CHITKARA UNIVERSITY

INTRODUCTION TO CRYPTOGRAPHY

Objectives

- Define Cryptography
  - Cryptographic Algorithm
  - Hashing Algorithm
  - Symmetric Algorithm
- Asymmetric Algorithm
- Use of Public and Private Key

Defining Cryptography

CHITKARA UNIVERSITY

- Defining cryptography involves understanding what it is and what it can do
- It also involves understanding how cryptography can be used as a security tool to protect data

What is Cryptography

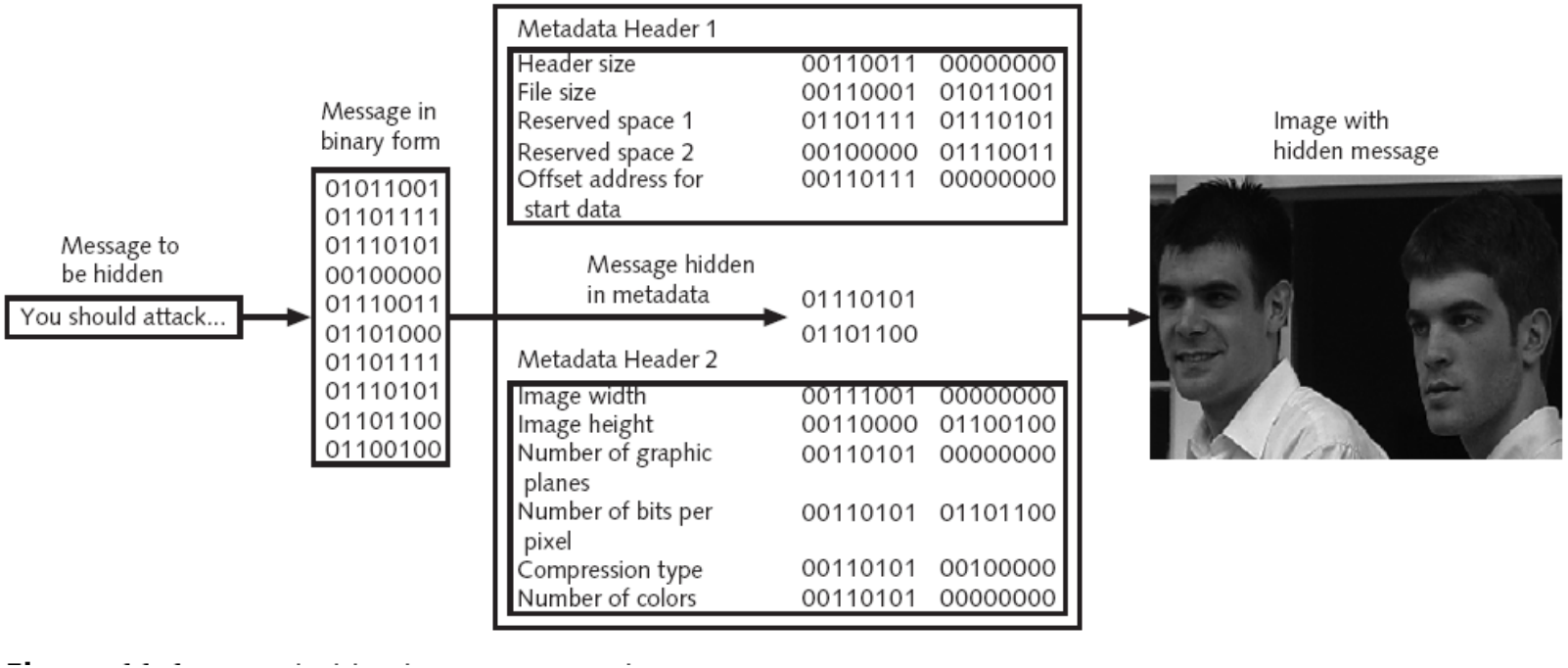
- An important means of protecting information is to “scramble” it so that even if an attacker reaches the data, he cannot read it. This scrambling is a process known as **cryptography.**
- Cryptography is the science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it.

What is Cryptography

CHITKARA UNIVERSITY

- **Cryptography**
  - The science of transforming information into an unintelligible form while it is being transmitted or stored so that unauthorized users cannot access it
- **Steganography**
  - Hides the existence of the data
  - What appears to be a harmless image can contain hidden data embedded within the image
  - Can use image files, audio files, or even video files to contain hidden information

