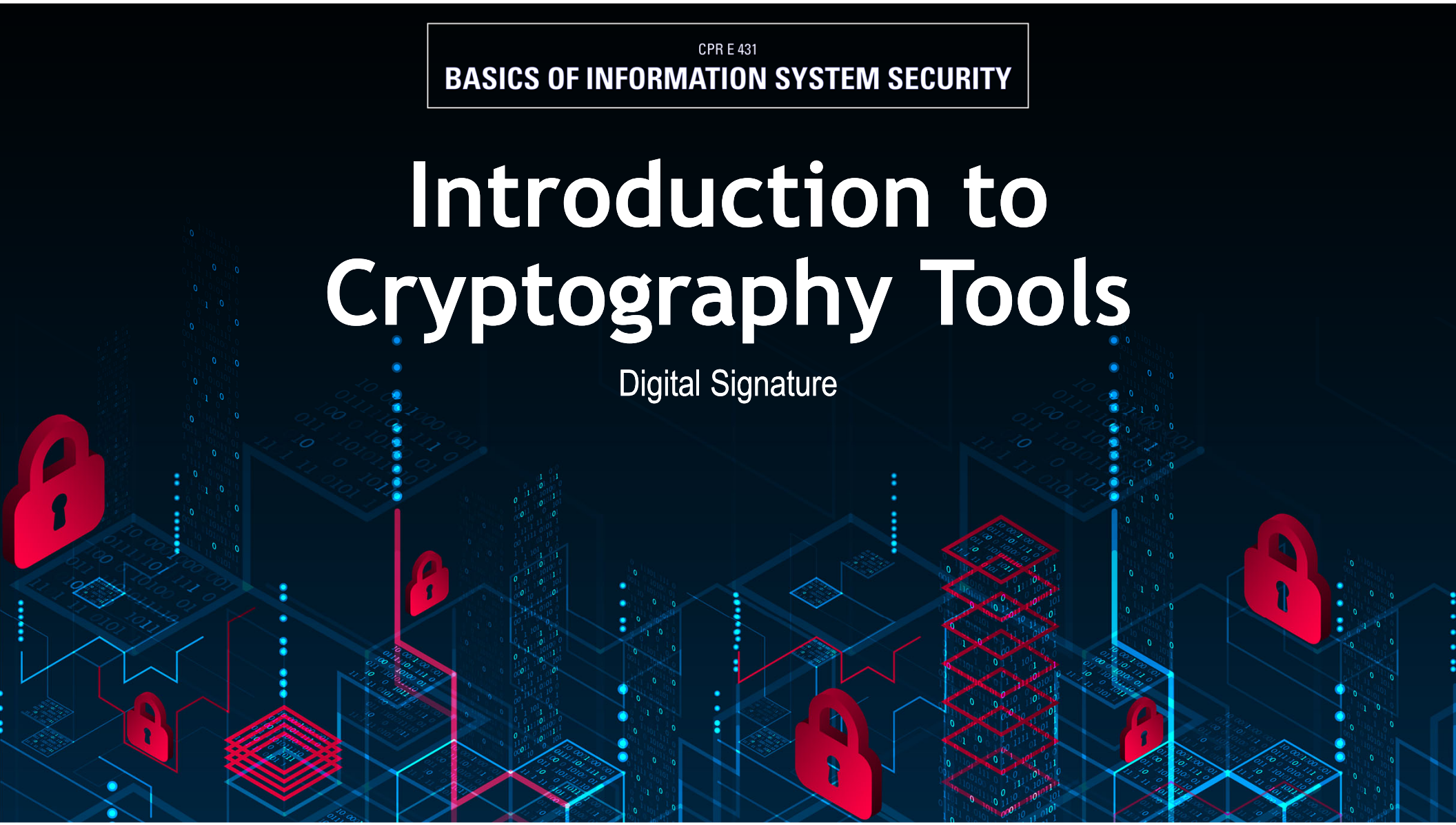
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Digital Signature



Video Summary

- What is a Digital Signature
- Applications of Digital Signature
- Digital Signature (Symmetric vs Asymmetric Keys)
- Digital Signature Example
- Digital Signature Operations

What is Digital Signature

- A digital signature is equivalent to handwritten signature
- It is an electronic verification of the sender

Purpose of Digital Signature:

User Authentication

Data Authentication (Data Integrity)

Non-repudiation

Digital Signature

- Applications of Digital Signature
  - **Sensitive Email Communications**
  - **Financial Transactions**
  - **Software Distribution**

Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:

  ”The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and non-repudiation.”

