NETWORK

SECURITY

05 CRYPTOGRAPHY BASIC

Contents

5.1 Defining 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.*
- And *changing the original text to a secret message using cryptography is known as* **encryption**.

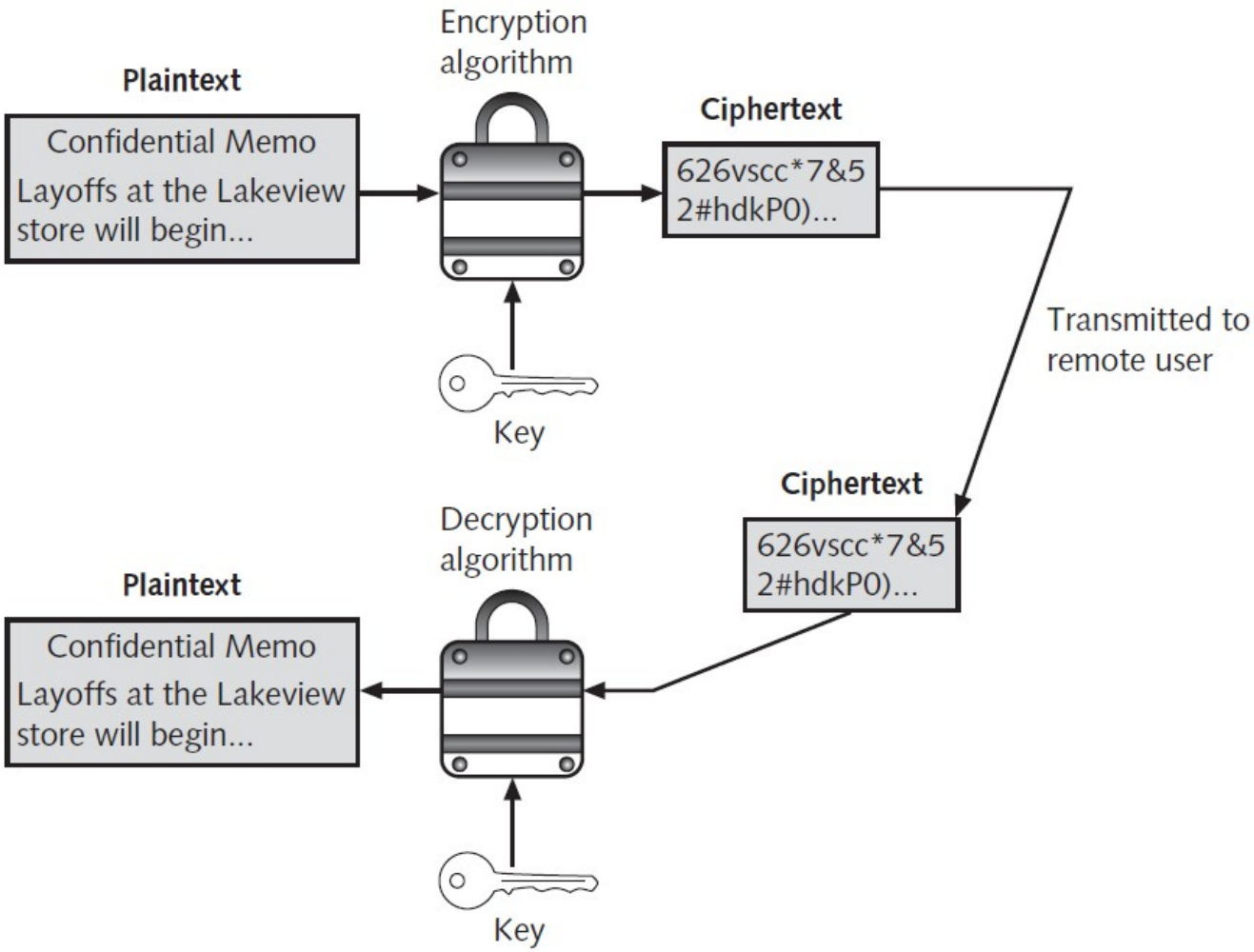
5.1 Defining Cryptography

- Clear-text data that is to be encrypted is called **plaintext**.
- Plaintext data is input into an encryption **algorithm**, which consists of procedures based on a mathematical formula used to encrypt the data.
- A **key** is a mathematical value entered into the algorithm to produce **ciphertext**, or text that is “scrambled.”

5.1 Defining Cryptography

- Once the ciphertext is transmitted or needs to be returned to clear-text, the reverse process occurs with a **decryption** algorithm.

5.1 Defining Cryptography



5.2 Cryptography & Security

- Cryptography can provide basic security protection for information.
- There are five basic protections that cryptography can provide:
  - Cryptography can protect the *confidentiality* of information by ensuring that only authorized parties can view it.
  - Cryptography can protect the *integrity* of the information.

5.2 Cryptography & Security

  - Cryptography can help ensure the *availability* of the data so that authorized users (with the key) can access it.
  - Cryptography can verify the *authenticity* of the sender.
- But, Not all types of cryptography provide all five protections.

5.2 Cryptography & Security

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

5.3 Cryptographic Algorithms

- There are three categories of cryptographic algorithms.

- These are known as :
  - hashing algorithms,
  - symmetric encryption algorithms, and
  - asymmetric encryption algorithms.

5.3 Cryptographic Algorithms

5.3.1 Hashing Algorithms

- The most basic type of cryptographic algorithm is a hashing algorithm.

