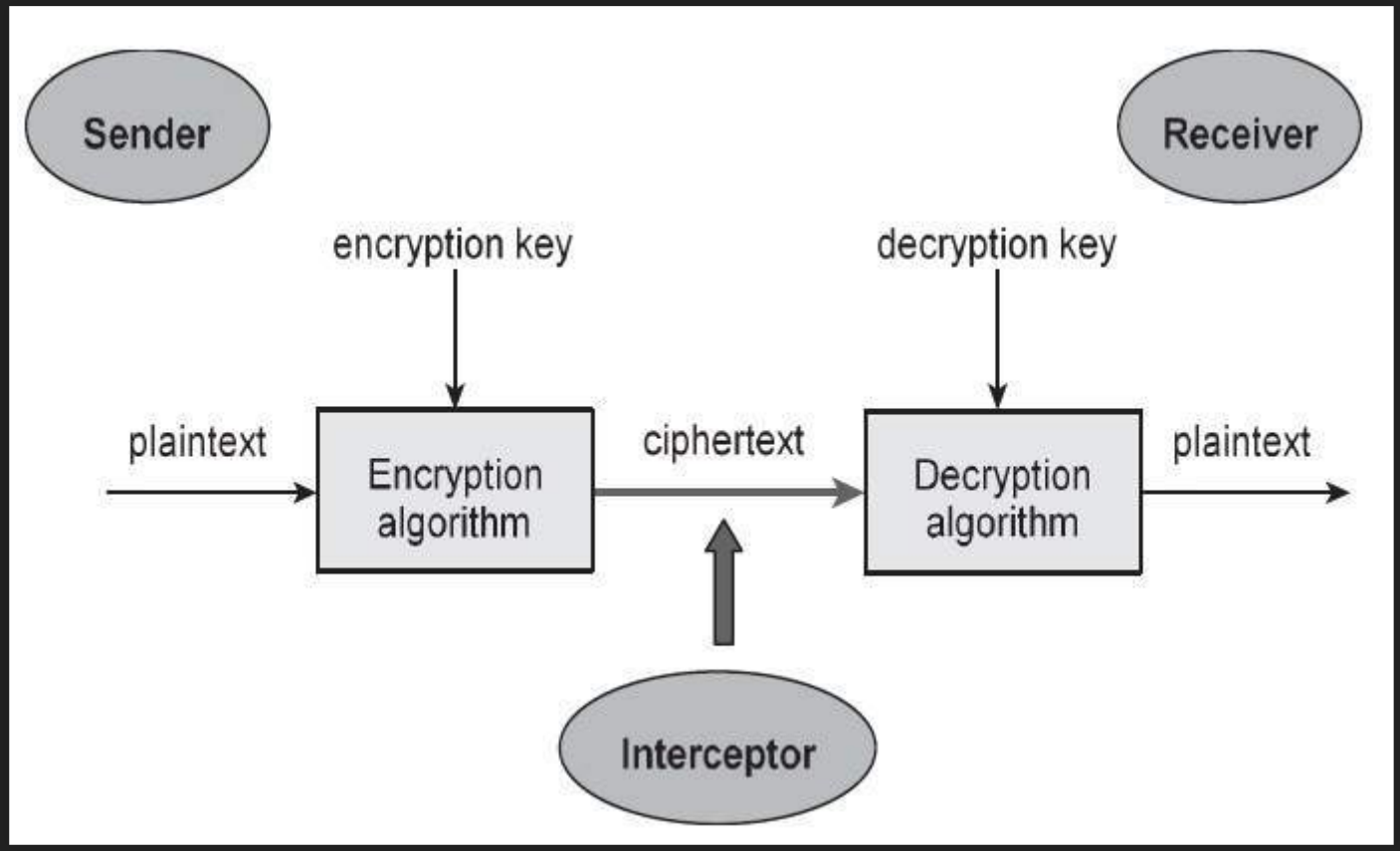
CRYPTO FOR BEGINNERS

BY:

@_RIDDHISHREE

CRYPTOSYSTEM?