- Digital signature algorithms:
  - Digital Signature Algorithm (DSA)
  - RSA Digital Signature Algorithm
  - Elliptic Curve Digital Signature Algorithm (ECDSA)

Digital Signatures (symmetric vs asymmetric)

K_{AB}

K_{AC}

K_{AD}

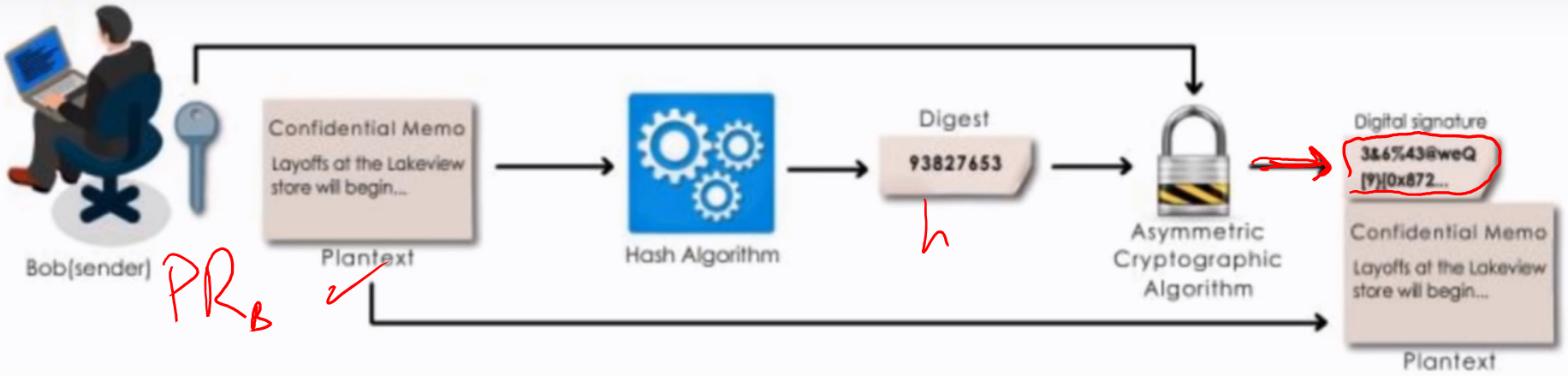
- Symmetric key cryptography
  - Two users, A and B, share a secret key K
  - Receiver of message (user A) can verify that message came from the other user (B)
  - User C *cannot* prove that the message came from B (it may also have came from A)
- Public key cryptography can provide signature: only one user has the private key

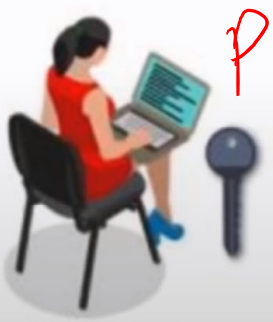
  - Digital Signature uses Public Key Encryption

