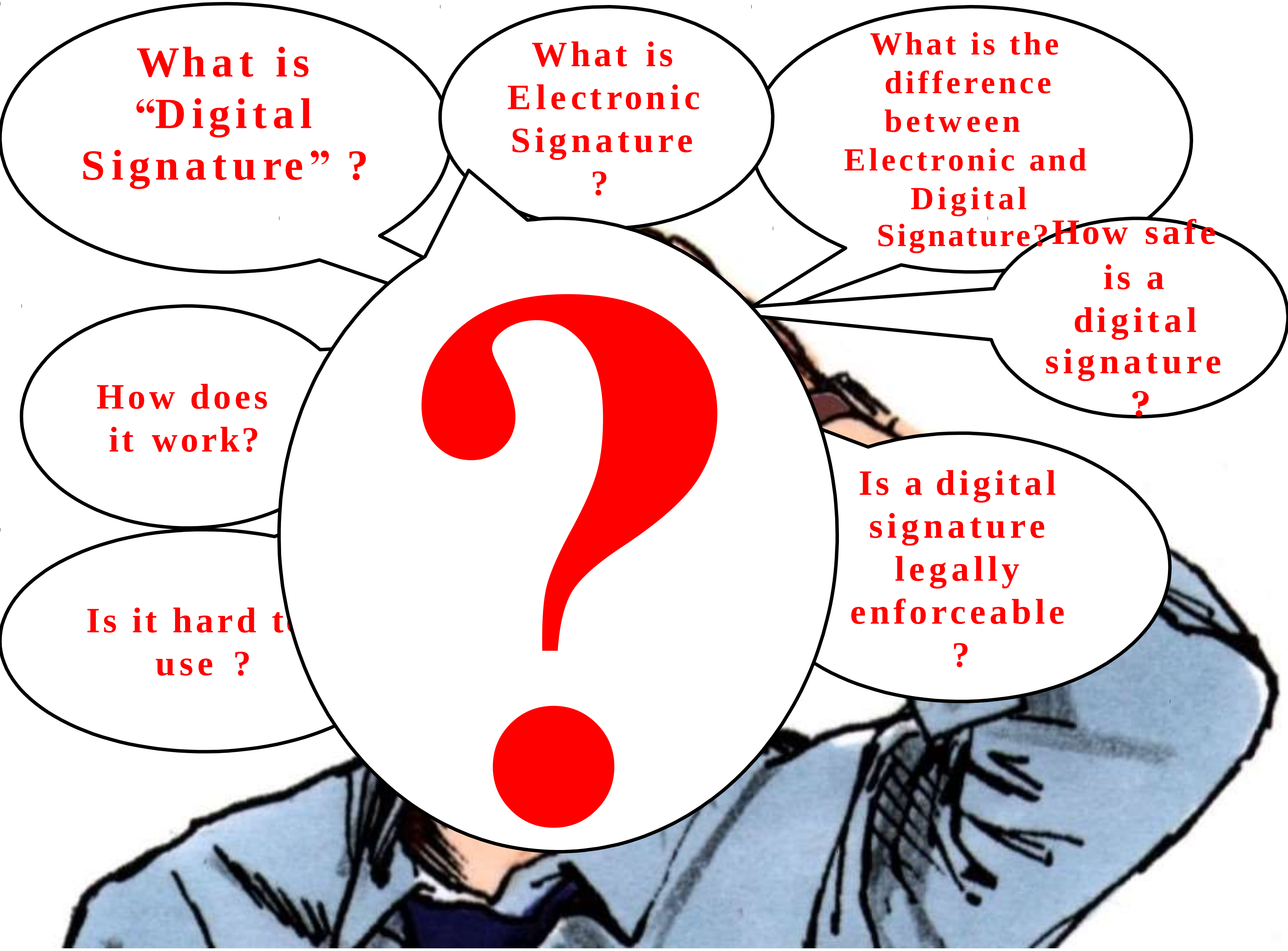
Course Name – B.A.LL.B 4th sem/ LL.B 2nd sem

Subject – Cyber Law

Teacher – Mrs. Aakanksha

Concept – Digital Signature

Digital Signature



What is “Digital Signature” ?

What is Electronic Signature ?

What is the difference between Electronic and Digital Signature?

How safe is a digital signature ?