Steganography



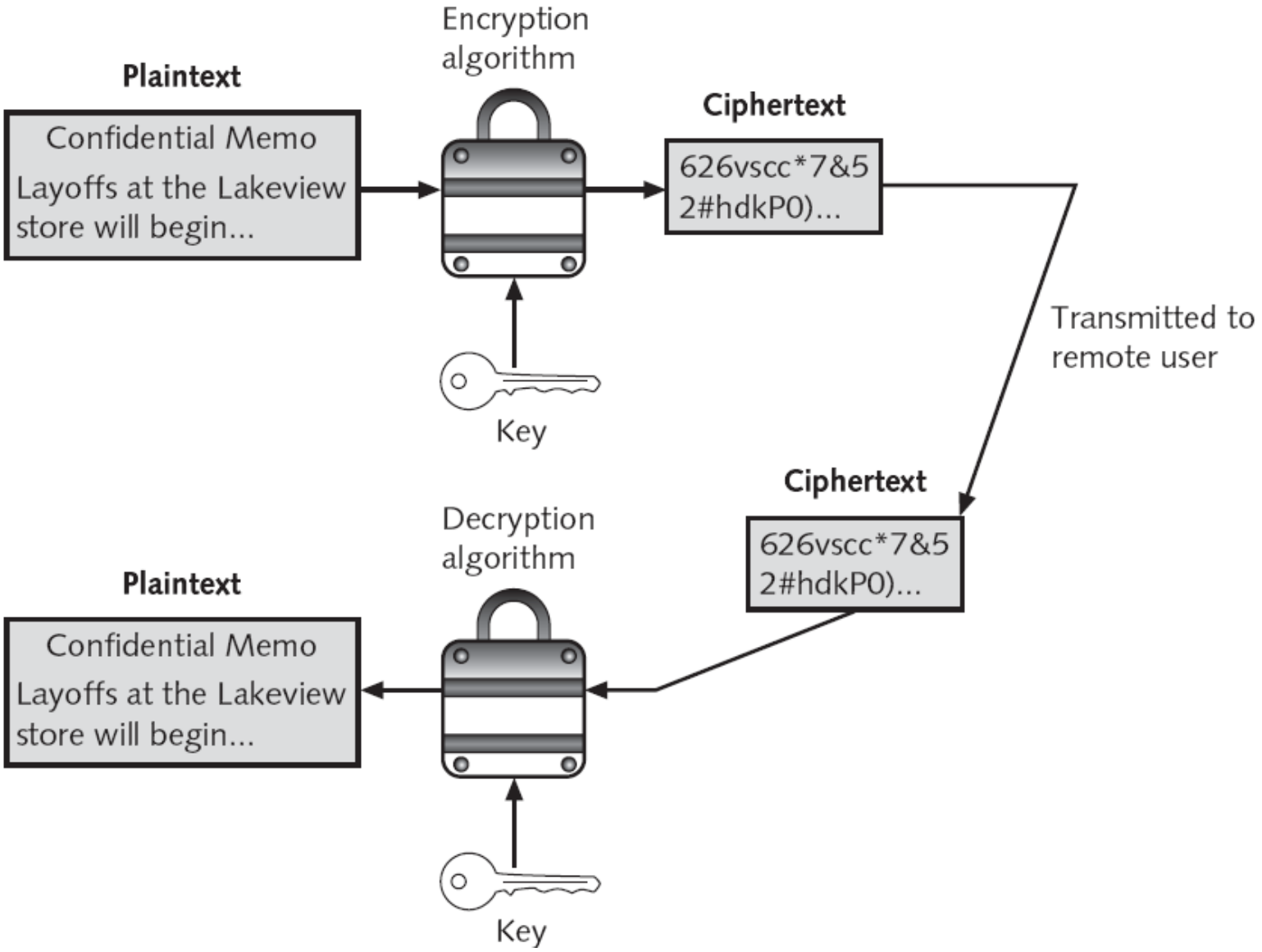
What Is Cryptography? (continued)

CHITKARA UNIVERSITY

- One of the most famous ancient cryptographers was Julius Caesar
- Caesar shifted each letter of his messages to his generals three places down in the alphabet

HELLO→KHOOR

- **Encryption**
  - Changing the original text to a secret message using cryptography
- **Decryption**
  - Change the secret message back to its original form


Encryption algorithm
Plaintext
Confidential Memo
Layoffs at the Lakeview store will begin...
Ciphertext
626vscc*7&5 2#hdkP0)...
Transmitted to remote user
Key
Ciphertext
626vscc*7&5 2#hdkP0)...
Decryption algorithm
Plaintext
Confidential Memo
Layoffs at the Lakeview store will begin...
Key

Cryptography and Security

CHITKARA UNIVERSITY

- Cryptography can provide basic security protection for information:
  - Cryptography can protect the *confidentiality* of information
  - Cryptography can protect the *integrity* of the information
  - Cryptography can help ensure the *availability* of the data
  - Cryptography can verify the *authenticity* of the sender
  - Cryptography can enforce *non-repudiation*

Cryptography and Security (continued)

CHITKARA UNIVERSITY

Characteristic	Description	Protection
Confidentiality	Ensures that only authorized parties can view the information	Encrypted information can only be viewed by those who have been provided the key
Integrity	Ensures that the information is correct and no unauthorized person or malicious software has altered that data	Encrypted information cannot be changed except by authorized users who have the key
Availability	Ensures that data is accessible to authorized users	Authorized users are provided the decryption key to access the information
Authenticity	Provides proof of the genuineness of the user	Cryptography can prove that the sender was legitimate and not an imposter
Non-repudiation	Proves that a user performed an action	Cryptographic non-repudiation prevents an individual from fraudulently denying they were involved in a transaction

Cryptographic Algorithms

CHITKARA UNIVERSITY

- There are three categories of cryptographic algorithms:
  - Hashing algorithms
  - Symmetric encryption algorithms
  - Asymmetric encryption algorithms

