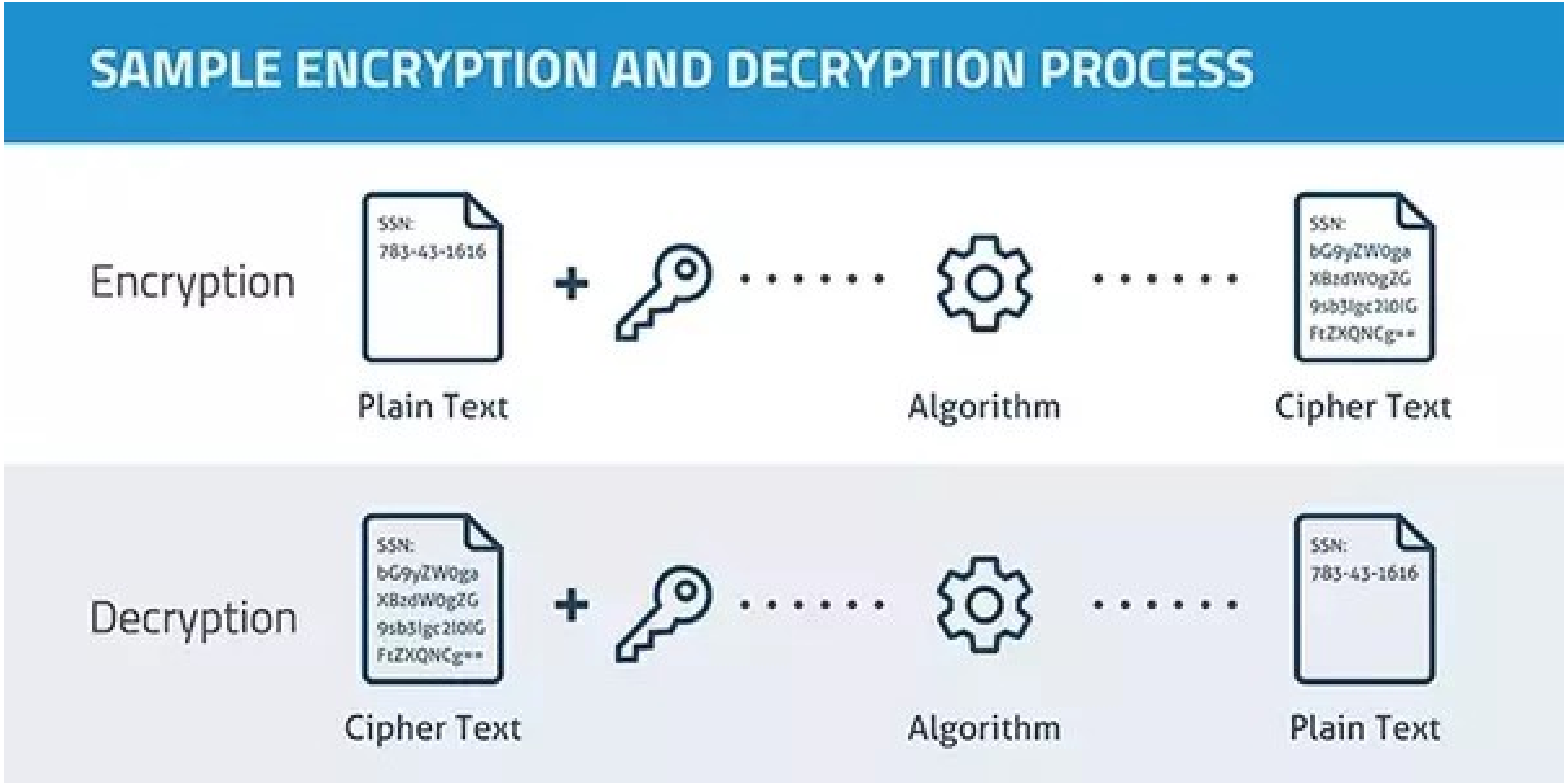
*https://searchsecurity.techtarget.com/definition/cryptography

Cryptographic key

- A cryptographic key is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.*
- This key remains private and ensures secure communication.*
- A cryptographic key is the core part of cryptographic operations.*
- Many cryptographic systems include pairs of operations, such as encryption and decryption.*
- A key is a part of the variable data that is provided as input to a cryptographic algorithm to execute this sort of operation.*
- In a properly designed cryptographic scheme, the security of the scheme is dependent on the security of the keys used.*