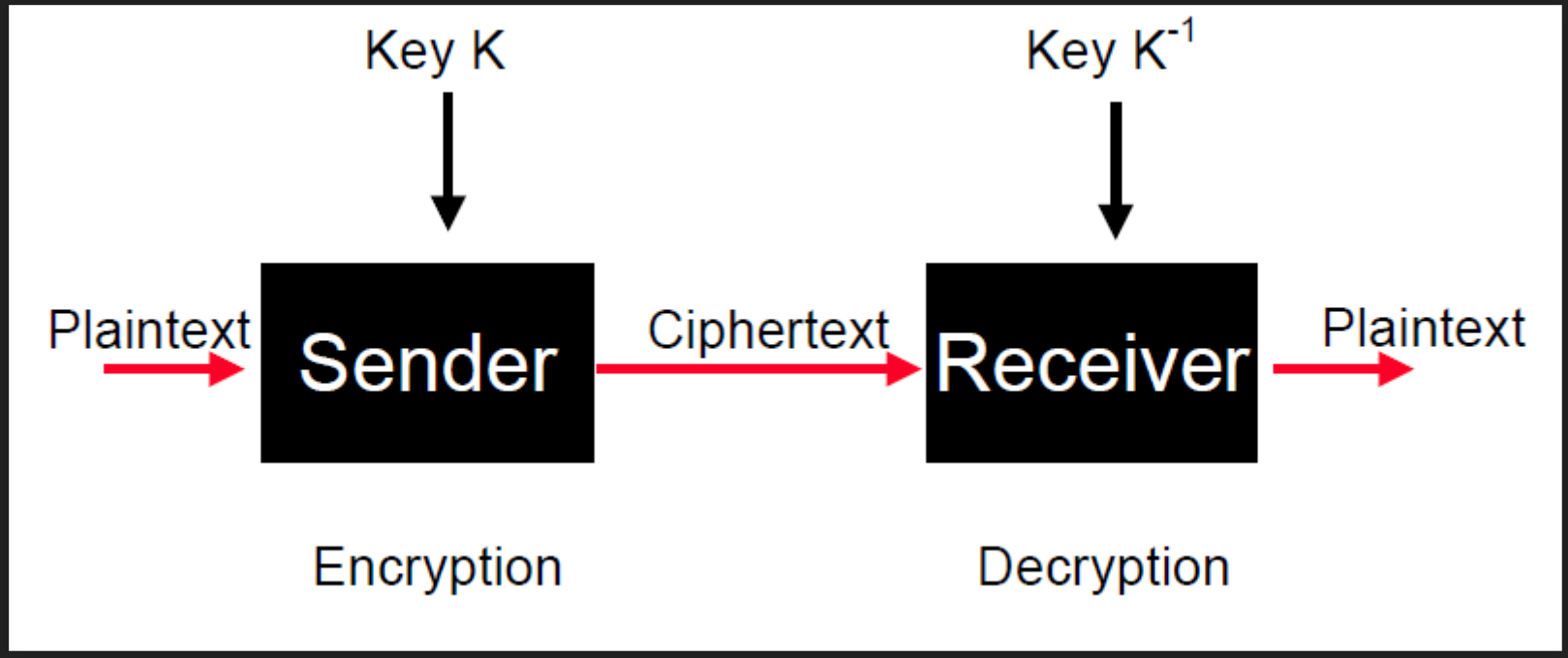
- An implementation of **cryptographic techniques** and their accompanying infrastructure to provide *information security services*.



"https://www.tutorialspoint.com/cryptography/images/

CRYPTOGRAPHY?

- Refers to the design of mechanisms based on **mathematical algorithms** that provide fundamental information security services.
- It is required in order to protect the **confidentiality** and **integrity** of *sensitive user data*.

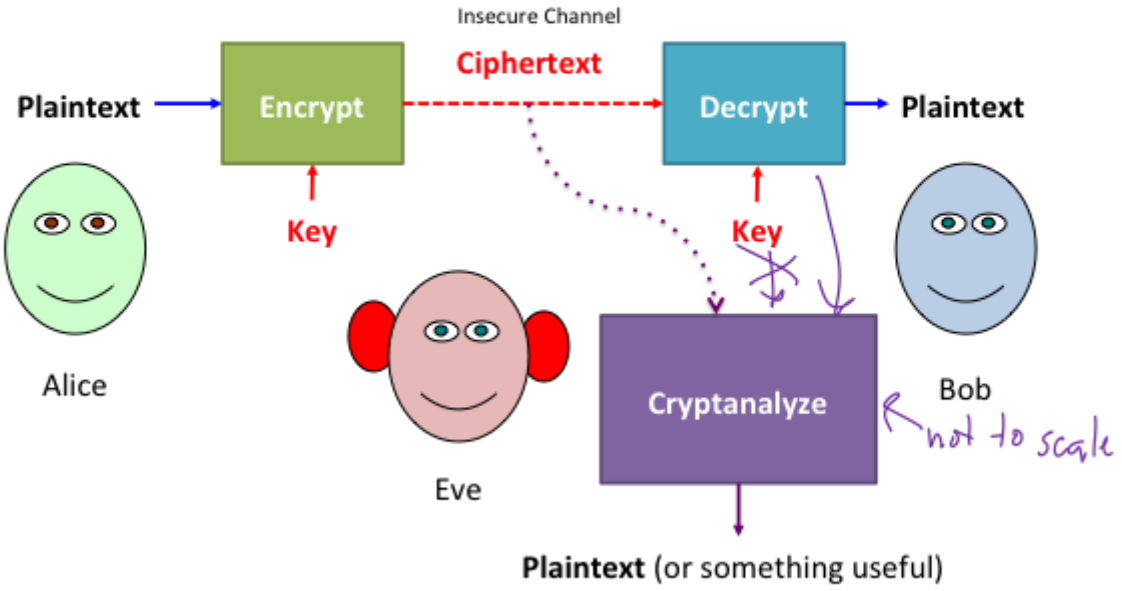


"http://www.pling.org.uk/cs/cry.html"

CRYPTANALYSIS?