Hashing Algorithms

CHITKARA UNIVERSITY

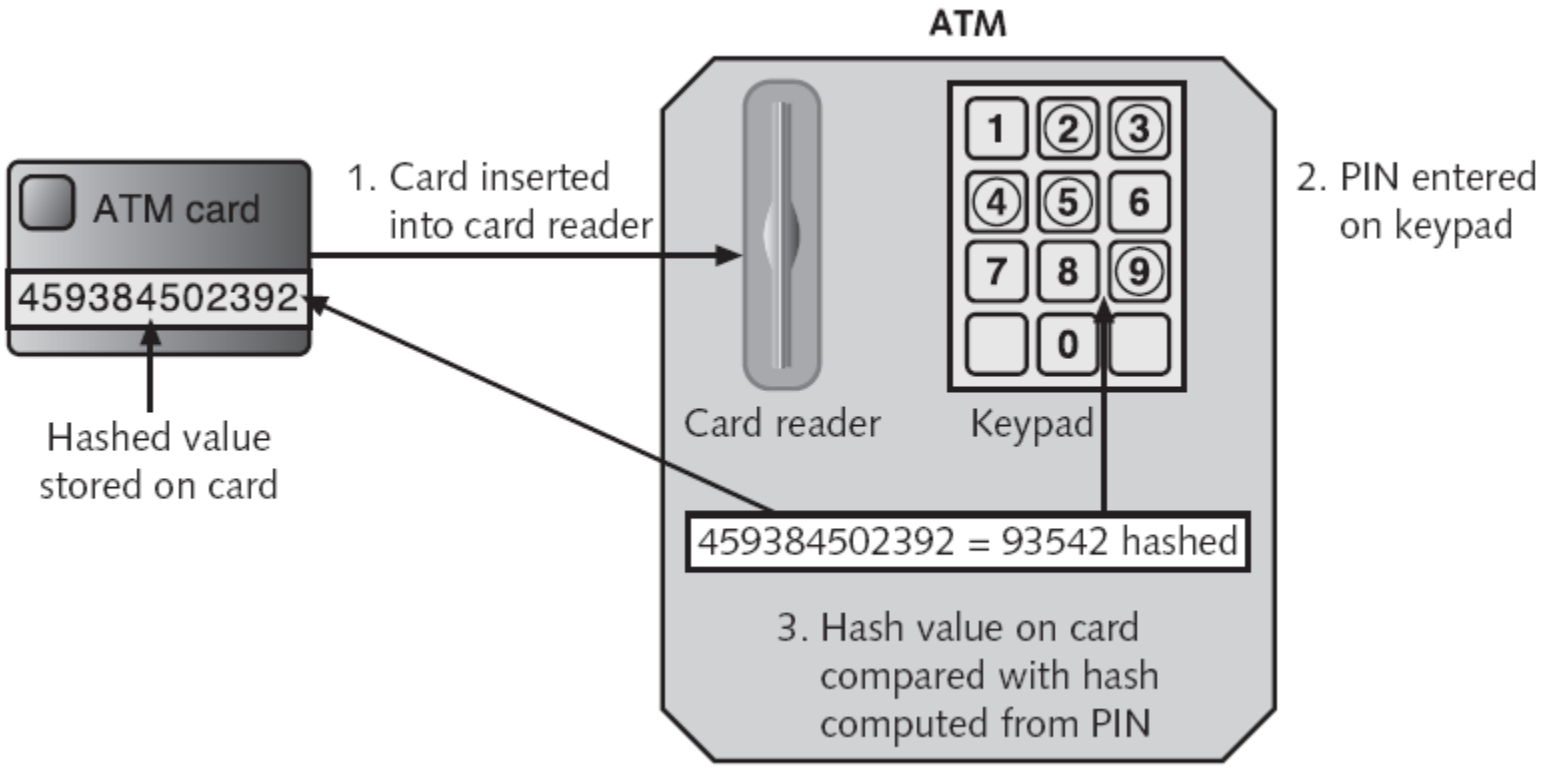
- The most basic type of cryptographic algorithm is a hashing algorithm.
  - Also called a **one-way hash**
  - A process for creating a unique “signature” for a set of data
    - This signature, called a **hash** or **digest**, represents the contents
- Hashing is used only for integrity to ensure that:
  - Information is in its original form
  - No unauthorized person or malicious software has altered the data
- Hash created from a set of data cannot be reversed

Example Hashing Algorithm

CHITKARA UNIVERSITY

- If 12,345 is multiplied by 143, the result is 1,765,335. If the number 1,765,335 was given to a user, and the user was asked to determine the two original numbers used to create 1,765,335, it would be virtually impossible for her to work backward and derive the original numbers. This is because there are too many mathematical possibilities (1765334+1, 665334+100000, 2222222–456887, etc.).
- Similarly Hashing is used to create a value.

Hashing Algorithms (continued)