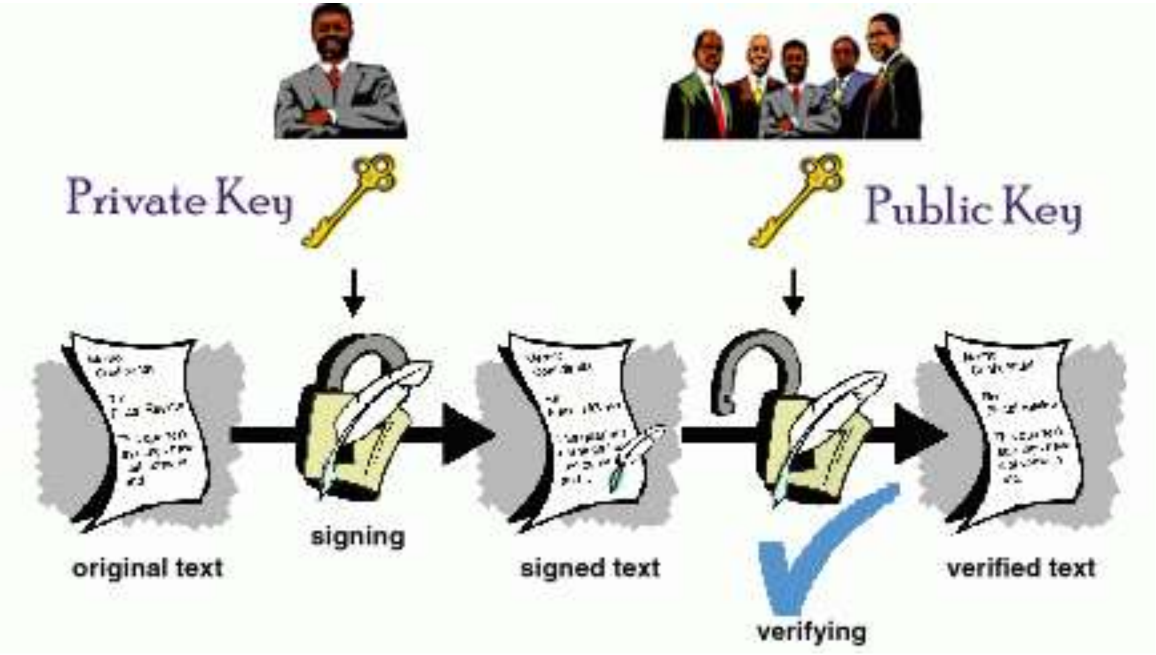
How does it work?

Is it hard t
use ?

Is a digital signature legally enforceable ?

What is Digital Signature?

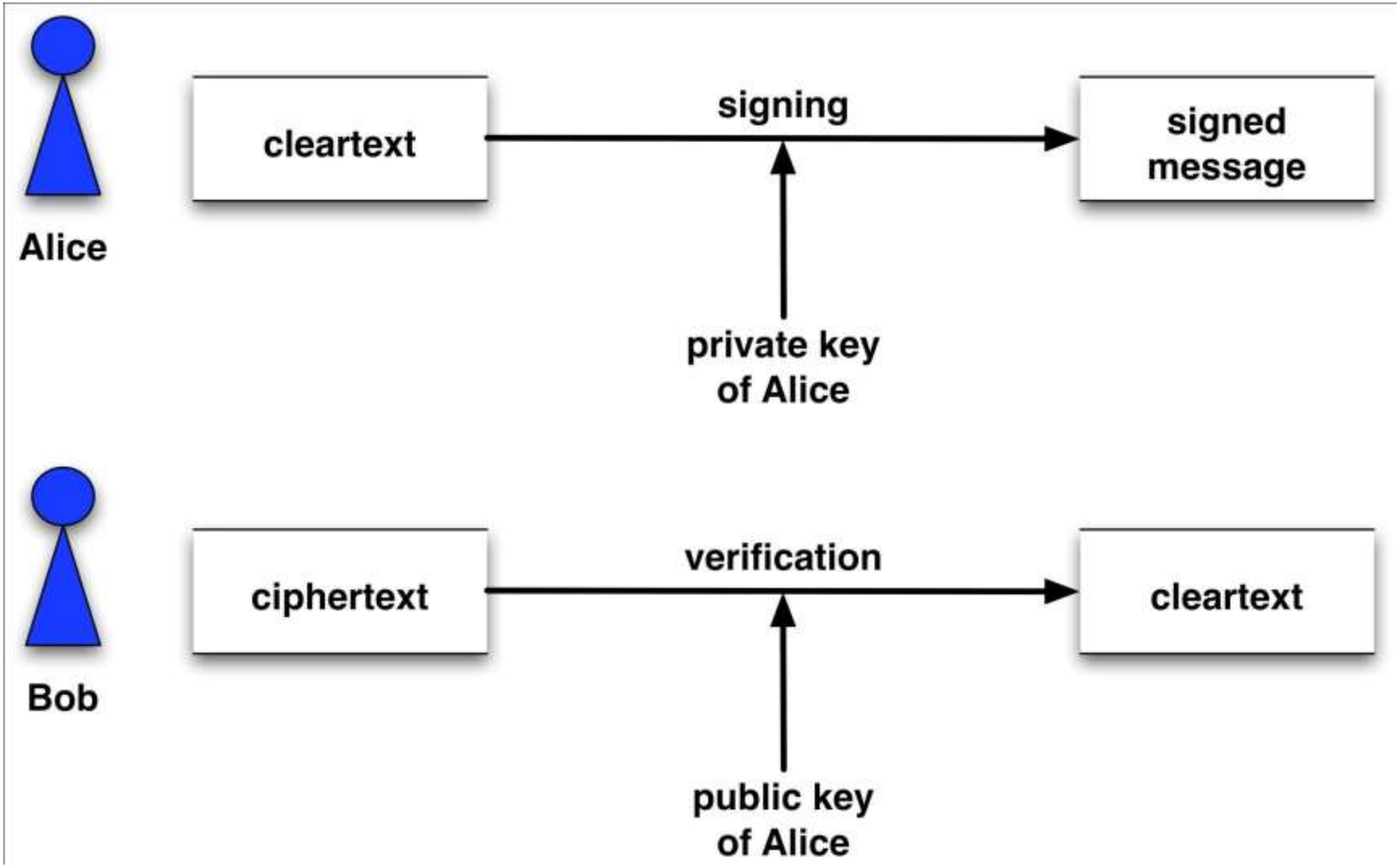
- Digital Signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.
- A digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds them together.
- It is used to validate the authenticity and integrity of a message, software or *digital* document. Digital signatures cryptographically bind an electronic identity to an electronic document and the signature cannot be copied to another document.