*https://www.techopedia.com/definition/24749/cryptographic-key

Cryptography - data encryption & decryption



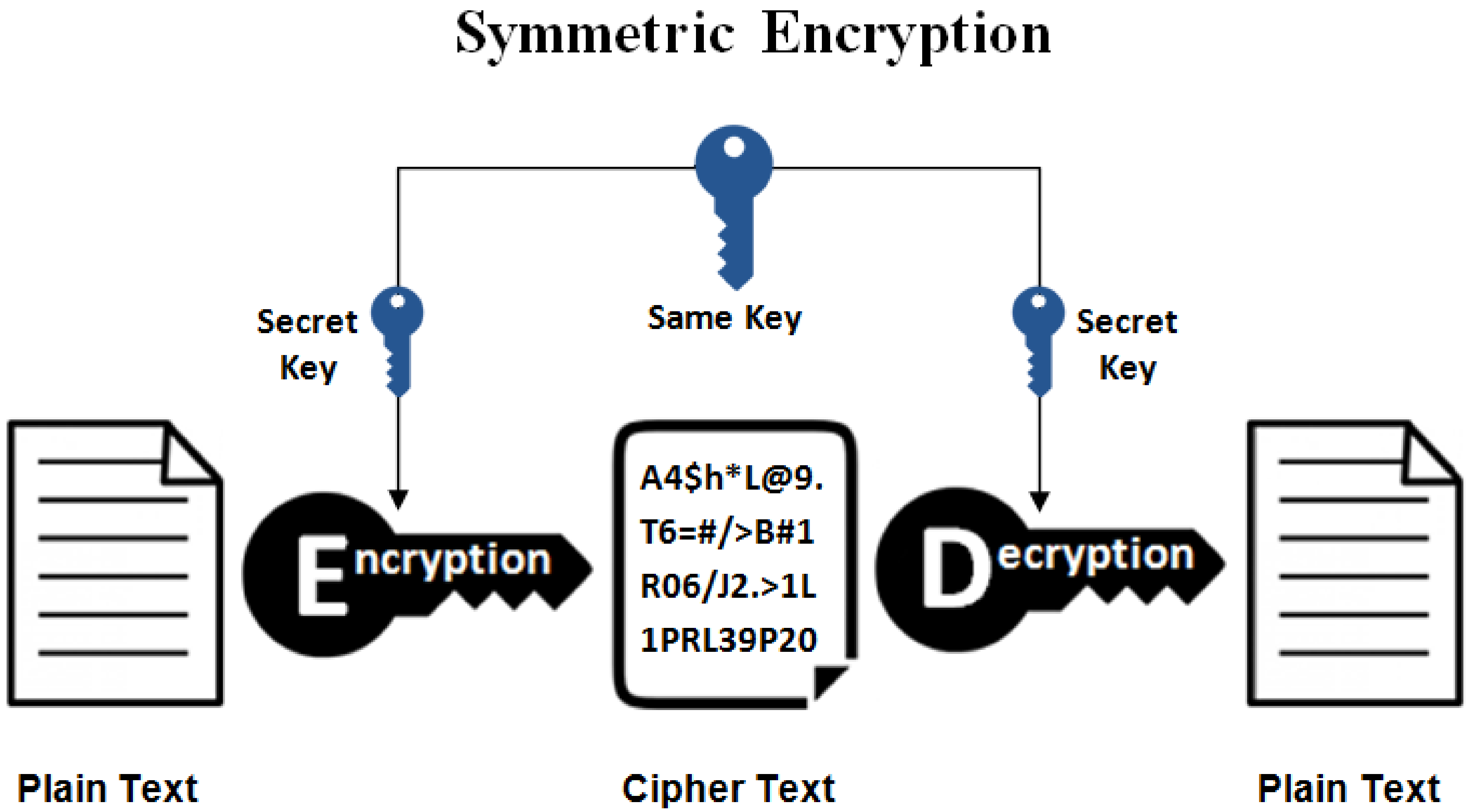
*https://medium.com/@daser/a-lazy-mans-introduction-to-multi-party-encryption-and-decryption-59f62b8616d8

Symmetric encryption

- This is the simplest kind of encryption that involves only one secret key to cipher and decipher information.
- Symmetrical encryption is an old and best-known technique.
- It uses a secret key that can either be a number, a word or a string of random letters.
- It is a blended with the plain text of a message to change the content in a particular way.
- The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.