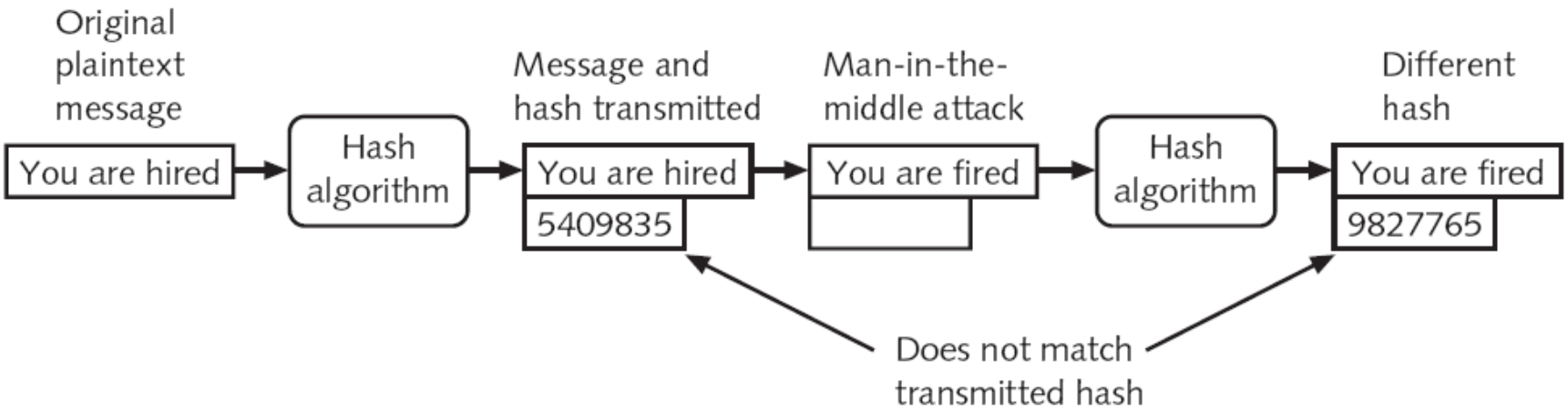


Hashing Algorithms (continued)

CHITKARA UNIVERSITY

- A hashing algorithm is considered secure if it has these characteristics:
  - The ciphertext hash is a fixed size
  - Two different sets of data cannot produce the same hash, which is known as a **collision**
  - It should be impossible to produce a data set that has a desired or predefined hash
  - The resulting hash ciphertext cannot be reversed
- The hash serves as a check to verify the message contents

Hashing Algorithms (continued)



Hashing Algorithms (continued)

CHITKARA UNIVERSITY

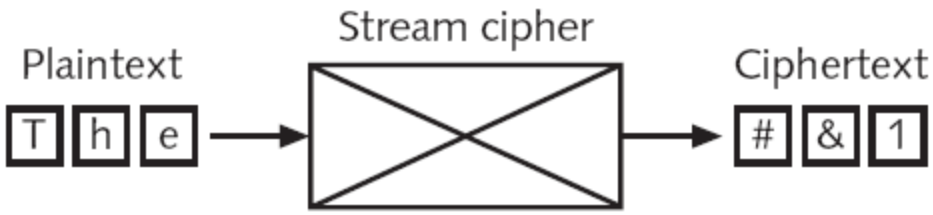
Characteristic	Protection?
Confidentiality	No
Integrity	Yes
Availability	No
Authenticity	No
Non-repudiation	No

Symmetric Cryptographic Algorithms

CHITKARA UNIVERSITY

- **Symmetric cryptographic algorithms**
  - Use the same single key to encrypt and decrypt a message
  - Also called private key cryptography
- **Stream cipher**
  - Takes one character and replaces it with one character
- **Substitution cipher**
  - The simplest type of stream cipher
  - Simply substitutes one letter or character for another