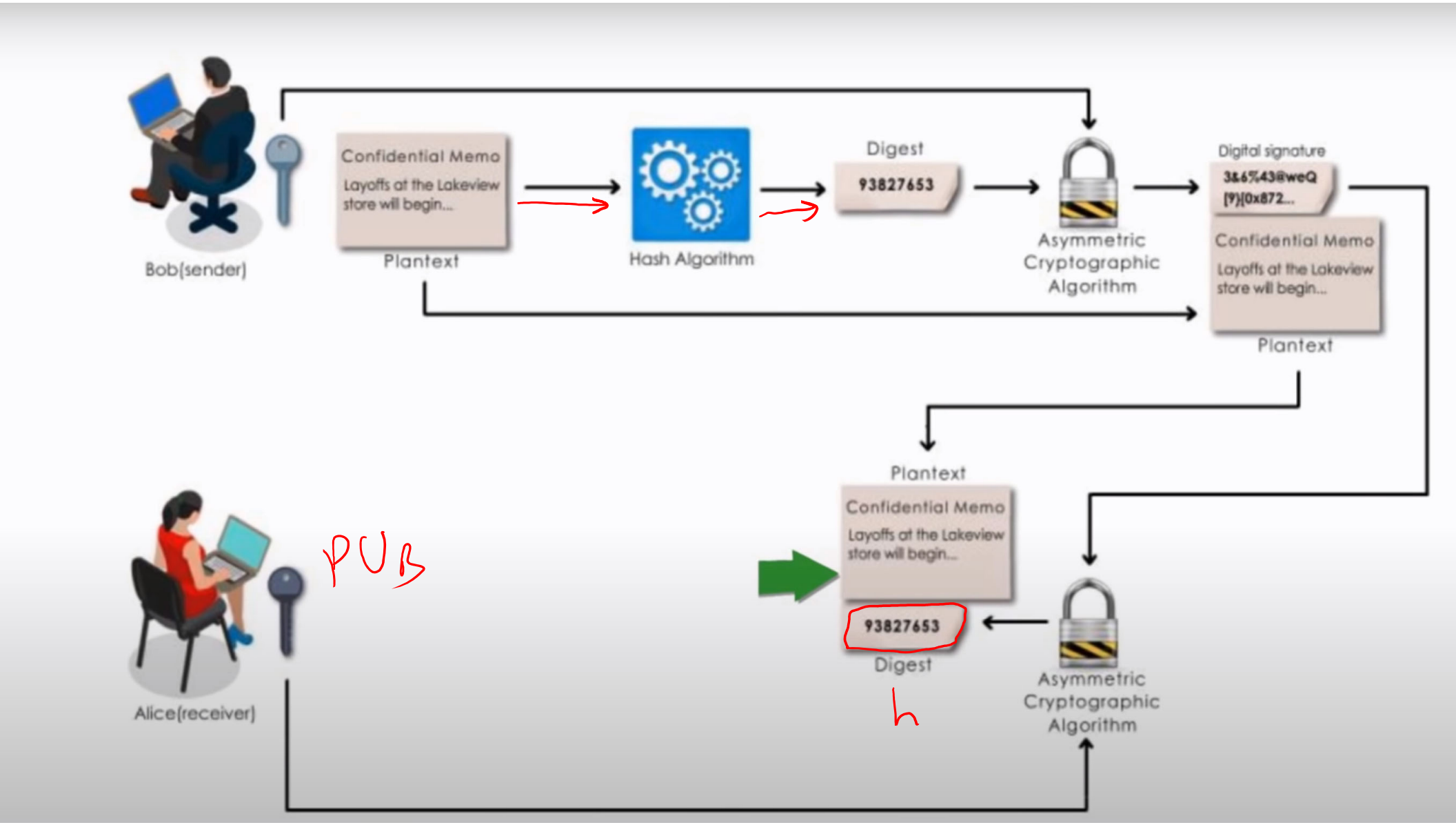
Digital Signature Example

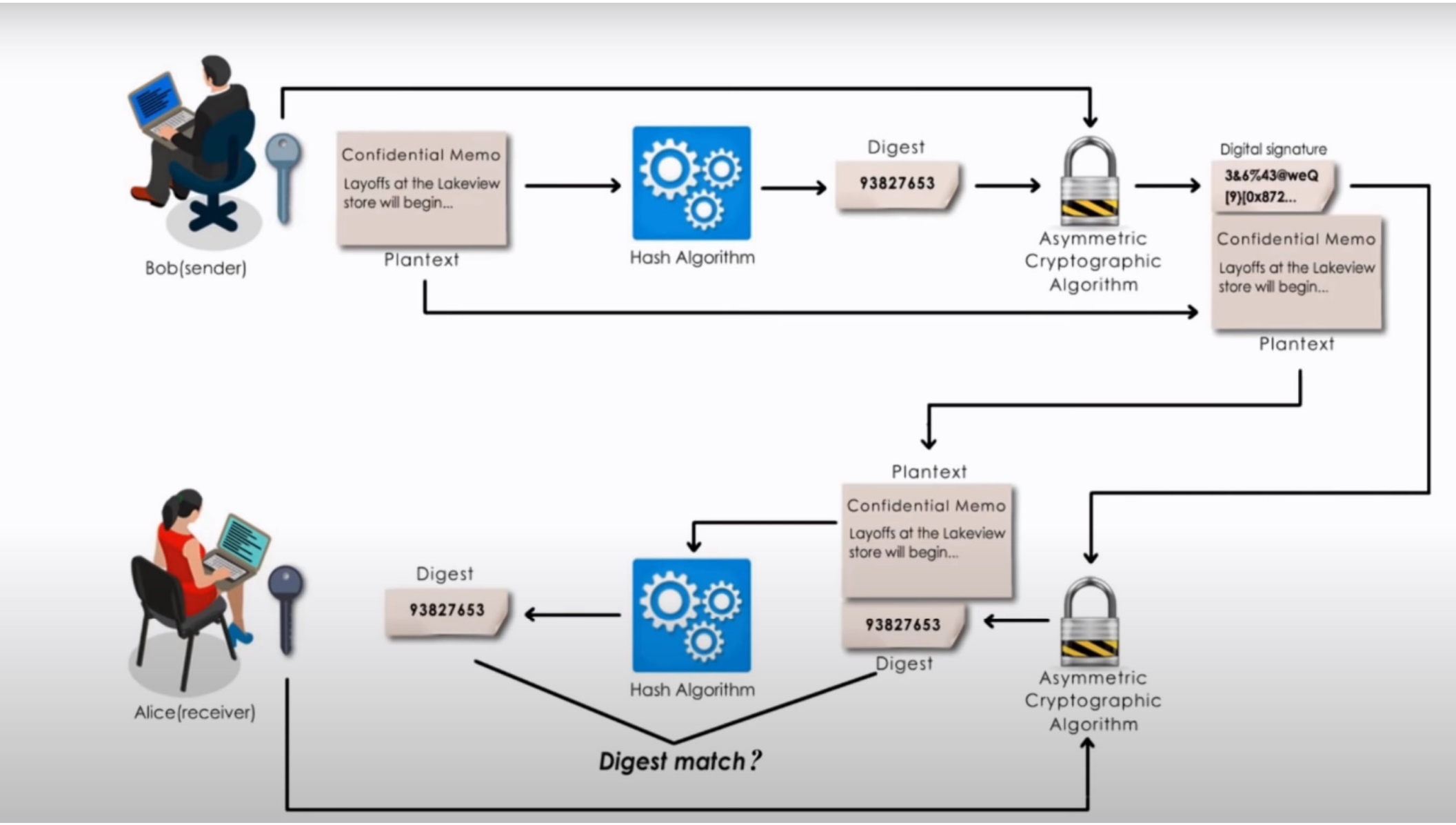
- Suppose Bob is going to send a plaintext message to Alice with his unique digital signature using DSA (in this case, he has to generate his own public-private key pairs and then share his public key with Alice).

- For simplicity, we will not encrypt the plaintext since we will concentrate on the digital signature procedures.


Bob(sender)
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext
Hash Algorithm
Digest
93827653
Asymmetric Cryptographic Algorithm
Digital signature
3&6%43@weQ
[9](0x872...
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext


Alice(receiver)


Bob(sender)
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext
Hash Algorithm
Digest
93827653
Asymmetric Cryptographic Algorithm
Digital signature
3&6%43@weQ
[9]{0x872...
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext
Plantext
Confidential Memo
Layoffs at the Lakeview store will begin...
93827653
Digest
Asymmetric Cryptographic Algorithm
Alice(receiver)
PUB
h


Bob(sender)
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext
Hash Algorithm
Digest
93827653
Asymmetric Cryptographic Algorithm
Digital signature
3&6%43@weQ
[9]{0x872...
Confidential Memo
Layoffs at the Lakeview store will begin...
Plantext
Alice(receiver)
Digest
93827653
Hash Algorithm
Plantext
Confidential Memo
Layoffs at the Lakeview store will begin...
93827653
Digest
Asymmetric Cryptographic Algorithm
Digest match?

Digital Signature Operations (Not Practical)

Signing

- User signs a message by encrypting with own private key

$$S = E(PR_A, M)$$

- User attaches signature to message

Verification

- User verifies a message by decrypting signature with signer's public key

$$M' = D(PU_A, S)$$

- User then compares received message M with decrypted M'; if identical, signature is verified

Digital Signature Operations (Practice)

No need to encrypt entire message; encrypt hash of message

Signing

- User signs a message by encrypting hash of message with own private key

$$S = E(PR_A, H(M))$$

- User attaches signature to message

Verification

- User verifies a message by decrypting signature with signer's public key

$$h = D(PU_A, S)$$

Video Summary

- What is a Digital Signature
- Applications of Digital Signature
- Digital Signature (Symmetric vs Asymmetric Keys)
- Digital Signature Example
- Digital Signature Operations