Fundamentals of Cryptography

Steganography: Hiding the Message

- Steganography hides the existence of data
- An image, audio, or video file can contain hidden messages embedded in the file
  - It is achieved by dividing data and hiding in unused portions of the file
- A common scheme is to hide data in the file header fields that describe the file, between sections of the **metadata** (data used to describe the content or structure of the actual data)

Cryptography: Hiding the Meaning

- **Cryptography** is the practice of transforming (“scrambling”) information so that its meaning cannot be understood by unauthorized parties
  - One method is transposition, in which each letter of the message is rearranged
  - Another method is substitution, where one letter is substituted for another letter

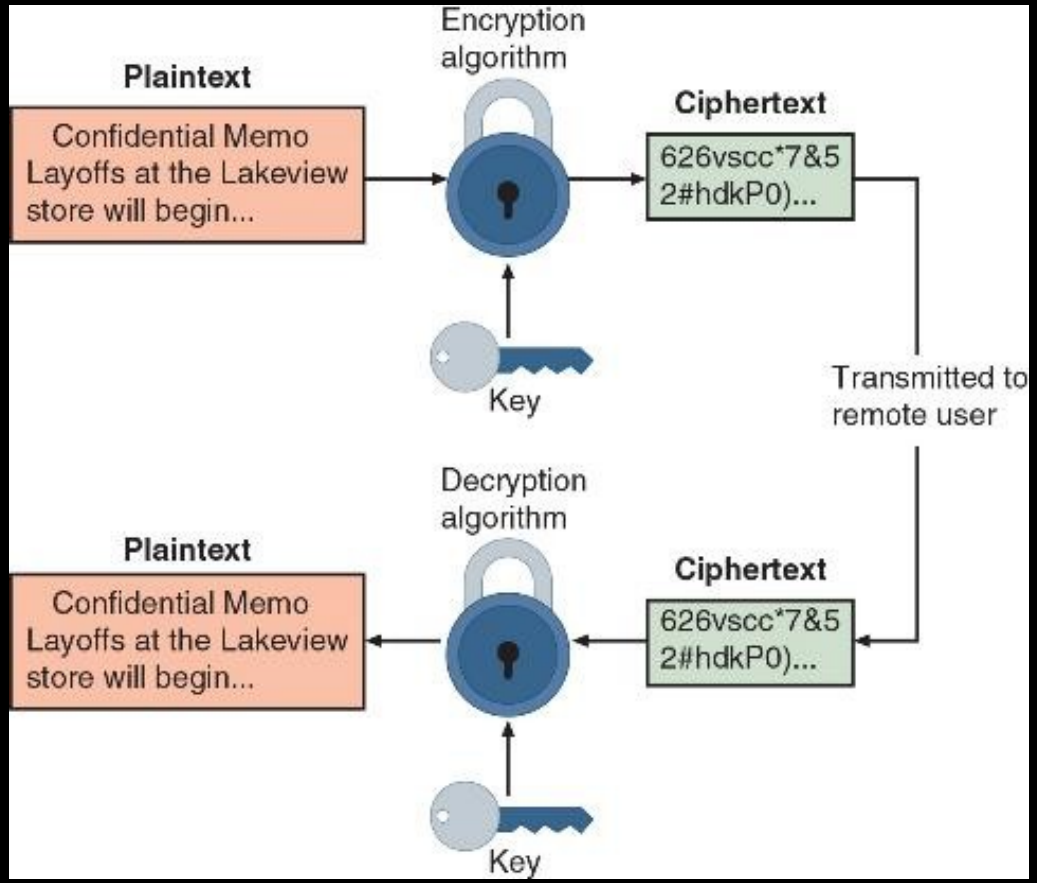
Cryptography: Hiding the Meaning

- The process of changing the original text into a scrambled message is known as encryption (the reverse process is decryption)
- The following terminology applies to cryptography:
  - **Plaintext** is unencrypted data that is input for encryption or is the output of decryption
  - **Ciphertext** is the scrambled and unreadable output of encryption
  - **Cleartext** is unencrypted data that is not intended to be encrypted

Cryptography: Hiding the Meaning

- Plaintext data is input into a cryptographic algorithm (also called a **cipher**), which consists of procedures based on a mathematical formula used to encrypt and decrypt the data
- A **key** is a mathematical value entered into the algorithm to produce ciphertext
  - The reverse process uses the key to decrypt the message
- The critical factor in cryptography is that one or more elements must be kept secret at all costs
  - The key for the algorithm must always be kept secret

Cryptography: Hiding the Meaning



Benefits of Cryptography

- Cryptography can provide the following security protections:
  - **Confidentiality** *e*nsures only authorized parties can view it
  - **Integrity** ensures information is correct and unaltered
  - **Authentication** ensures sender can be verified through cryptography
  - **Nonrepudiation** proves that a user performed an action
  - **Obfuscation** is making something obscure or unclear
- **Security through obscurity** is an approach in security where virtually any system can be made secure as long as outsiders are unaware of it or how it functions

Question?