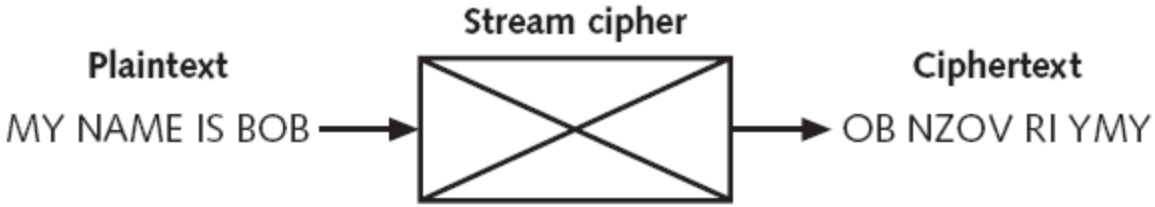
Symmetric Cryptographic Algorithms



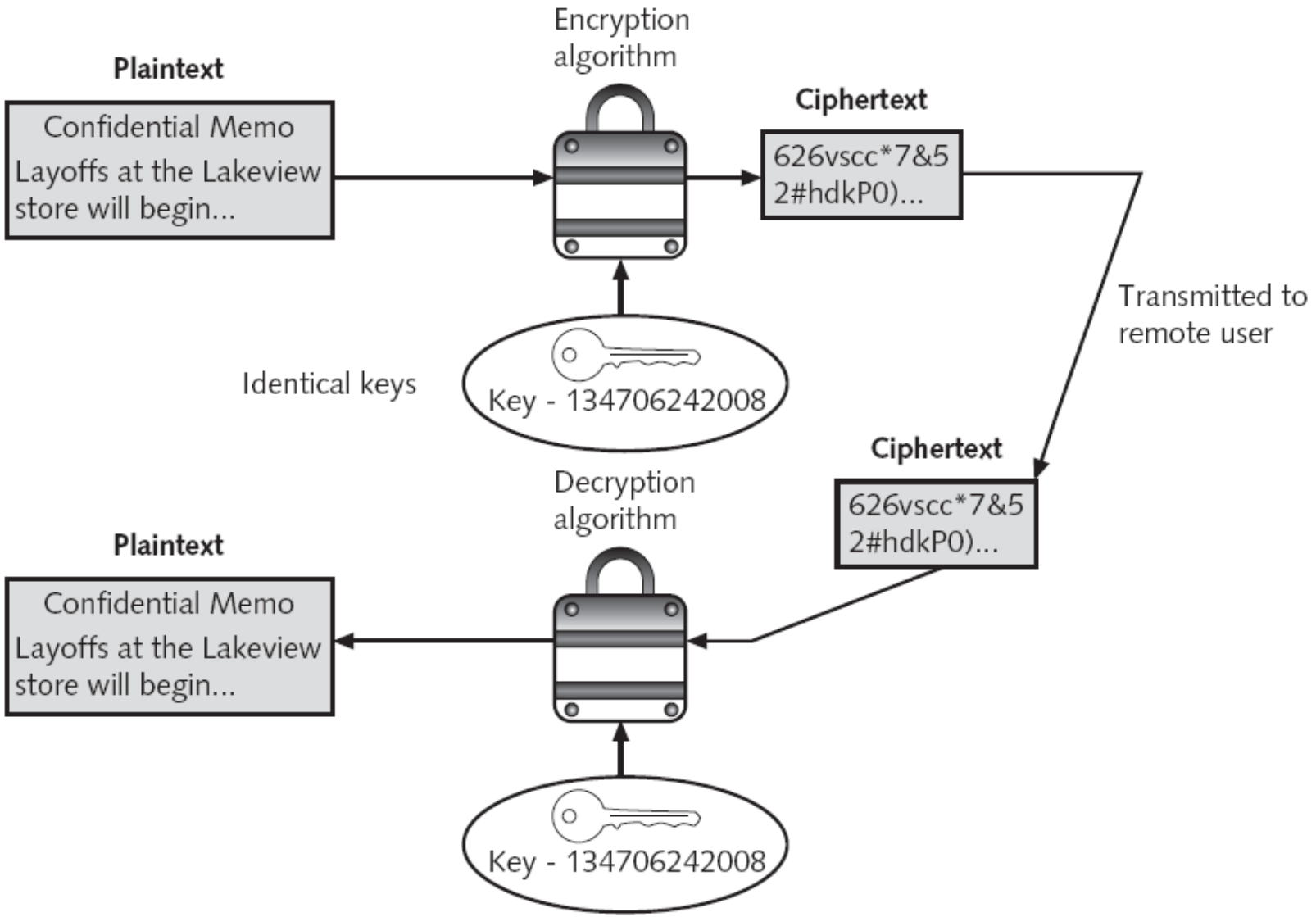
Stream Cipher

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z - **Plaintext letters**

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A - **Substitution letters**



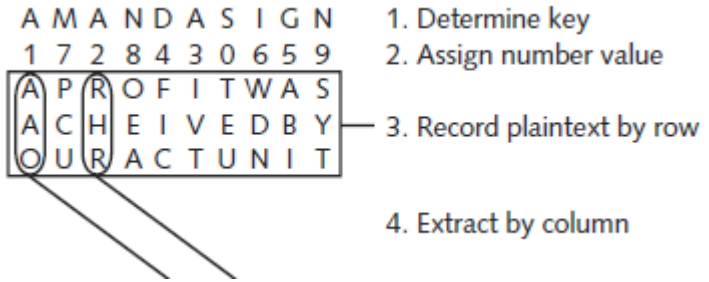
Substitution Cipher


Encryption algorithm
Plaintext
Confidential Memo
Layoffs at the Lakeview store will begin...
Ciphertext
626vscc*7&5 2#hdkP0)...
Transmitted to remote user
Identical keys
Key - 134706242008
Ciphertext
626vscc*7&5 2#hdkP0)...
Decryption algorithm
Plaintext
Confidential Memo
Layoffs at the Lakeview store will begin...
Key - 134706242008