- The common hashing algorithms are:
  - Message Digest,
  - Secure Hash Algorithm

5.3 Cryptographic Algorithms

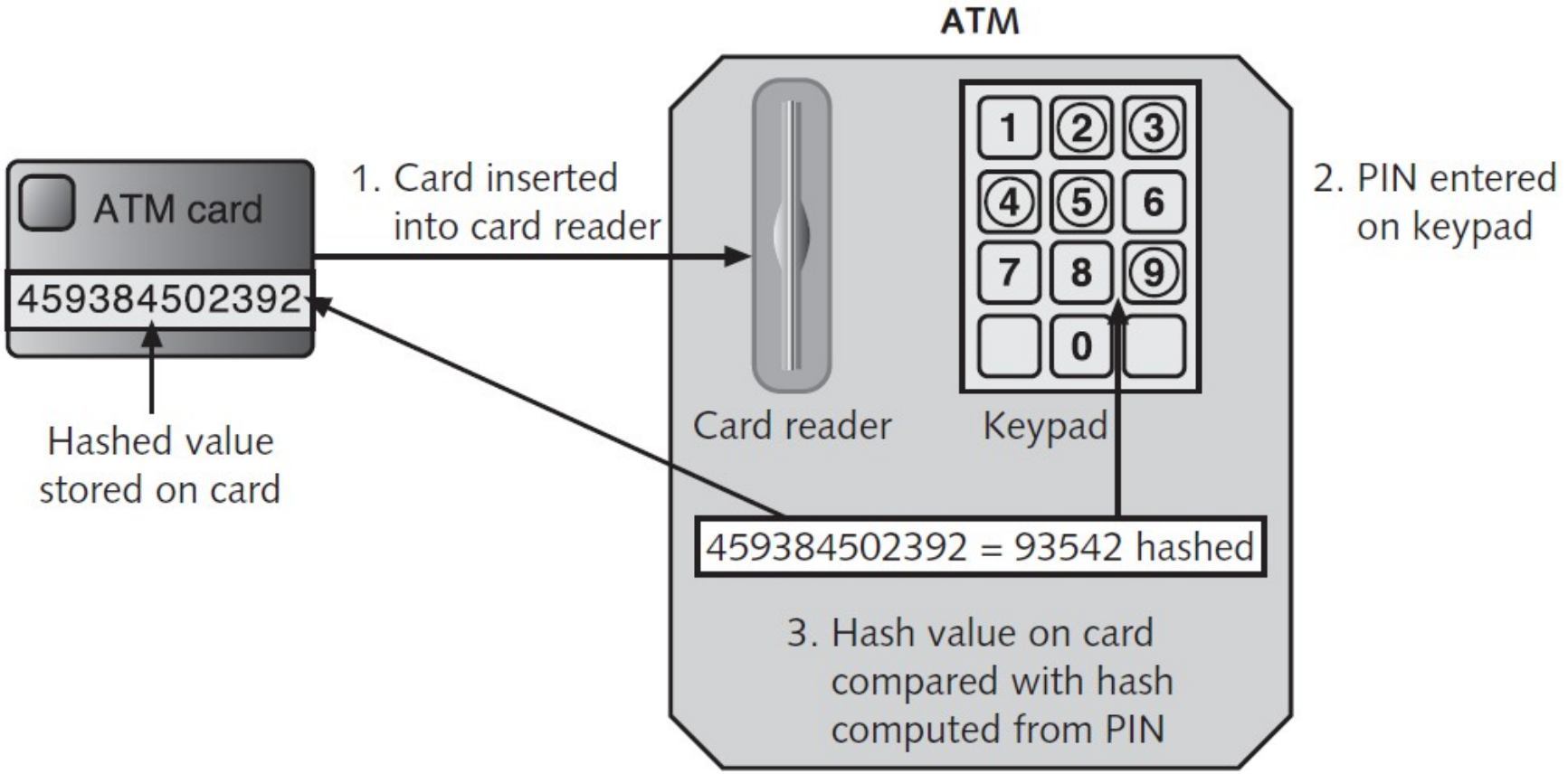
- **Hashing,** also called a **one-way hash**, *is a process for creating a unique "signature" for a set of data.*
- This signature, called a **hash** or **digest**, that represents the contents.
- Hashing is used to determine the integrity of a message or contents of a file.

- A hash that is created from a set of data cannot be reversed.

5.3 Cryptographic Algorithms

- A practical example of a hash algorithm is used with automatic teller machine (ATM) cards.
  - A bank customer has a personal identification number (PIN).
  - This number is hashed and the resulting ciphertext is stored on a magnetic strip on the back of the ATM card.