Private Key
Public Key
signing
original text
signed text
verifying
verified text

What is Digital Signature?

- Digital signature technique is based on public key cryptography with a difference.
- In public key cryptography a pair of keys are used, one public key and one private key. The public key is often used for message encryption , and the private key is often used for decrypting the message.
- However in case of digital signature message is encrypted with the private key and decrypted with the public key.
- Only a specific person with the corresponding private key can encrypt the message or in other words sign the message. However any party who has the signatory's public key can encrypt the message, in other words can verify the message.

How to Use?


Alice
cleartext
signing
signed message
private key of Alice
Bob
ciphertext
verification
cleartext
public key of Alice

Confidentiality Issues

- It should be possible for the receiver of a message to ascertain its origin. An intruder should not be able to masquerade as someone else.
- It should be possible for the receiver of a message to verify that it has not been modified in transit. An intruder should not be able to substitute a false message for a legitimate one.
- A sender should not be able to falsely deny later that he sent a message.

Attributes of Digital Signature

- Digital signature ensures the confidentiality via the following three attributes:

1. Authentication
2. Integrity
3. Non-repudiation

Attributes of Digital Signature

- **Authentication:** Authentication means *the act of proving who you say you are.* Authentication means that you know who created and sent the message. Digital signature is used to authenticate the source of messages. It ensures the user of the sender.
- **Integrity:** Integrity ensures that when a message is sent over a network, the data that arrives is the same as the data that was originally sent. Integrity is the assurance that the information is trustworthy and accurate. Digital signature ensures the integrity of message.
- **Non-repudiation:** this is an important criteria of digital signature. As digital signature ensures the authentication of the message, so the sender can't repudiate it later. At the same time it also ensures the identity of the receiver, so the receiver can't repudiate it later.

What is Electronic Signature?

- An electronic signature is a typed name or a scanned image of a handwritten signature.
- As a result, e-signatures are very problematic when it comes to maintaining integrity and security, as nothing prevents one individual from typing another individual's name.
- Due to this reality, an electronic signature that does not incorporate additional measures of security (the way digital signatures do) is considered an insecure way of signing documentation.

Difference Between Digital and Electronic Signature

- A digital signature, often referred to as advanced or standard version of electronic signature, that provides the highest levels of security and universal acceptance.
- Digital signatures are based on Public Key Infrastructure (PKI) technology, and guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents. The digital signature cannot be copied, tampered with or altered.

Difference Between Digital and Electronic Signature

- In addition, because digital signatures are based on standard PKI technology, they can be validated by anyone without the need for proprietary verification software.
- On the other hand, there is no standard format for electronic signatures that may be a digitized image of a handwritten signature, a symbol, voiceprint, etc., used to identify the author(s) of an electronic message.
- An electronic signature is vulnerable to copying and tampering, and invites forgery. In many cases, electronic signatures are not legally binding and will require proprietary software to validate the e-signature.

Is Digital Signature Legally Enforceable?

“Yes”

- As per section 3 of the information Technology Act 2000 , a Digital Signature is legally binding in India. Income Tax act 1961 also approves digital signature in the case of tax filling.

- Today, digital signature (standard electronic signature) solutions carry recognized legal significance, enabling organizations to comply with regulations worldwide.