*https://medium.com/@daser/a-lazy-mans-introduction-to-multi-party-encryption-and-decryption-59f62b8616d8

Symmetric encryption



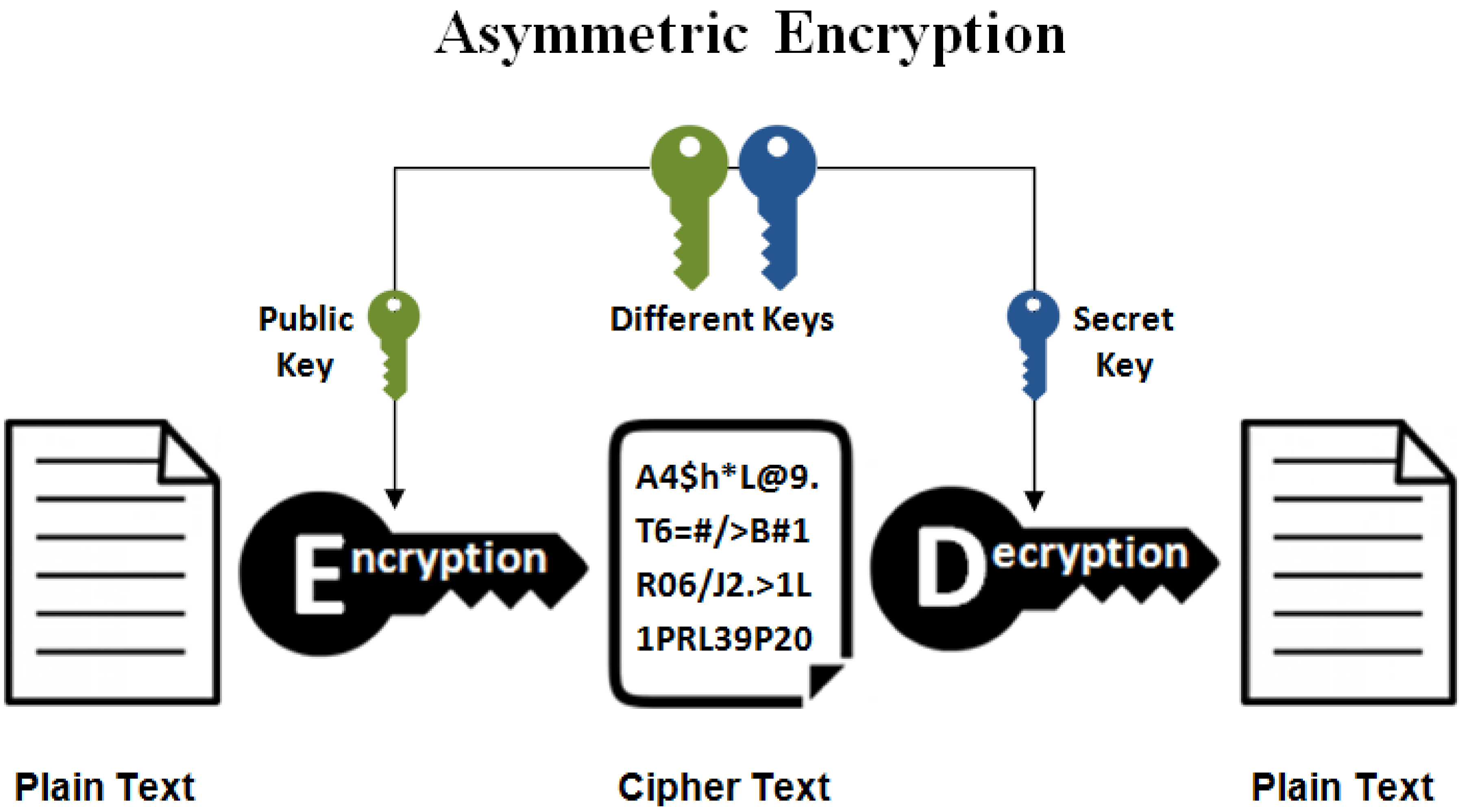
*https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Asymmetric encryption

- Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption.
- Asymmetric encryption uses two keys to encrypt a plain text.
- It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security.
- A public key is made freely available to anyone who might want to send you a message.
- The second private key is kept a secret so that you can only know.