5.3 Cryptographic Algorithms



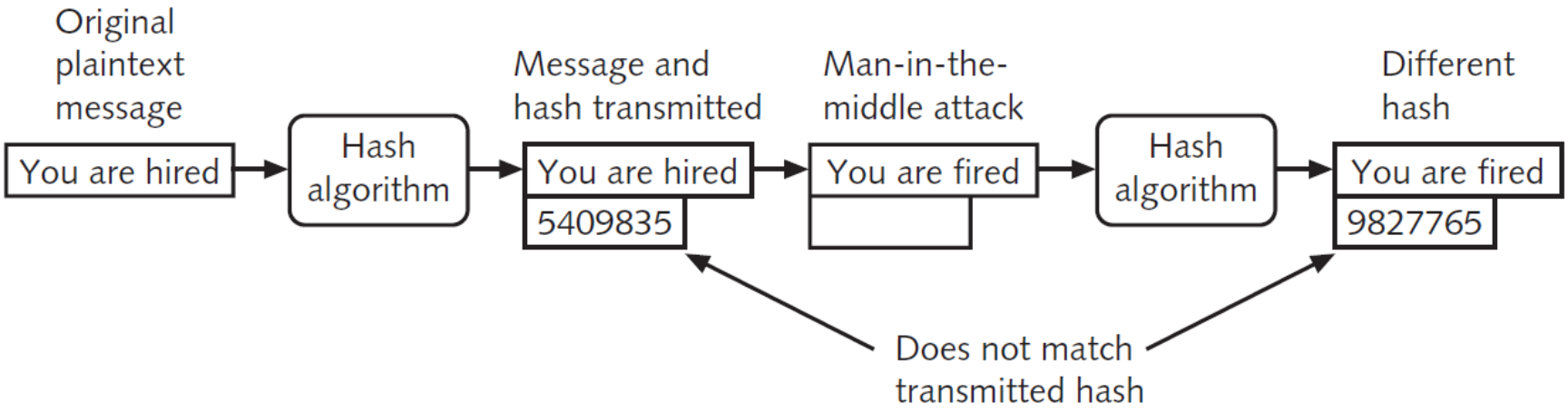
5.3 Cryptographic Algorithms

- A hashing algorithm is considered secure if it has these characteristics:
  - The ciphertext hash is a **fixed size**. A hash of a short set of data will produce the same size as a hash of a long set of data.
  - 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 in order to determine the original plaintext.

5.3 Cryptographic Algorithms

- Hash can be used to defeat man in the middle attack.
  - Both the message and the hash are transmitted.
  - Upon receiving the message, the same hash is generated again on the message.
  - If the original (transmitted) hash equals the new hash, then the message has not been altered.
- Hash values are often posted on Internet sites in order to verify the file integrity of files that can be downloaded.

5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

Message Digest

- One common hash algorithm is the **Message Digest (MD)** algorithm, which has three versions.
- **Message Digest 2 (MD2)** takes plaintext of any length and creates a hash 128 bits long.
- MD2 begins by dividing the message into 128-bit sections. If the message is less than 128 bits, data known as **padding** is added.

5.3 Cryptographic Algorithms

- After padding, a 16-byte checksum is appended to the message. Then the entire string is processed to create a 128-bit hash.
- MD2 is considered too slow today and is rarely used.

5.3 Cryptographic Algorithms

- **Message Digest 4 (MD4)** was developed in 1990 for computers that processed 32 bits at a time.
- Like MD2, MD4 takes plaintext and creates a hash of 128 bits.
- The plaintext message itself is padded to a length of 512 bits.
- Flaws in the MD4 hash algorithm have prevented this MD from being widely accepted.

5.3 Cryptographic Algorithms

- The **Message Digest 5 (MD5)**, a revision of MD4, was created in 1991 by Ron Rivest and designed to address MD4's weaknesses.
- Like MD4, the length of a message is padded to 512 bits.
- The hash algorithm then uses four variables of 32 bits each in a round-robin fashion to create a value that is compressed to generate the hash.
- But, it is still leading to collision.

5.3 Cryptographic Algorithms

Secure Hash Algorithm SHA

- A more secure hash than MD is the **Secure Hash Algorithm (SHA)**.
- The first is **SHA-1**. SHA-1 is patterned after MD4, but creates a hash that is 160 bits and pads the messages of less then 512 bits with zeros and an integer that describes the original length of the message.

5.3 Cryptographic Algorithms

- The other hashes are known as **SHA-2**.
- SHA-2 actually is comprised of four variations, known as SHA-224, SHA-256, SHA-384, and SHA-512.
- The number following *SHA* indicates the length in bits of the digest.
- To date there have been no weaknesses identified with it. Most security experts recommend that SHA-2 be substituted in place of MD5.

5.3 Cryptographic Algorithms

Whirlpool

- Named after the first galaxy recognized to have a spiral structure, it creates a hash of 512 bits.
- According to its creators, Whirlpool will not be patented and can be freely used for any purpose.
- It takes a message of any length less than 2^{256} bits and returns a 512-bit message digest.