- It's goal is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

Cryptanalysis



"https://www.cs.virginia.edu/~evans/crypto/static/day1/

CRYPTOGRAPHIC ALGORITHMS

1. Symmetric Cryptography
2. Asymmetric Cryptography
3. Hashes
4. Key Exchange Algorithms

SYMMETRIC CRYPTOGRAPHY

- It's a two-step process:
  - Involved parties share a **common secret** like password, pass phrase, or a key.
  - Data is encrypted & decrypted using the **same key**.
- e.g., DES, 3DES and AES

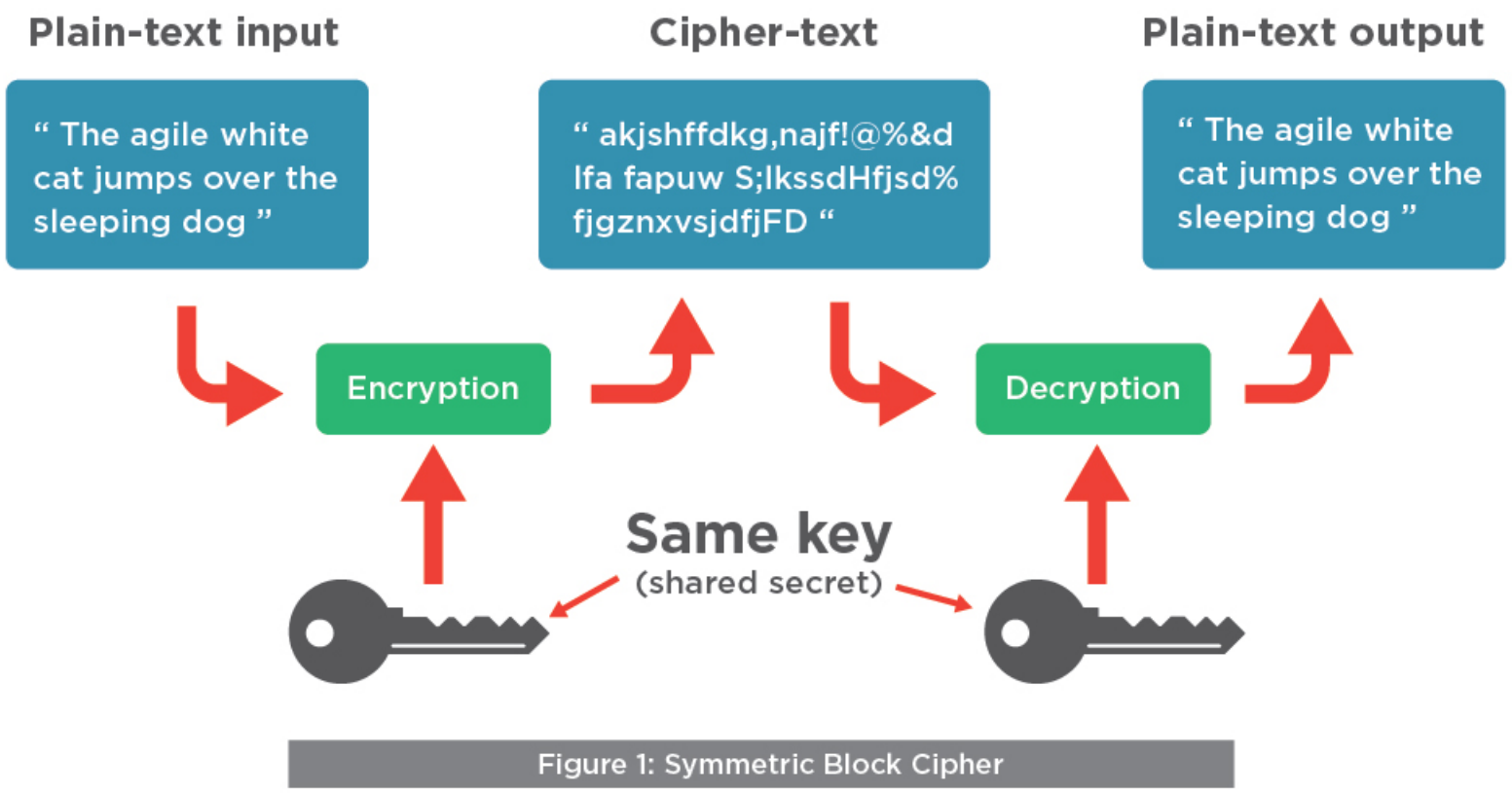
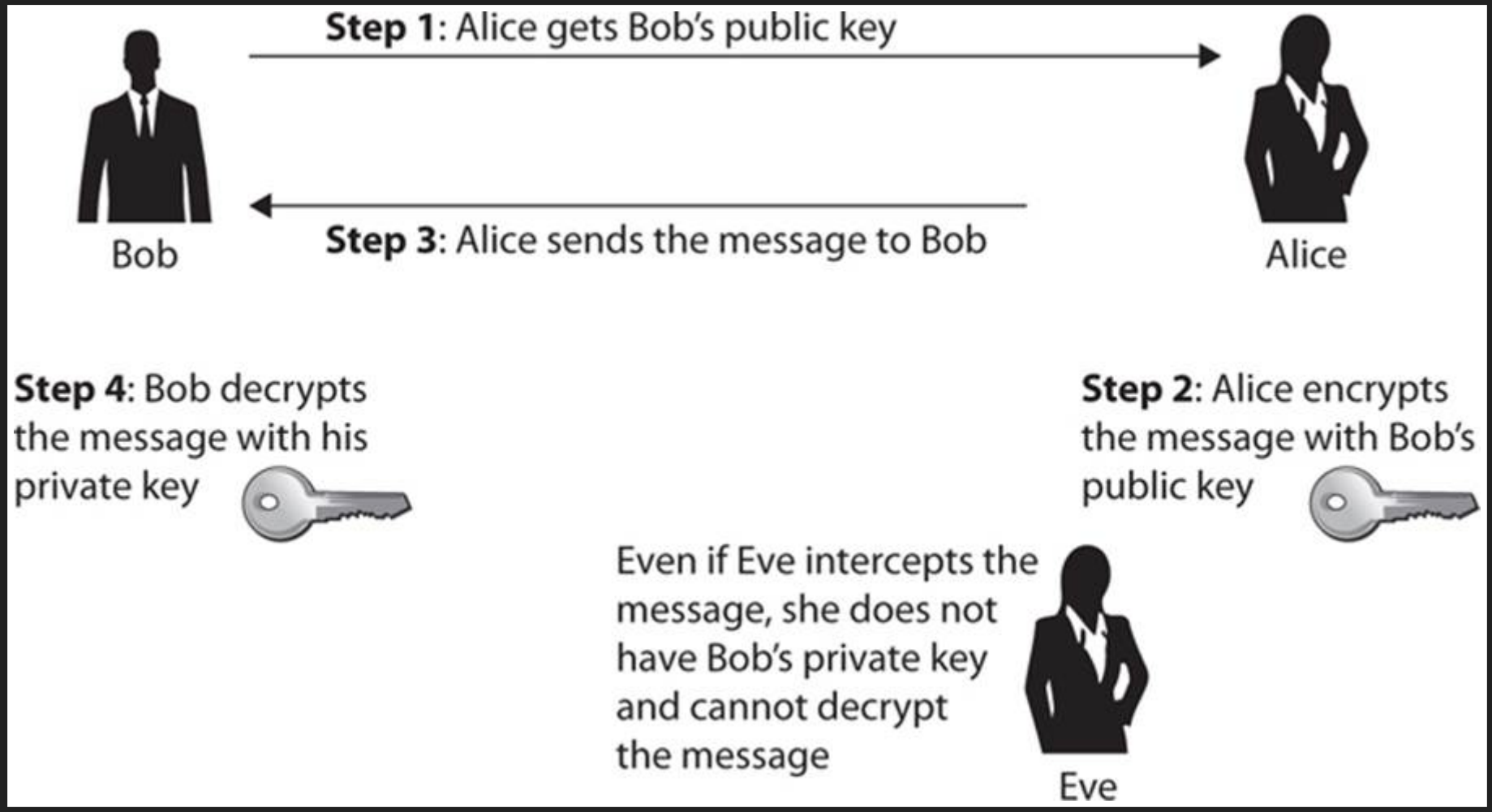


