Steganography

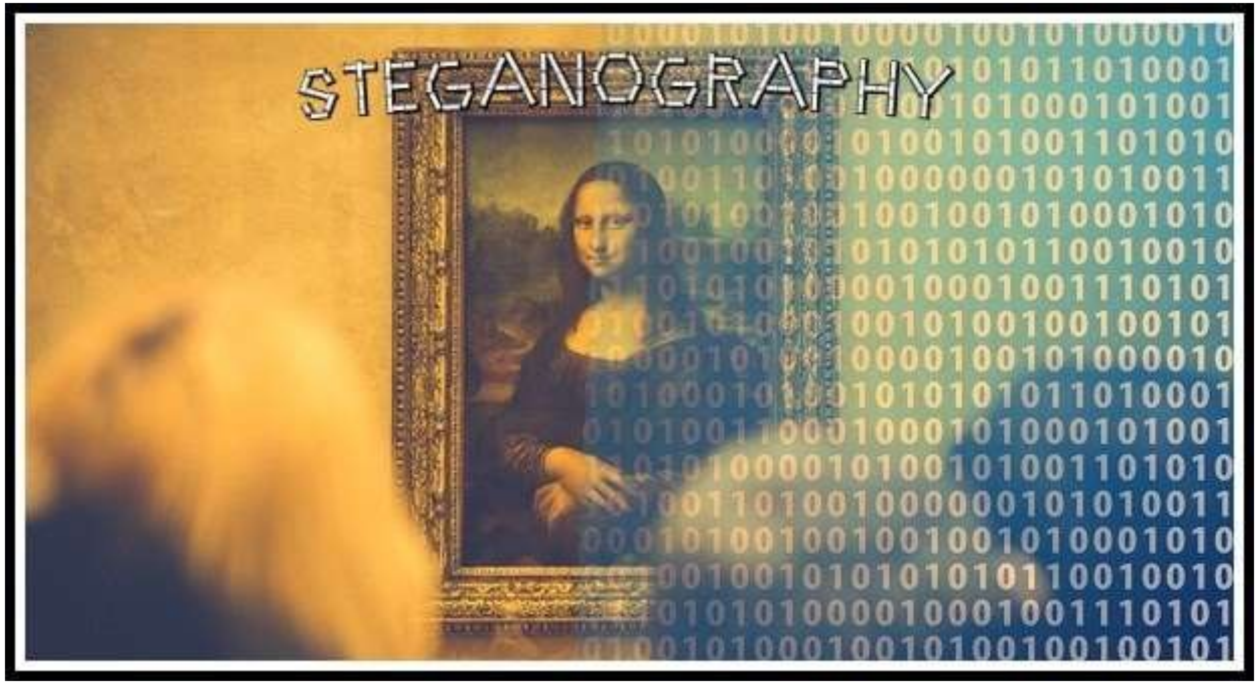
- Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender & intended recipient knows of the existence of the message.
- The word steganography is of Greek origin words steganos (στεγανός), meaning "covered or protected", and graphei (γραφή) meaning "writing".
- Steganography takes one piece of information and hides it within another.
- Both are used to protect information but steganography is concerned with hiding information thereby making it unseen while cryptography is concerned with encrypting information thereby making it unreadable.

Contd....

- Types of Steganography:

  1. Audio steganography
  2. Video steganography
  3. Textual steganography
  4. Image steganography

Steganography

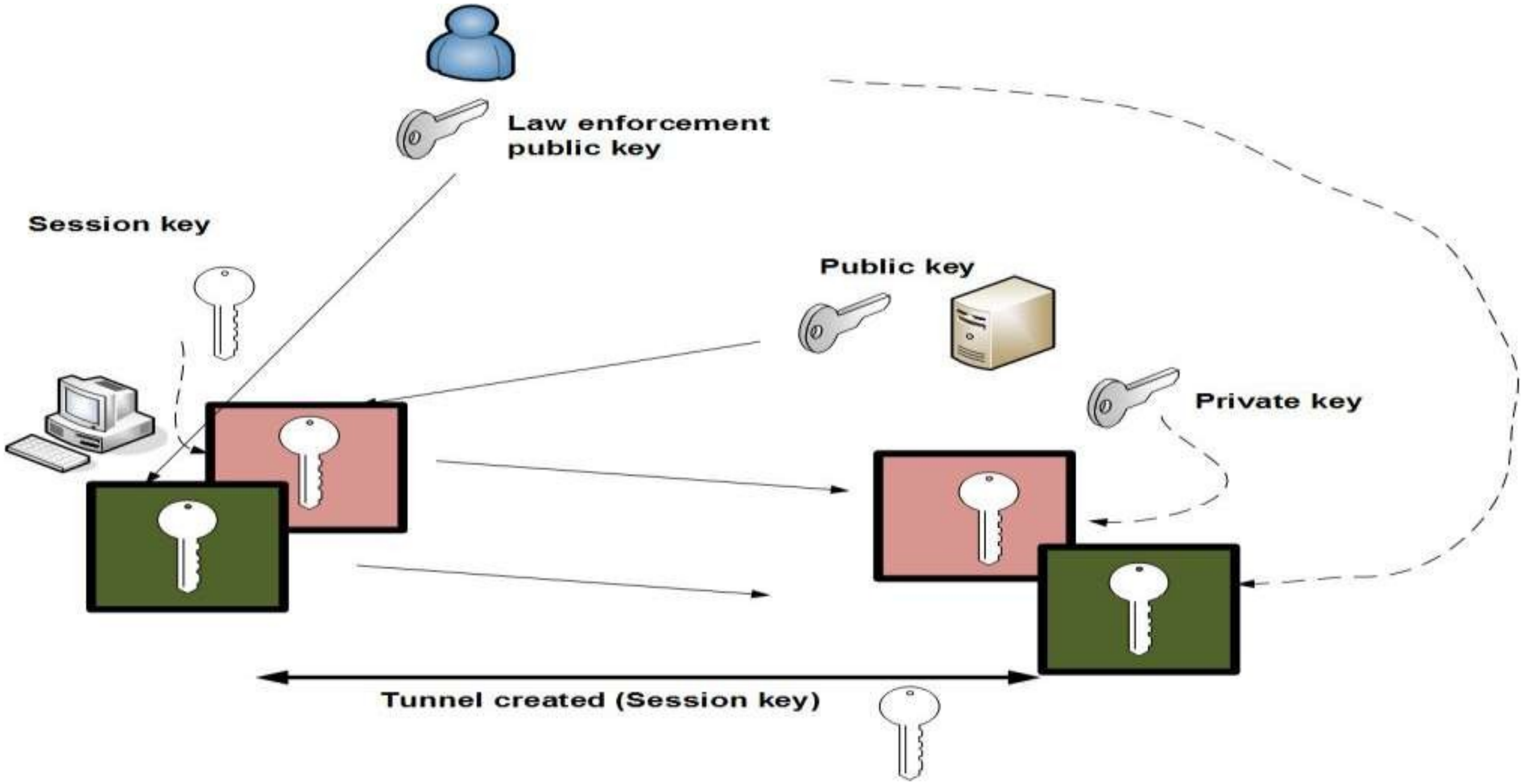


Hiding the code
message

Key escrow

- Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.
- Key escrow systems provide a backup source for cryptographic keys. Escrow systems are somewhat risky because a third party is involved[8].