5.3 Cryptographic Algorithms

5.3.2 Symmetric Cryptographic

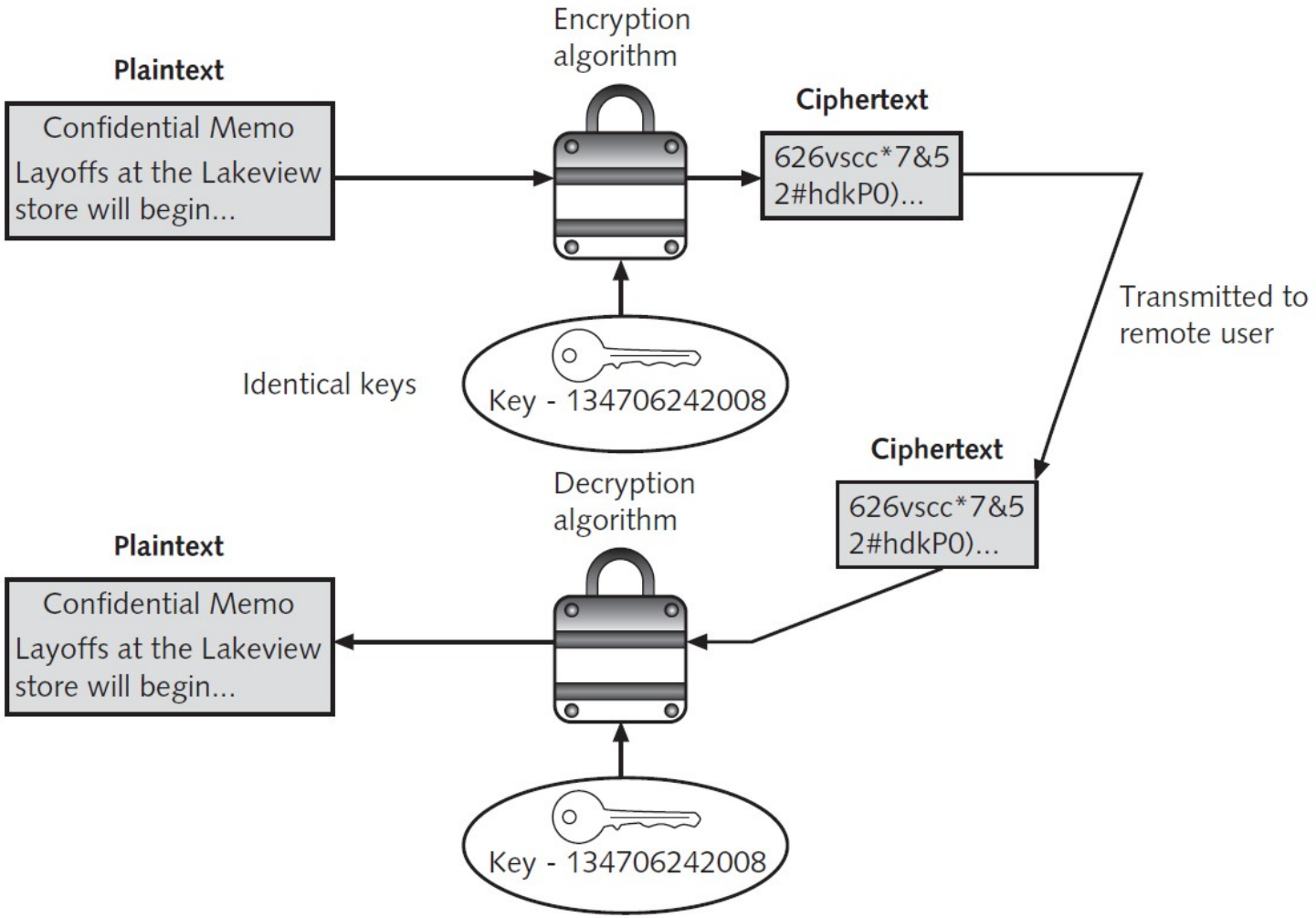
- The original cryptographic algorithms for encrypting and decrypting documents are symmetric cryptographic algorithms.

- These include the Data Encryption Standard DES, Triple Data Encryption Standard 3DES, Advanced Encryption Standard AES, and several other algorithms.

5.3 Cryptographic Algorithms

- **Symmetric cryptographic algorithms** use the same single key to encrypt and decrypt a message.
- It is therefore essential that the key be kept confidential, because if an attacker secured the key he could decrypt all encrypted messages.
- For this reason, symmetric encryption is also called **private key cryptography**.

5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

- Symmetric algorithms can be classified into two categories based on the amount of data that is processed at a time.

Stream Cipher

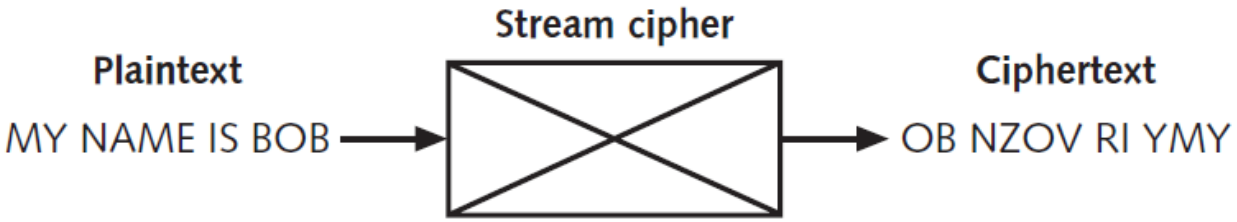
- The first category is known as a **stream cipher**. A stream cipher takes one character and replaces it with one character.

5.3 Cryptographic Algorithms

- The simplest type of stream cipher is a **substitution cipher**. Substitution ciphers simply substitute one letter or character for another.