Figure 1: Symmetric Block Cipher

"https://cdn.transcend-info.com/Embedded/images/15/Ind_web_AES_07.jpg"

ASYMMETRIC CRYPTOGRAPHY

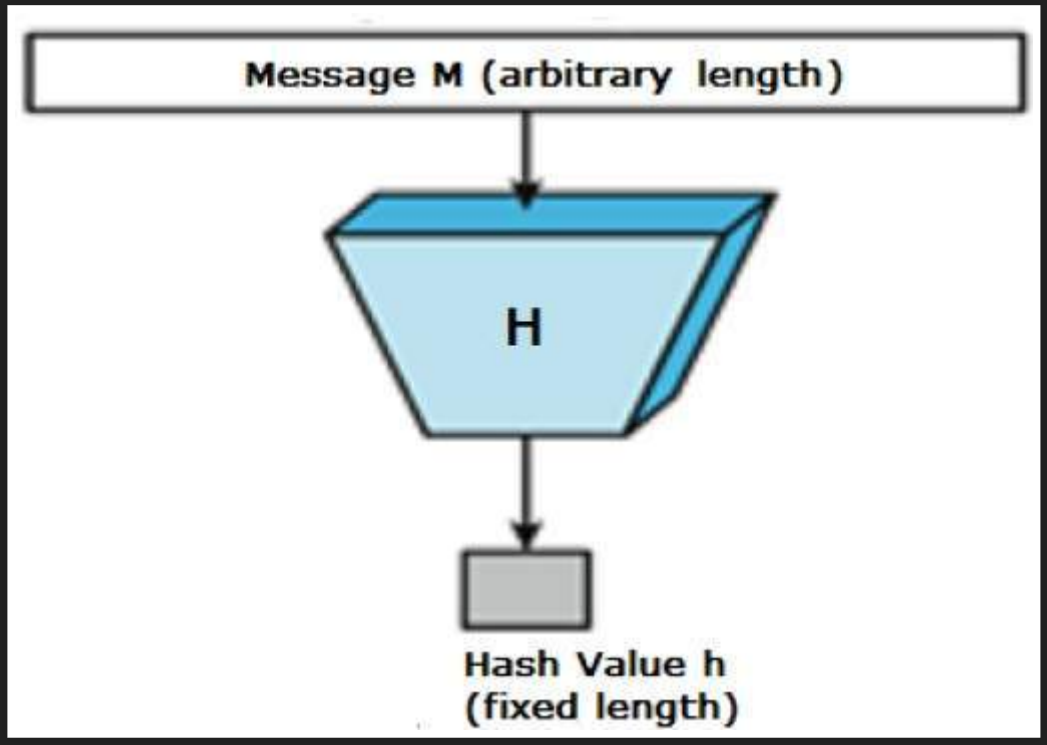
- "Public/Private Key Cryptography"
- Asymmetric algorithms use two keys, one to encrypt the data, and the other key to decrypt it.
- e.g., PGP and SSL are systems that implement asymmetric cryptography, using RSA or other algorithms.