- Layla has encrypted a document so that it can only be viewed by those who have been provided the key. What protection has she given to this document?

Answer

- Layla has encrypted a document so that it can only be viewed by those who have been provided the key. What protection has she given to this document?
- Confidentiality ensures that only authorized parties can view the information. Encrypted information that can only be viewed by those who have been provided the key is an example of confidentiality.

Cryptographic Algorithms

- The three categories of cryptographic algorithms include the following:
  - Hash algorithms
  - Symmetric cryptographic algorithms
  - Asymmetric cryptographic algorithms

Variations of Algorithms

- A secure cryptographic algorithm that is hand-calculated is a **one-time pad** (**OTP**) that combines plaintext with a random key
  - A **pad** is a long sequence of random letters
  - To decipher the message, the recipient must have a copy of the pad
- A **stream cipher** takes one character and replaces it with another
- A **block cipher** manipulates an entire block of plaintext at one time
- A **sponge function** takes as input a string of any length and returns a string of any requested variable length

Hash Algorithms

- A **hash** algorithm creates a unique “digital fingerprint” of a set of data and is commonly called *hashing*
  - This fingerprint, called a digest (sometimes called a *message digest* or *hash*), represents the contents
  - It is primarily used for comparison purposes
- Hashing is intended to be one way in that its digest cannot be reversed to reveal the original set of data
- A hashing algorithm is considered secure if it has a fixed size, is unique, is original, and is secure (hash cannot be reversed to determine original plaintext)

Hash Algorithms

- The following are considered to be secure hash algorithms:
  - Secure Hash Algorithm (SHA)
  - RipeMD
  - Whirlpool
- Hashing is often used as a check to verify that the original contents of an item have not been changed

Hash Algorithms

Hashes

KeePass 2.53

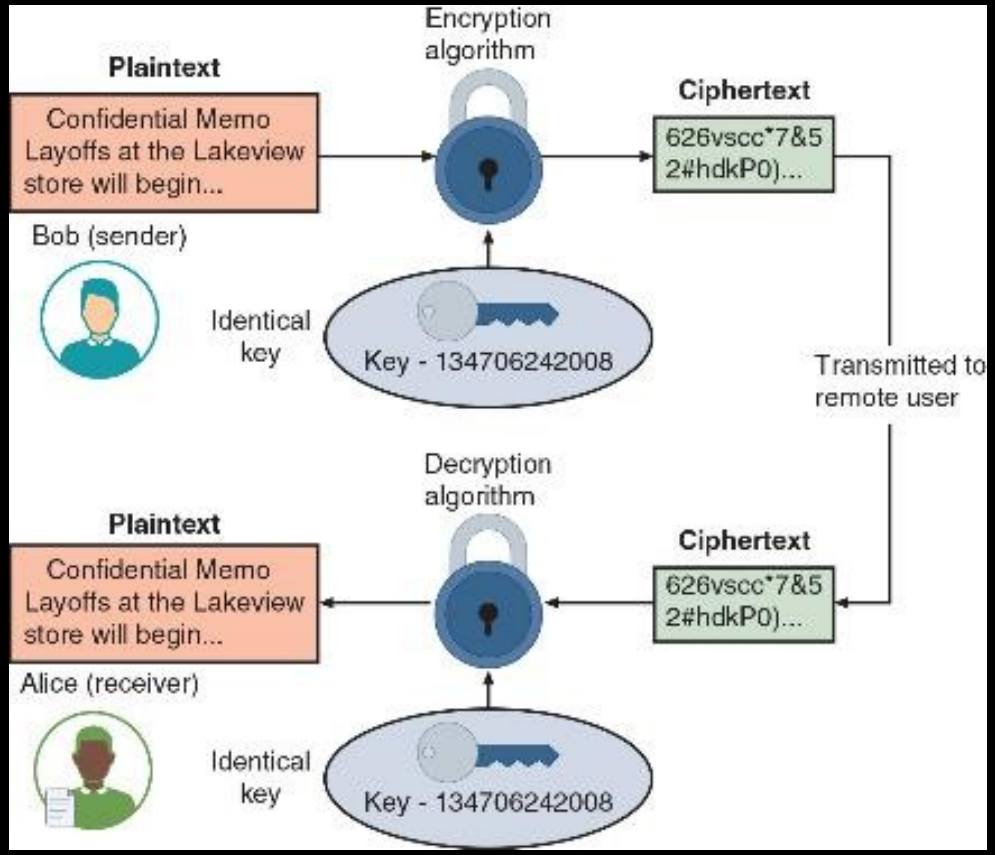
KeePass-2.53.zip:

```
SHA-1:    092CC353 1A46B600 968636B5 6851E23F FEE5505F
SHA-256:  DCA1B970 9A87BA67 ECEF8905 80C0B2AD 6E3ACF38 546A642C AFE36D70 62E40AD4
Size:     3225609 B
Sig.:     [OpenPGP ASC]
```