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**

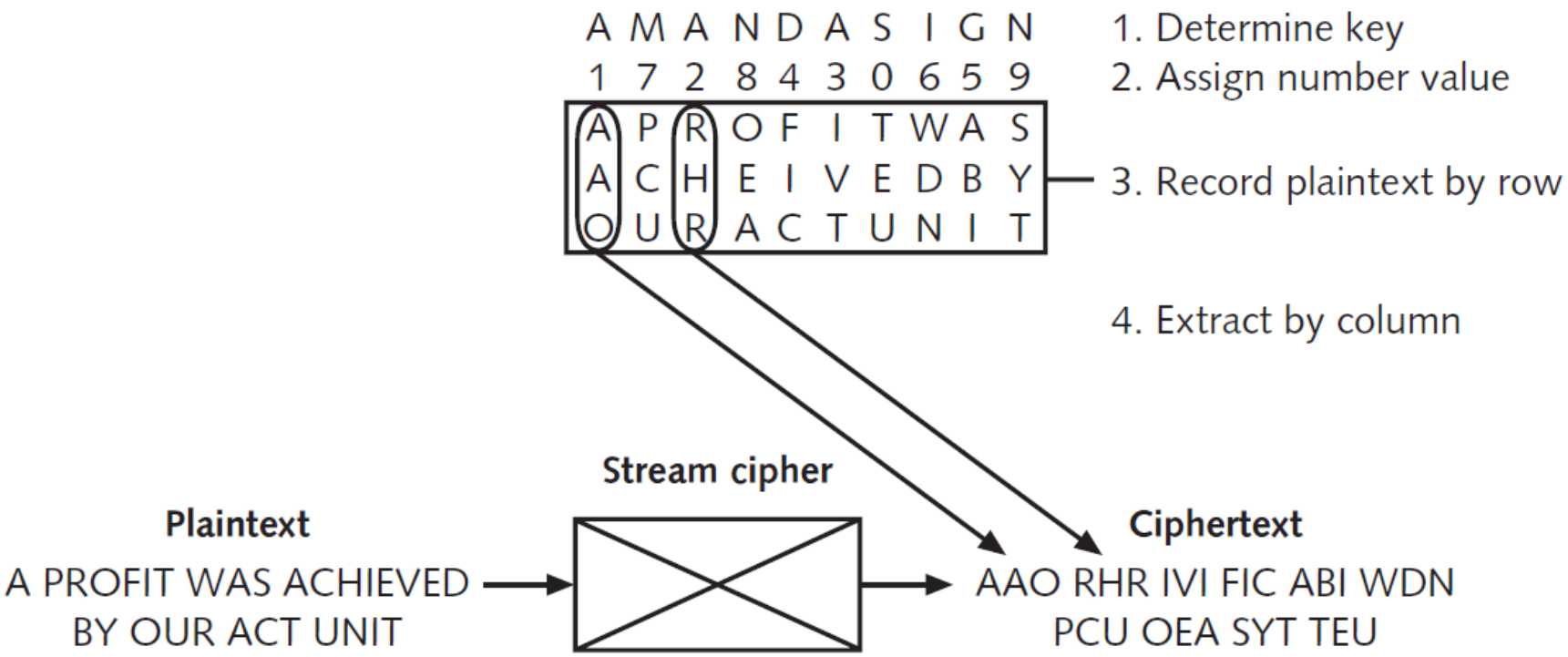
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A - **Substitution letters**



5.3 Cryptographic Algorithms

- 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).
- The plaintext is written in rows beneath the key and its numbers (Step 3).
- In Step 4, each column is extracted based upon the numeric value.

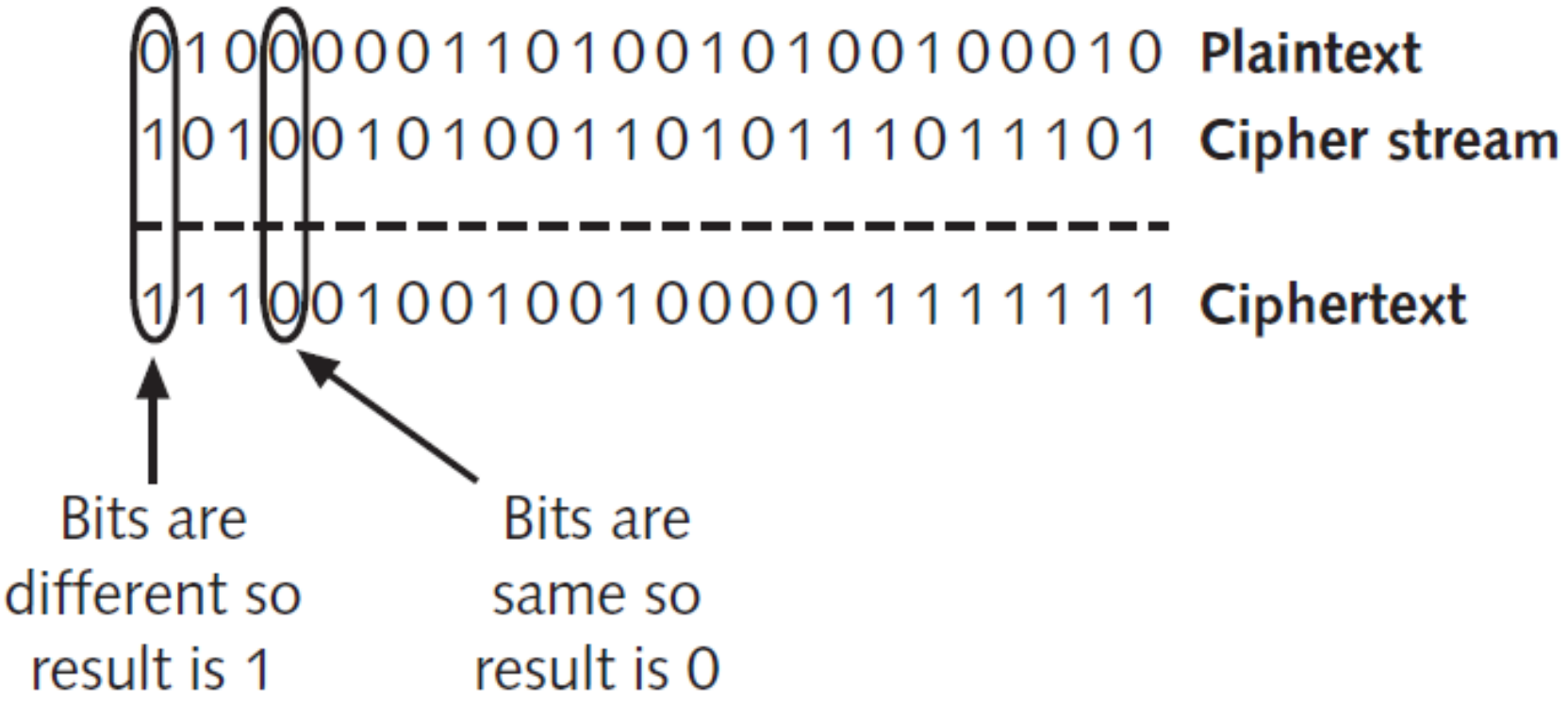
5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