"http://apprize.info/security/cryptography/cryptography

HASHES

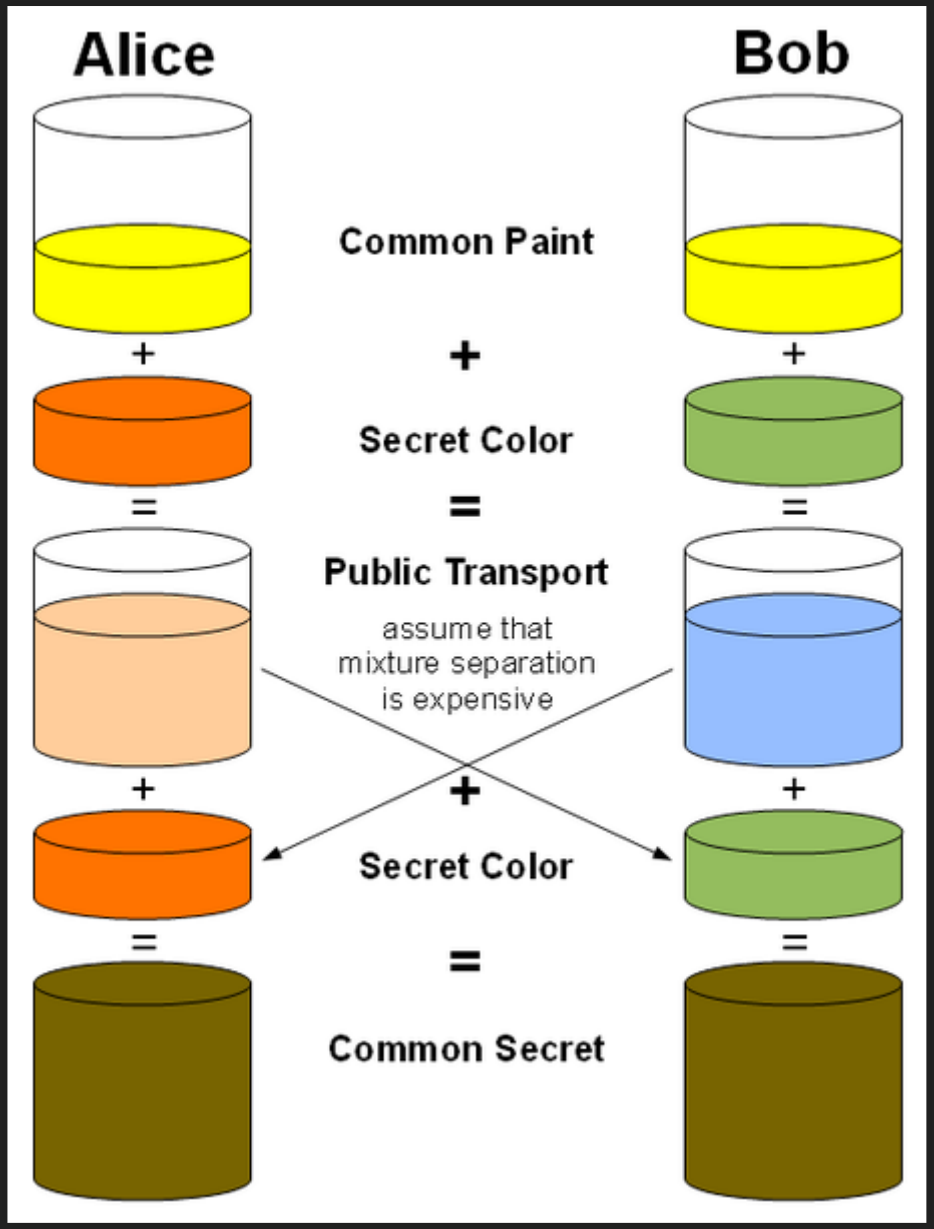
- Hash functions take some data of an arbitrary length (and possibly a key or a password) and generate a **fixed-length hash** based on this input.
- e.g., MD5, SHA-1, SHA-2
- Refer this article to understand the difference between SHA-1, SHA-2 and SHA-256 Hash Algorithms.