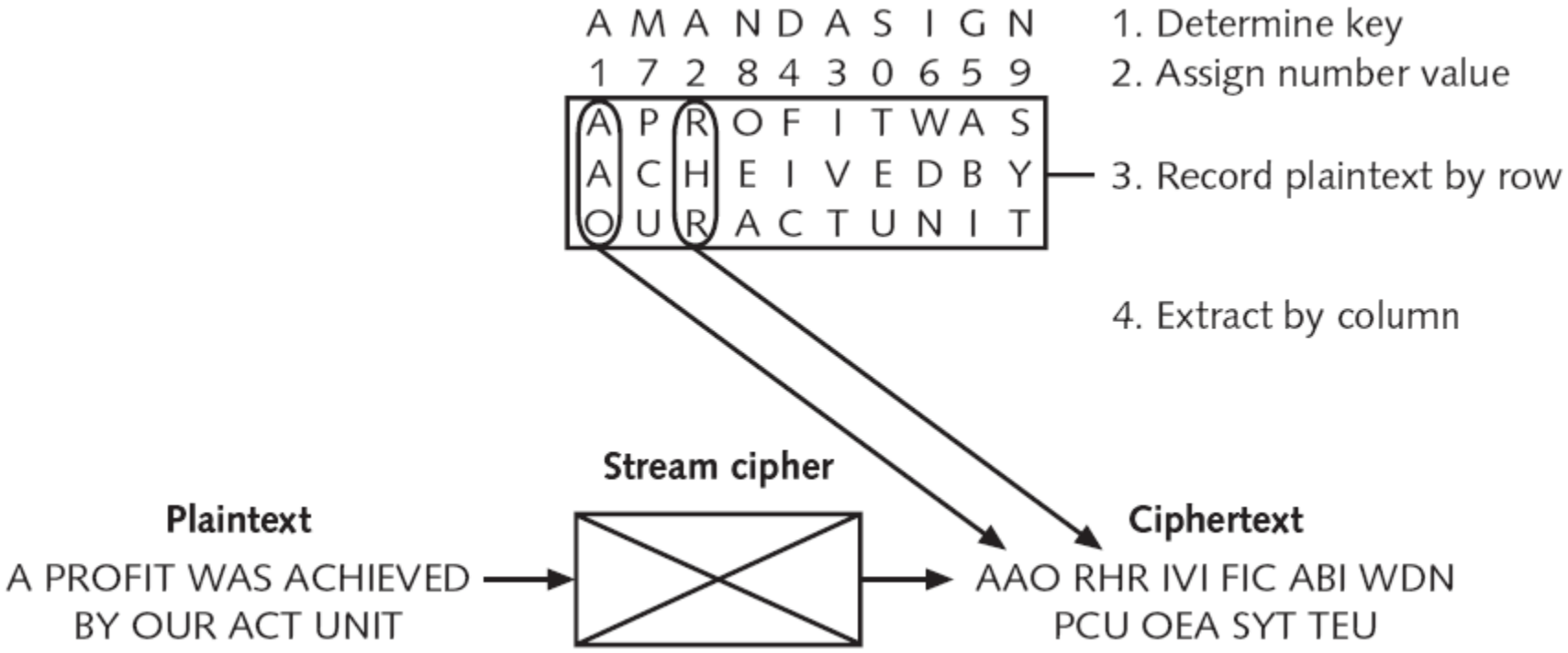
Transposition Stream Cipher

CHITKARA UNIVERSITY

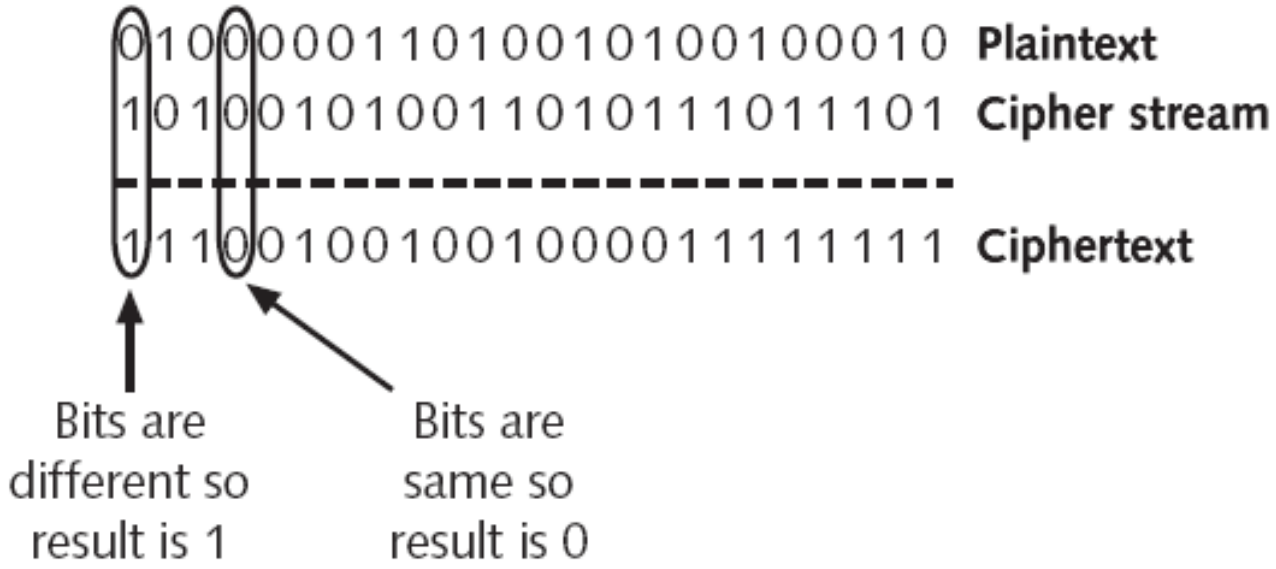
- A more complicated stream cipher is a **transposition cipher,** which rearranges letters without changing them.
- A Single Column Transposition Cipher begins by determining a key (step 1) and assigning a number to each letter of the key (step 2).
- In step 3, the plaintext is written in rows beneath the key and its numbers.



Transposition Stream Cipher



Creating Cipher text with XOR



Symmetric Cryptographic Algorithms (continued)

CHITKARA UNIVERSITY

- **Block cipher**
  - Manipulates an entire block of plaintext at one time
  - Plaintext message is divided into separate blocks of 8 to 16 bytes
    - And then each block is encrypted independently
- Stream cipher advantages and disadvantages
  - Fast when the plaintext is short
  - More prone to attack because the engine that generates the stream does not vary

Information Protection by Symmetric Cryptography

CHITKARA UNIVERSITY

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Non-repudiation	No

Asymmetric Cryptographic Algorithms

- The primary weakness of symmetric encryption algorithms is keeping the single key secure.
- Maintaining a single key among multiple users, scattered geographically, poses a number of significant challenges.