- With most symmetric ciphers, the final step is to combine the cipher stream with the plaintext to create the ciphertext.
- The process is accomplished through the exclusive OR (XOR) binary logic operation because all encryption occurs in binary.

5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

- Instead of combining the cipher stream with the plaintext, a variation is to create a truly random key (called a **pad**) to be combined with the plaintext.
- This is known as a **one-time pad (OTP)**.
- If the pad is a random string of numbers that is kept secret and not reused then an OTP can be considered secure.

5.3 Cryptographic Algorithms

Block Cipher

- The second category of symmetric algorithms is known as a **block cipher**.
- a block cipher manipulates an entire block of plaintext at one time.
- The plaintext message is divided into separate blocks of 8 to 16 bytes, and then each block is encrypted independently.
- For additional security, the blocks can be randomized.

5.3 Cryptographic Algorithms

- ***Data Encryption Standard DES***
  - One of the first widely popular symmetric cryptography algorithms is the **Data Encryption Standard (DES)**.
  - DES is a block cipher and encrypts data in 64-bit blocks. However, the 8-bit parity bit is ignored so the effective key length is only 56 bits.
  - DES encrypts 64-bit plaintext by executing the algorithm 16 times, with each time or iteration called a round.

5.3 Cryptographic Algorithms

DES Mode	Cipher Algorithm	Operation	Strength
Electronic code book (ECB)	Block cipher	Uses a 56-bit key to encrypt 64-bit blocks	Because it uses the same encryption pattern each time, it is vulnerable to attackers
Cipher block chaining (CBC)	Block cipher	Message blocks are linked together	More secure than ECB
Cipher feedback (CFB)	Block cipher that functions like a stream cipher	Ciphertext created in one round is used to encrypt the next round	Very secure but slower than ECB
Output feedback (OFB)	Block cipher that functions like a stream cipher	Results of cipher are added to a message for the next round	Less secure than CFB

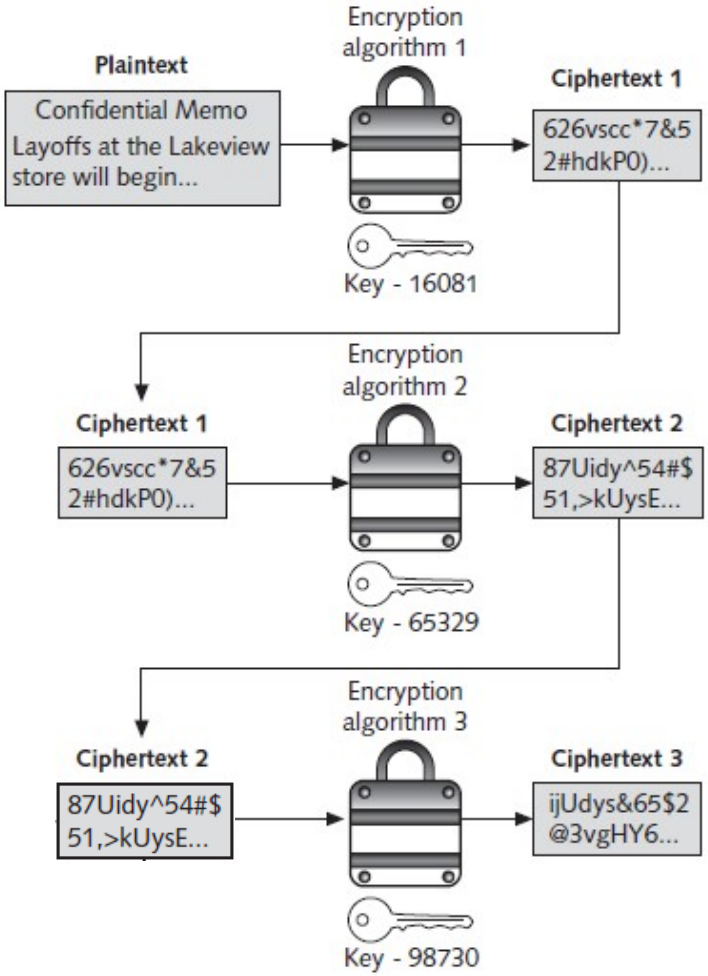
5.3 Cryptographic Algorithms

- DES is said to have catapulted the study of cryptography into the public arena.
- Until the deployment of DES, cryptography was studied almost exclusively by military personnel.
- DES helped move cryptography implementation and research to academic and commercial organizations.
- Although DES was widely implemented, its 56-bit key is no longer considered secure and has been broken several times.