"https://www.tutorialspoint.com/cryptography/images/

KEY EXCHANGE ALGORITHMS

- Key exchange algorithms allow us to safely exchange encryption keys with an unknown party.
- e.g., Diffie-Hellman for SSL



"https://upload.wikimedia.org/wikipedia/commons/thu

Hellman_Key_Exchange.png/451px-Diffie-Hellman_Key_Exchange.png"

CRYPTOGRAPHIC PROTOCOLS

Cryptographic algorithms, when used in networks, are used within a cryptographic protocol. Cryptographic protocols cover a range of different applications:

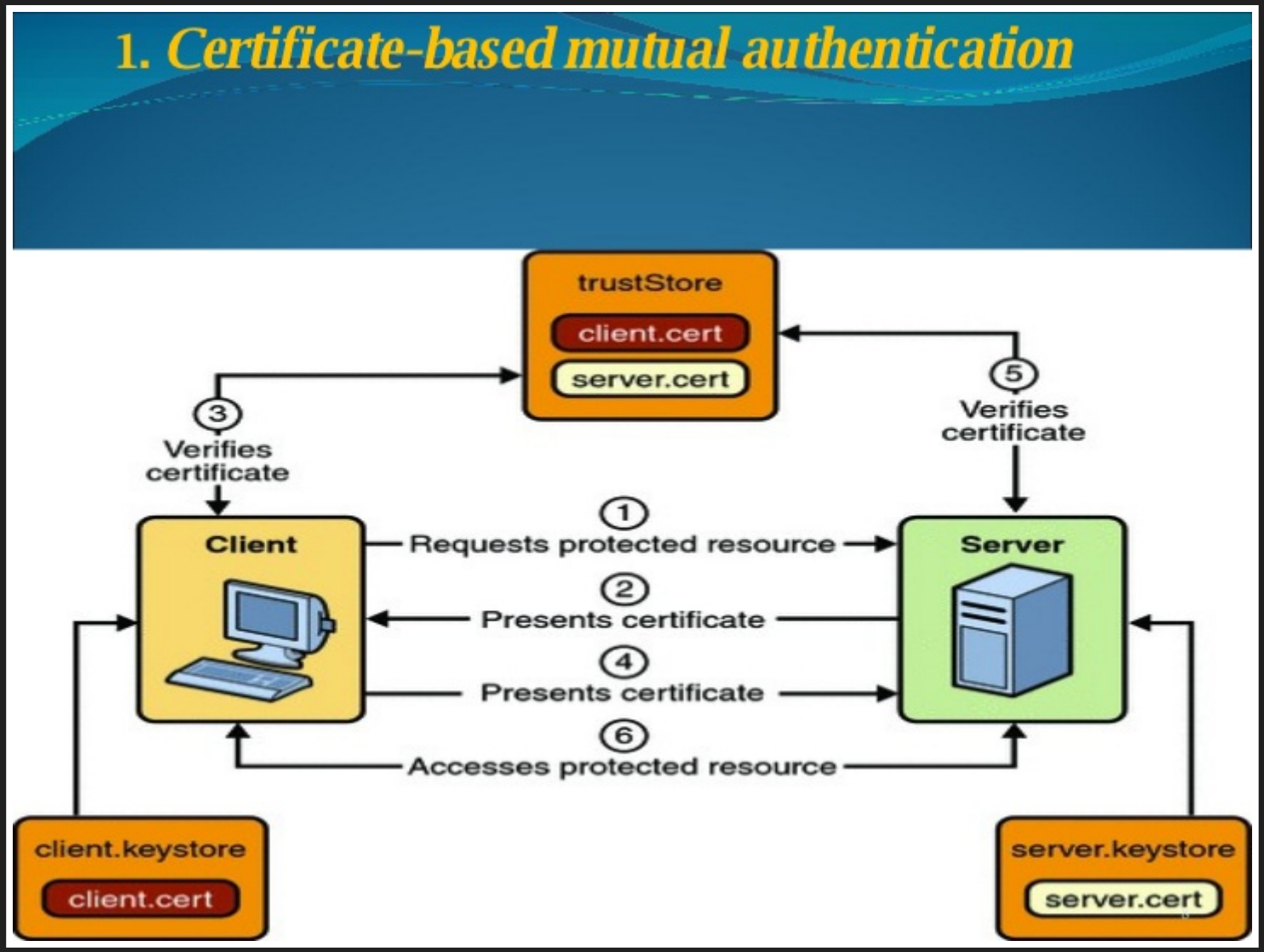
1. Communicating securely
2. Signing documents
3. Authenticating users
4. Exchanging keys

SECURITY SERVICES OF CRYPTOGRAPHY

1. Authentication
2. Non-Repudiation
3. Confidentiality
4. Data Integrity

AUTHENTICATION

- Using cryptography, it is possible to identify a remote user (or system), e.g., via SSL certificates.