Asymmetric Cryptographic Algorithms

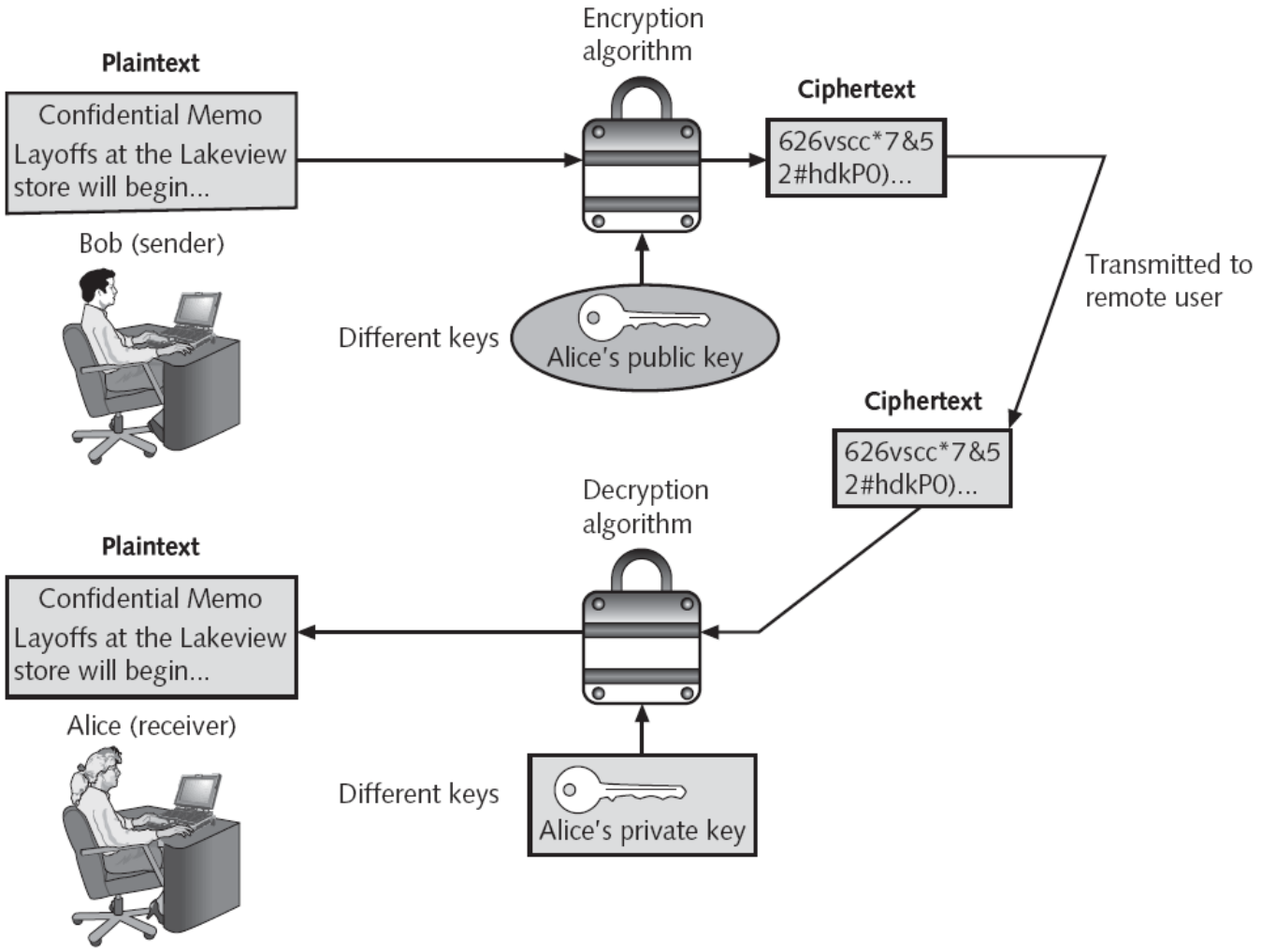
CHITKARA UNIVERSITY

- **Asymmetric cryptographic algorithms**
  - Also known as **public key cryptography**
  - Uses two keys instead of one
    - The **public key** is known to everyone and can be freely distributed
    - The **private key** is known only to the recipient of the message
- Asymmetric cryptography can also be used to create a **digital signature**

Asymmetric Cryptographic Algorithms

- When Bob wants to send a secure message to Alice, he uses Alice's public key to encrypt the message. Alice then uses her private key to decrypt it.