Key escrow

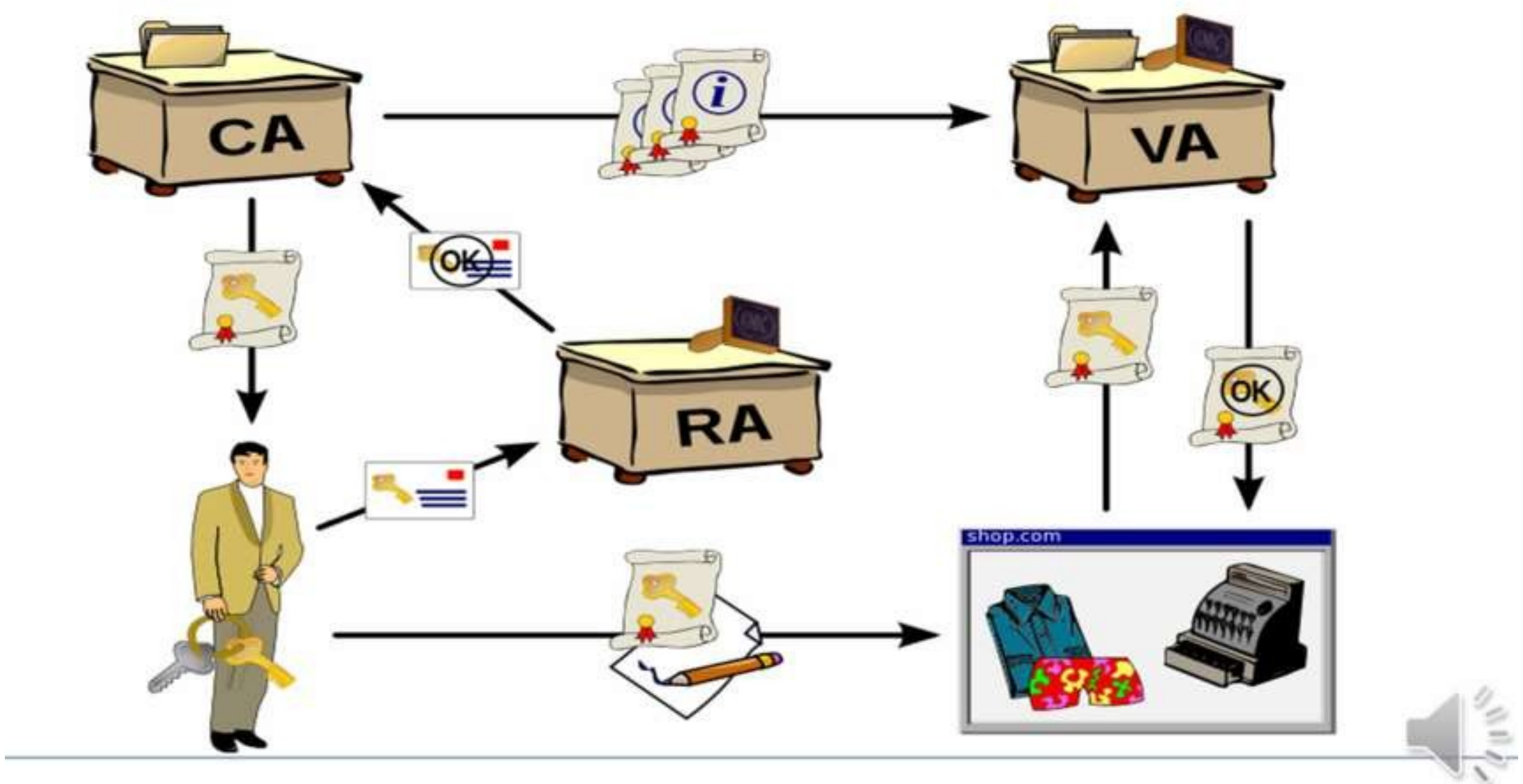


Law enforcement public key
Session key
Public key
Private key
Tunnel created (Session key)

PKI (PUBLIC KEY INFRASTRUCTURE)

- ❑ A public key infrastructure (PKI) is a fixed of roles, policies, hardware, software and processes had to create, manage, distribute, use, save and revoke virtual certificates and manipulate public-key encryption.
- ❑ The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
- ❑ In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations).

Diagram of a public key infrastructure



PKI

A PKI consists of:

- A certificate authority (CA) that stores, issues and signs the digital certificates;
- A registration authority (RA) which verifies the identity of entities requesting their digital certificates to be stored at the CA;
- A central directory—i.e., a secure location in which keys are stored and indexed;
- A certificate management system managing things like the access to stored certificates or the delivery of the certificates to be issued;
- A *certificate policy* stating the PKI's requirements concerning its procedures. Its purpose is to allow outsiders to analyze the PKI's trustworthiness