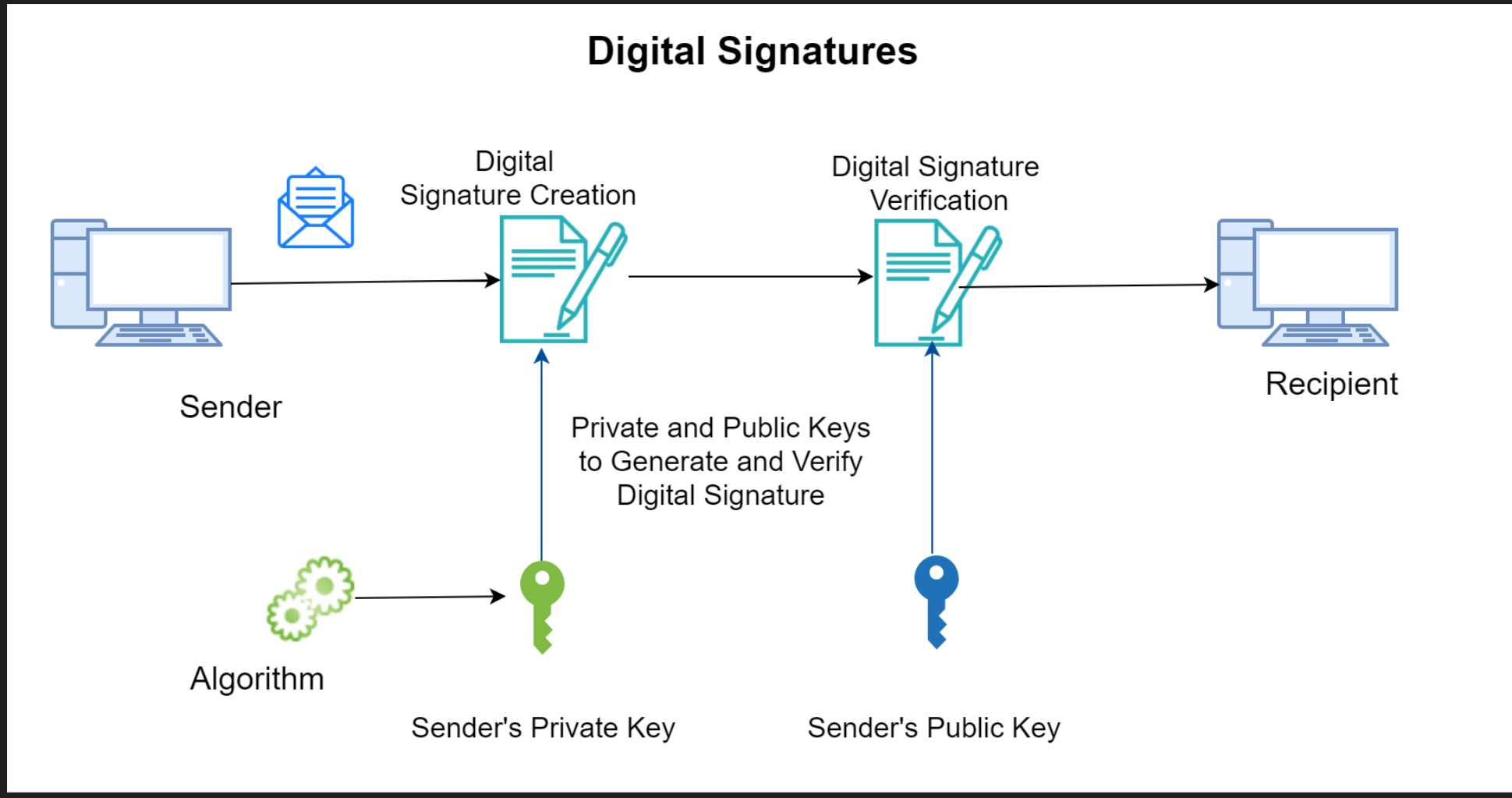


"https://image.slidesharecdn.com/mutual-authentication-for-wireless-communication-

1220180143497412-9/95/mutual-authentication-for-wireless-communication-8-728.jpg?cb=1220155117"

NON-REPUDIATION

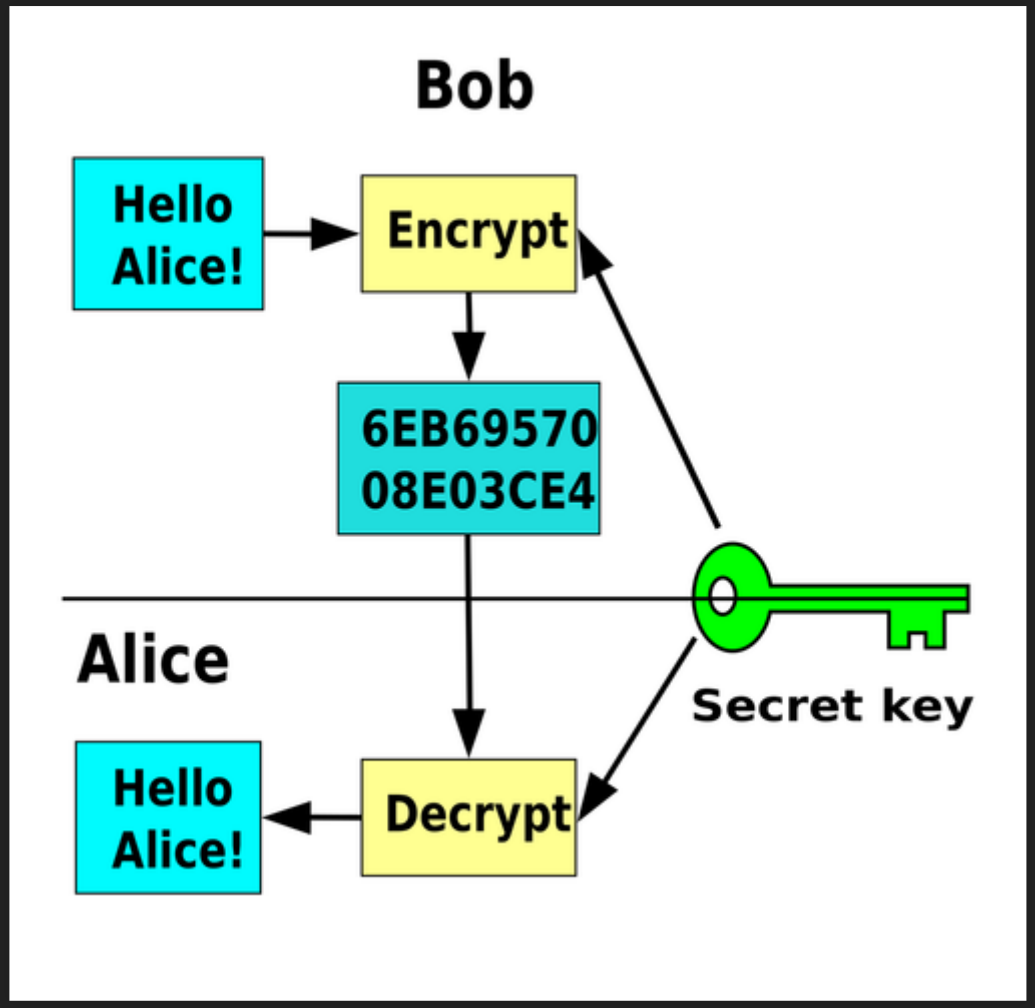
- By **digitally signing** a transaction request, it is possible to ensure non-repudiation (i.e., guarantee that a specific user authorized the transaction) on a financial or an e-commerce application.