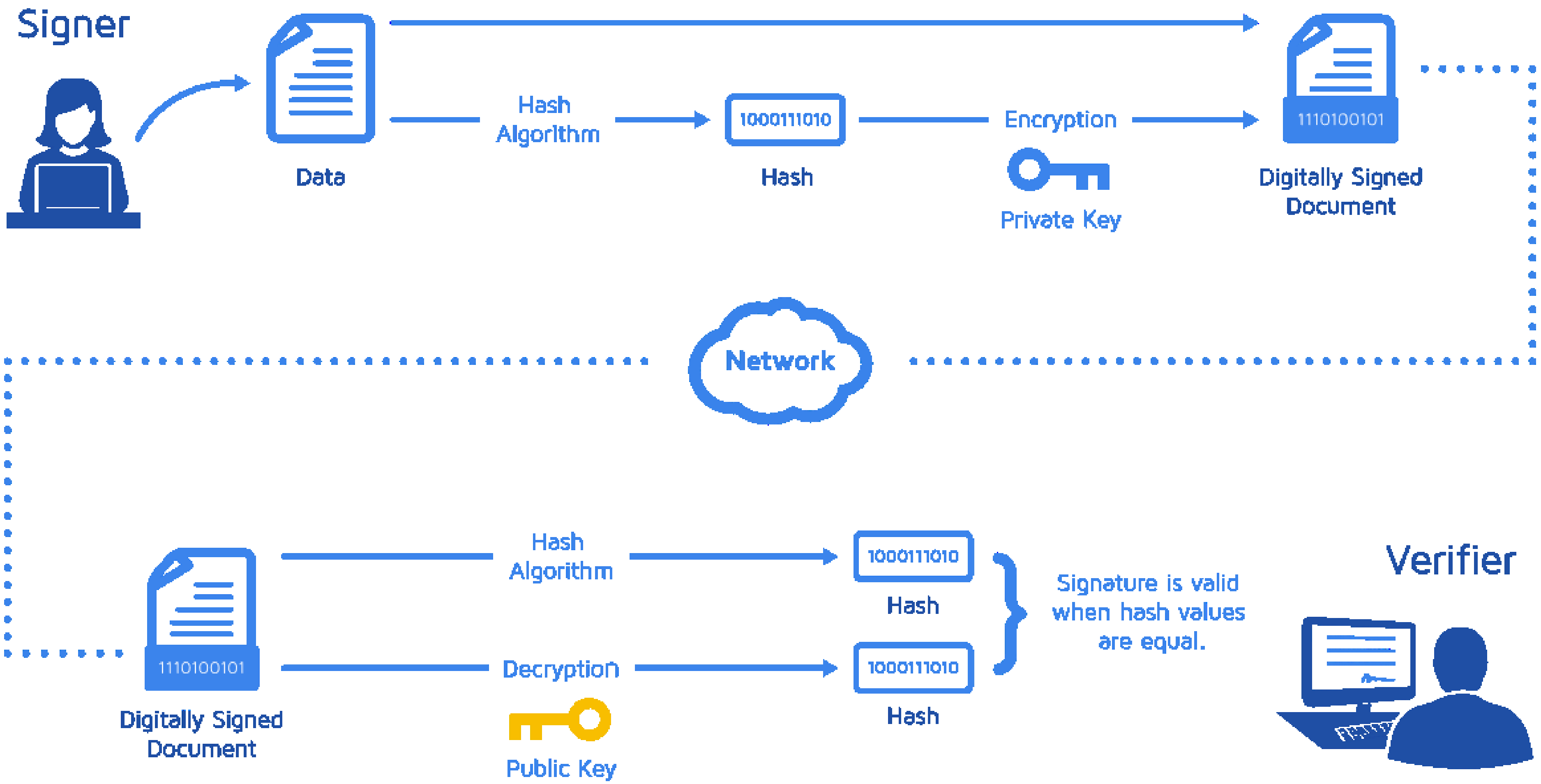
*https://medium.com/@daser/a-lazy-mans-introduction-to-multi-party-encryption-and-decryption-59f62b8616d8

Asymmetric encryption



*https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Digital signature



*https://medium.com/@meruja/digital-signature-generation-75cc63b7e1b4

Digital signature

- https://www.instantssl.com/digital-signature
- https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq
- https://searchsecurity.techtarget.com/definition/digital-signature
- https://www.securedsigning.com/resources/intro-to-digital-signatures
- https://www.profitbooks.net/digital-signature/
- https://www.signinghub.com/electronic-signatures/
- https://signeasy.com/blog/electronic-signature-101/esign-vs-digital-sign/

The end

Thank you for your attention!

Any questions?