5.3 Cryptographic Algorithms

- **Triple Data Encryption Standard (3DES)**
  - Triple Data Encryption Standard (3DES) was designed to replace DES.
  - As its name implies, 3DES uses three rounds of encryption instead of just one. The ciphertext of one round becomes the entire input for the second iteration.
  - 3DES employs a total of 48 iterations in its encryption (three iterations times 16 rounds).

5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

- In some versions of 3DES, only two keys are used, but the first key is repeated for the third round of encryption.
- The version of 3DES that uses three keys is estimated to be 2 to the power of 56 times stronger than DES.
- Although 3DES addresses several of the key weaknesses of DES, it is no longer considered the most secure symmetric cryptographic algorithm.

5.3 Cryptographic Algorithms

- **Advanced Encryption Standard (AES)**
  - New algorithm that was fast enough and function on older computers with 8-bit processors as well as on current 32-bit and future 64-bit processors.
  - AES performs three steps on every block (128 bits) of plaintext.
  - Within Step 2, multiple rounds are performed depending upon the key size: a 128-bit key performs nine rounds, a 192-bit key performs 11 rounds, and a 256-bit key, known as AES-256, uses 13 rounds.

5.3 Cryptographic Algorithms

- Within each round, bytes are substituted and rearranged, and then special multiplication is performed based on the new arrangement.

5.3 Cryptographic Algorithms

- Other Algorithms
  - Several other symmetric cryptographic algorithms are also used. **Rivest Cipher (RC)** is a family of cipher algorithms designed by Ron Rivest.
  - **RC2** is a block cipher that processes blocks of 64 bits.
  - **RC4** is a stream cipher that accepts keys up to 128 bits in length. It is used as part of the Wired Equivalent Privacy (WEP) encryption standard.

5.3 Cryptographic Algorithms

5.3.3 Asymmetric Cryptographic

- The newest type of cryptographic algorithm for encrypting and decrypting documents is asymmetric cryptographic algorithms.

- These include RSA, Diffie-Hellman, and elliptic curve cryptography.

5.3 Cryptographic Algorithms

- The primary weakness of symmetric encryption algorithms is keeping the single key secure.
- Maintaining a single key among multiple users, often scattered geographically, poses a number of significant challenges.
- Key can NOT be sent via Internet, nor can be encrypted as the receiver need a way to decrypted.

5.3 Cryptographic Algorithms

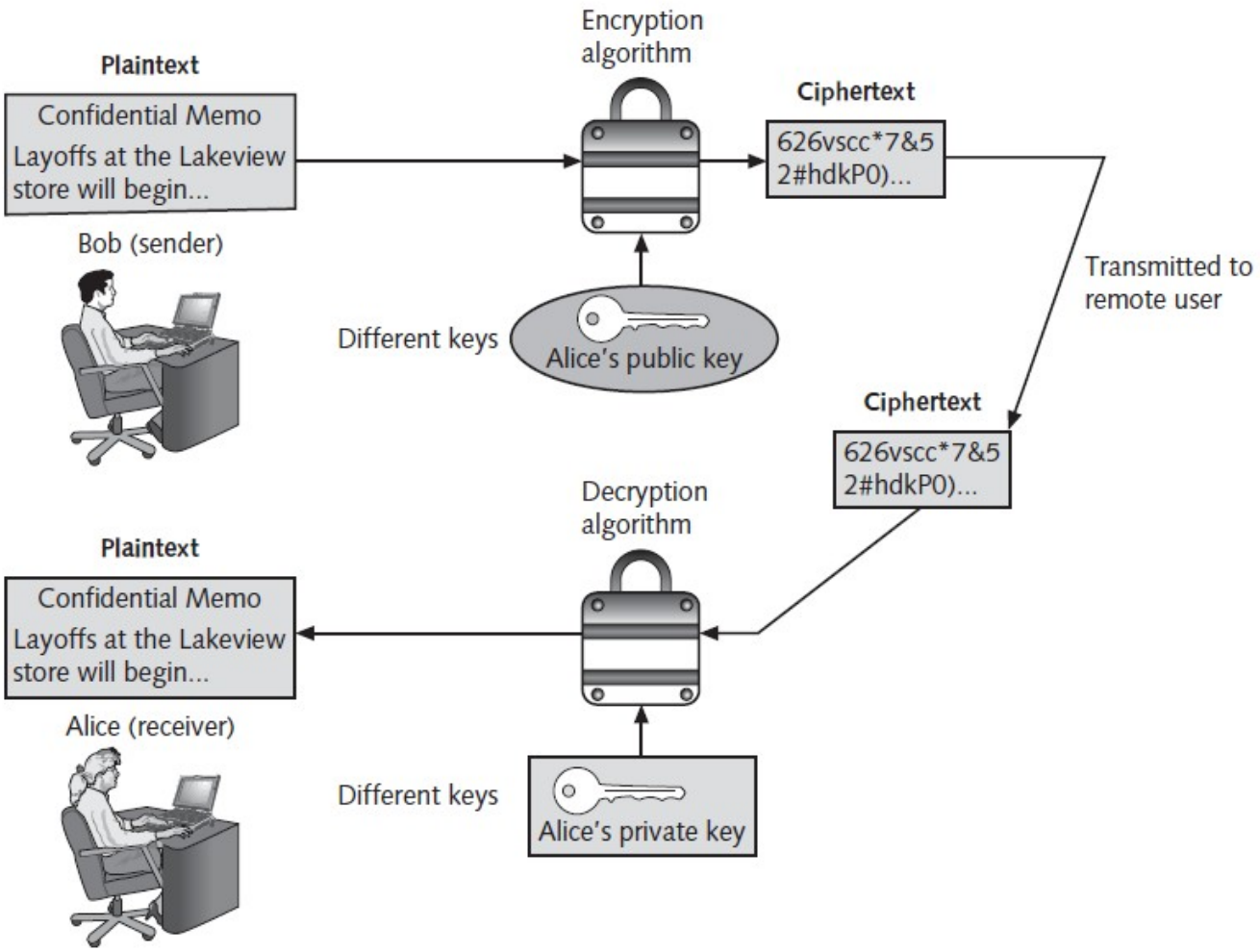
- A completely different approach to symmetric cryptography is **asymmetric cryptographic algorithms**, also known as **public key cryptography**.
- Asymmetric encryption uses two keys instead of one. These keys are mathematically related and are known as the public key and the private key.