"http://blog.infinitysltn.co.in/wp-content/uploads/2017/11/Digital-Signature.png"

CONFIDENTIALITY

- It is a security service that keeps the information from an unauthorized person.
- Sensitive data could be stored and transferred securely through **data encryption**.



"http://cybervaultsec.com/wp-content/uploads/2017/07/Symmetric_key_encryption.p

DATA INTEGRITY

- It deals with **identifying any alteration** to the data.
- Cryptographic hashes could provide a secure **checksum** to check if data was altered during storage or transmission.
- It cannot prevent the alteration of data, but provides a means for **detecting** whether data has been manipulated in an unauthorized manner.

ASSUMPTIONS OF ATTACKER

1. Details of the Encryption Scheme
2. Availability of Ciphertext
3. Availability of Plaintext and Ciphertext

DETAILS OF ENCRYPTION SCHEME

- The first assumption about security environment is that the *encryption algorithm* is known to the attacker.

AVAILABILITY OF CIPHERTEXT

- We know that once the plaintext is encrypted into ciphertext, it is put on unsecure public channel (say email) for transmission.
- Thus, the attacker can obviously assume that it has access to the ciphertext generated by the cryptosystem.

AVAILABILITY OF PLAINTEXT AND CIPHERTEXT

- There may be situations where an attacker can have access to plaintext and corresponding ciphertext, e.g., the attacker influences the sender to convert plaintext of his choice and obtains the ciphertext.

CRYPTANALYTIC ATTACKS

1. Ciphertext-only attack (COA)
2. Known-plaintext attack (KPA)
3. Related-key attack
4. etc.

CIPHERTEXT-ONLY ATTACK (COA)

- The attacker is assumed to have access only to a set of ciphertexts.
- Aim is to determine corresponding plaintext (or encryption key) from a given set of ciphertexts.
- Modern cryptosystems are guarded against this attack.

KNOWN-PLAINTEXT ATTACK (KPA)

- The attacker knows the plaintext for some parts of the ciphertext.
- Aim is to decrypt the rest of the ciphertext by determining the key or via some other method.
- The best example of this attack is linear cryptanalysis against block ciphers.

RELATED-KEY ATTACK

- The attacker can observe the operation of a cipher under several different keys whose values are initially unknown, but where some **mathematical relationship connecting the keys** is known to the attacker.
- e.g., the last 80 bits of the keys are always same.

PRACTICE LINKS

1. Decrypting RSA (Attack): https://www.riddhishree.com/posts/decrypting_rsa/
2. Cryptopals Challenges (that demonstrate attacks on real-world crypto): https://cryptopals.com/
3. Cryptool for Cryptography & Cryptanalysis https://www.cryptool.org/en/

REFERENCES

* https://youtu.be/68Pqir_moqA
* https://www.owasp.org/index.php/Guide_to_Cryptography
* https://en.wikipedia.org/wiki/Cryptography
* https://en.wikipedia.org/wiki/Ciphertext-only_attack
* https://en.wikipedia.org/wiki/Known-plaintext_attack
* https://en.wikipedia.org/wiki/Chosen-plaintext_attack
* https://en.wikipedia.org/wiki/Related-key_attack
* https://en.wikipedia.org/wiki/Man-in-the-middle_attack
* https://www.veracode.com/security/man-middle-attack
* https://www.thesslstore.com/blog/
  difference-sha-1-sha-2-sha-256-hash-algorithms/

REFERENCES (CONTD.)

* https://www.coursera.org/learn/crypto
* https://www.tutorialspoint.com/cryptography/attacks_on_cryptosystems.htm
* https://www.youtube.com/watch?v=60RnrDA4SvE&feature=youtu.be
* https://www.youtube.com/watch?v=gtyh8V5ootA&feature=youtu.be
* https://www.tutorialspoint.com/cryptography/modern_cryptography.htm
* https://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/crypto.html
* http://www.inf.unibz.it/dis/teaching/INFSEC/slides/chapter4.pdf
* https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Chosen_plaintext_attack.html

Thank You!