Example Asymmetric Cryptography



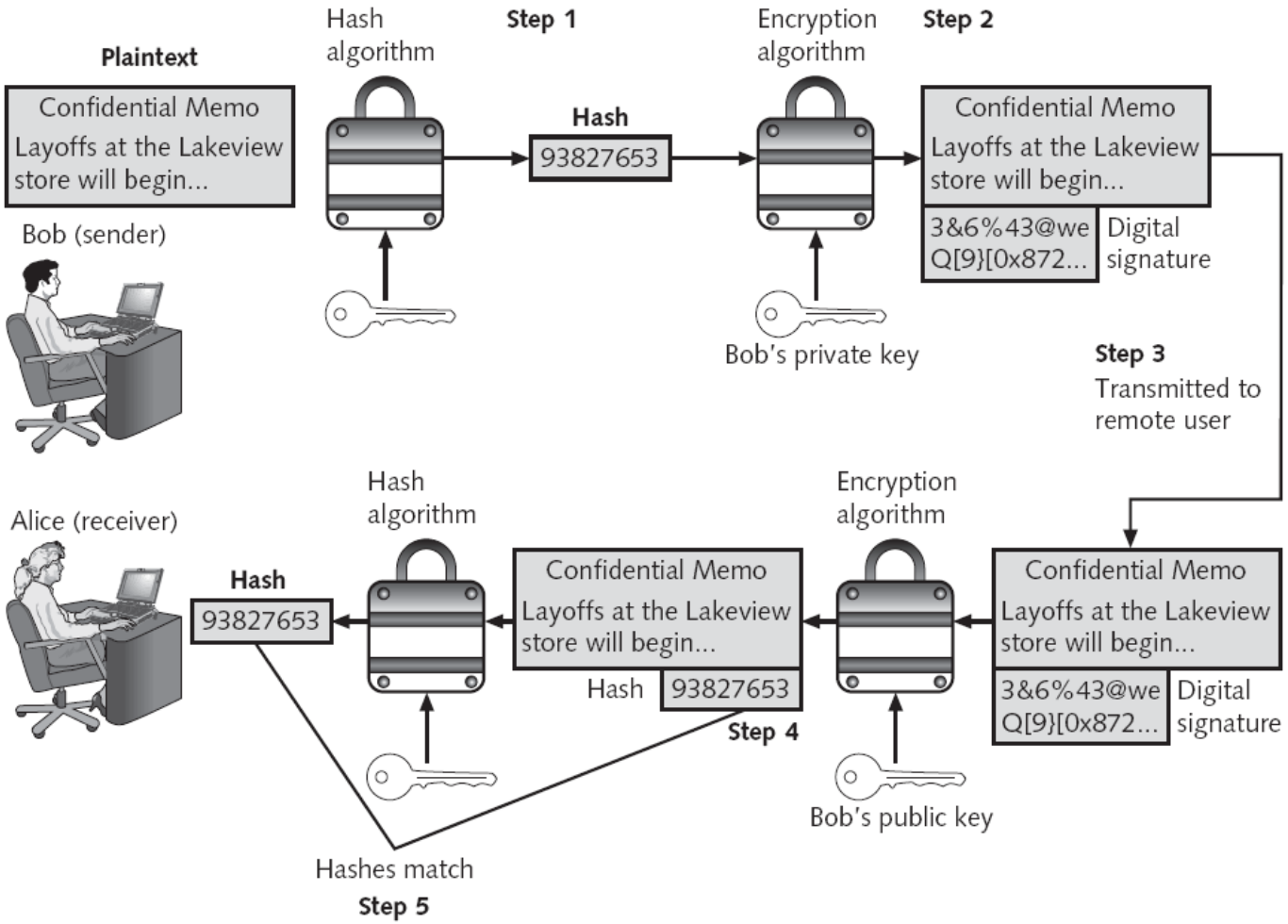
Asymmetric Cryptographic Algorithms (continued)

CHITKARA UNIVERSITY

- Asymmetric Cryptographic can also be used to create digital signatures to:
  - Verify the sender
  - Prove the integrity of the message
  - Prevent the sender from disowning the message

Steps to send digitally signed message

- Bob creates a hash by using a hash algorithm on the message
- Bob then encrypts the hash with his private key. This encrypted hash is the digital signature for the message.
- Bob sends both the message and the digital signature to Alice.
- When Alice receives them, she decrypts the digital signature using Bob's public key, revealing the hash.
- To verify the message, Alice then hashes the message with the same hash algorithm Bob used and compares the result to the hash she received from Bob. If they are equal, Alice can be confident that the message did indeed come from Bob and has not changed since he signed it; if the hashes are not equal, the message either originated elsewhere or was altered after it was signed.


Plaintext
Confidential Memo
Layoffs at the Lakeview store will begin...
Bob (sender)
Hash algorithm
Step 1
Hash
93827653
Encryption algorithm
Step 2
Confidential Memo
Layoffs at the Lakeview store will begin...
3&6%43@we Q[9}[0x872...
Digital signature
Bob's private key
Step 3
Transmitted to remote user
Alice (receiver)
Hash algorithm
Encryption algorithm
Hash
93827653
Confidential Memo
Layoffs at the Lakeview store will begin...
Hash 93827653
Step 4
Confidential Memo
Layoffs at the Lakeview store will begin...
3&6%43@we Q[9}[0x872...
Digital signature
Bob's public key
Hashes match
Step 5

Action	Whose Key to Use	Which Key to Use	Explanation
Bob wants to send Alice an encrypted message	Alice's key	Public key	Whenever an encrypted message is to be sent the recipient's key is always used and never the sender's keys.
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can only be read by using the recipient's private key.
Bob wants to send a copy to himself of the encrypted message that he sent to Alice	Bob's key	Public key to encrypt Private key to decrypt	An encrypted message can only be read by the recipient's private key. Bob would need to encrypt it with his own public key and then use his private key to decrypt it.
Bob receives an encrypted reply message from Alice	Bob's key	Private key	The recipient's private key is used to decrypt received messages.
Bob wants Susan to read Alice's reply message that he received	Susan's key	Public key	The message should be encrypted with Susan's key for her to decrypt and read it with her private key.
Bob wants to send Alice a message with a digital signature	Bob's key	Private key	Bob's private key is used to encrypt the hash.
Alice wants to see Bob's digital signature	Bob's key	Public key	Because Bob's public and private keys are mathematically related Alice can use his public key to decrypt the hash.

Information Protection by Asymmetric Cryptography

CHITKARA UNIVERSITY

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	Yes
Non-repudiation	Yes

Summary

- Cryptography is the science of transforming information into a secure form while it is being transmitted or stored so that unauthorized users cannot access it.
- Hashing creates a unique signature, called a hash or digest, which represents the contents of the original text
- Symmetric cryptography, also called private key cryptography, uses a single key to encrypt and decrypt a message

Summary

- Asymmetric cryptography, also known as public key cryptography, uses two keys instead of one

CHITKARA UNIVERSITY

Thanks