5.3 Cryptographic Algorithms

- The **public key** is known to everyone and can be freely distributed, while the **private key** is known only to the recipient of the message.

- Asymmetric encryption was developed by Whitfield Diffie and Martin Hellman of the Massachusetts Institute of Technology (MIT) in 1975.

5.3 Cryptographic Algorithms



5.3 Cryptographic Algorithms

- Public and private keys can often result in confusion regarding whose key to use and which key should be used.
- Next table, lists the practices to be followed when using asymmetric cryptography.

5.3 Cryptographic Algorithms

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.

5.3 Cryptographic Algorithms

Action	Whose Key to Use	Which Key to Use	Explanation
Bob receives an encrypted reply message from Alice	Bobś key	Private key	The recipientś private key is used to decrypt received messages.
Bob wants Susan to read Aliceś reply message that he received	Susanś key	Public key	The message should be encrypted with Susanś key for her to decrypt and read it with her private key.
Bob wants to send Alice a message with a digital signature	Bobś key	Private key	Bobś private key is used to encrypt the hash.
Alice wants to see Bobś digital signature	Bobś key	Public key	Because Bobś public and private keys are mathematically related Alice can use his public key to decrypt the hash.

5.3 Cryptographic Algorithms

RSA

- RSA stands for the last names of its three developers, Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman.
- The RSA algorithm multiplies two large prime numbers ***p*** and ***q***, to compute their product (***n=pq***).
- Next, a number *e* is chosen that is less than *n* and a prime factor to *(p-1)(q-1)*.

5.3 Cryptographic Algorithms

- Another number *d* is determined, so that *(ed-1)* is divisible by *(p-1)(q-1)*.
- The values of *e* and *d* are the public and private exponents.
- The public key is the pair (*n*,*e*) while the private key is (*n*,*d*).
- The numbers *p* and *q* can be discarded.

- RSA is slower than other algorithms.

5.3 Cryptographic Algorithms

Diffie-Hellman

- Unlike RSA, the Diffie-Hellman algorithm does not encrypt and decrypt text.
- Rather, the strength of Diffie-Hellman is that it allows two users to share a secret key securely over a public network.
- Once the key has been shared, then both parties can use it to encrypt and decrypt messages using symmetric cryptography.

5.3 Cryptographic Algorithms

Elliptic Curve

- Elliptic Curve Cryptography was first proposed in the mid-1980s.
- Instead of using prime numbers as with RSA, elliptic curve cryptography uses elliptic curves.
- By adding the values of two points on the curve, you can arrive at a third point on the curve.

5.3 Cryptographic Algorithms

- Elliptic curve cryptography has not been fully scrutinized as other types of asymmetric algorithms because the concept is still new.
- The studies that have been performed so far have indicated that elliptic curve cryptography may be a promising technology.

5.4 Cryptography on Files

- Cryptography can be applied to individual files or a group of files.
- Protecting individual files or multiple files through file system cryptography can be performed using:
  - Pretty Good Privacy (PGP), and
  - Microsoft Windows Encrypting File System.

5.4 Cryptography on Files

- Most widely used asymmetric cryptography system for files and e-mail messages is a commercial product called **Pretty Good Privacy (PGP)**.
- A similar program known as **GNU Privacy Guard (GPG)** is an open-source product.
- Messages **encrypted by PGP** can generally be **decrypted by GPG** and vice versa.

5.4 Cryptography on Files

- PGP and GPG use both asymmetric and symmetric cryptography.
- PGP/GPG generates a random symmetric key and uses it to encrypt the message.
- The symmetric key is then encrypted using the receiver’s public key and sent along with the message.

5.4 Cryptography on Files

- PGP can use either RSA or the Diffie-Hellman algorithm for asymmetric encryption and IDEA for symmetric encryption.
- GPG is unable to use IDEA because IDEA is patented.
- Instead, GPG uses one of several open-source algorithms.

5.4 Cryptography on Files

- Microsoft's **Encrypting File System (EFS)** is a cryptography system for Windows operating systems that use the Windows NTFS file system.
- Any file created in an encrypted folder or added to an encrypted folder is automatically encrypted.

5.4 Cryptography on Files

- EFS files are encrypted with a single symmetric key, and then the symmetric key is encrypted twice: once with the user's EFS public key (to allow transparent decryption), and once with the recovery agent's key to allow data recovery.

5.4 Cryptography on Files

- When using EFS, the following should be considered:
  - First encrypt the folder and then move the files to be protected into that folder.
  - Do not encrypt the entire drive that contains the system folder; this could significantly decrease performance and even cause the system to not boot.
  - A folder can be either compressed or encrypted but not both.