Symmetric Cryptographic Algorithms

- **Symmetric cryptographic algorithms** use the same key to encrypt and decrypt data
  - It is also called **private key cryptography** because the key is kept private between the sender and receiver
- Symmetric cryptography can provide strong encryption if the key is kept secure between the sender and the recipient
- Some strong symmetric cryptographic algorithms include:
  - Advanced Encryption Standard (AES)
  - Blowfish and Twofish

Symmetric Cryptographic Algorithms



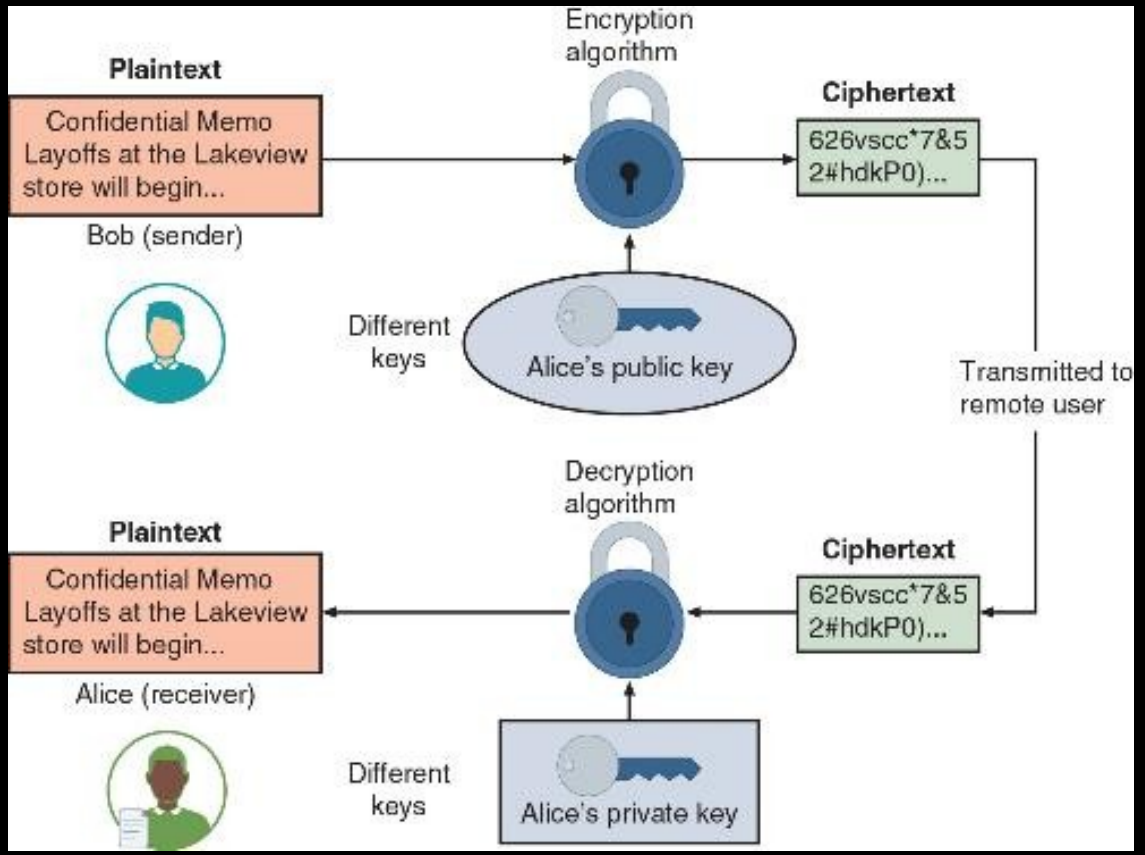
Asymmetric Cryptographic Algorithms

- The primary weakness of symmetric algorithms is that distributing and maintaining a secure key among multiple users poses challenges
  - Asymmetric cryptographic algorithms use two mathematically related keys known as the public key and the private key
  - It is also known as **public key cryptography**
- The public key is available to everyone and is freely distributed
- The private key is known only to the individual to whom it belongs

Asymmetric Cryptographic Algorithms

- The following are some important principles regarding asymmetric cryptography:
  - **Key pairs**
  - **Public key**
  - **Private key**
  - **Both directions** - keys can work in both directions

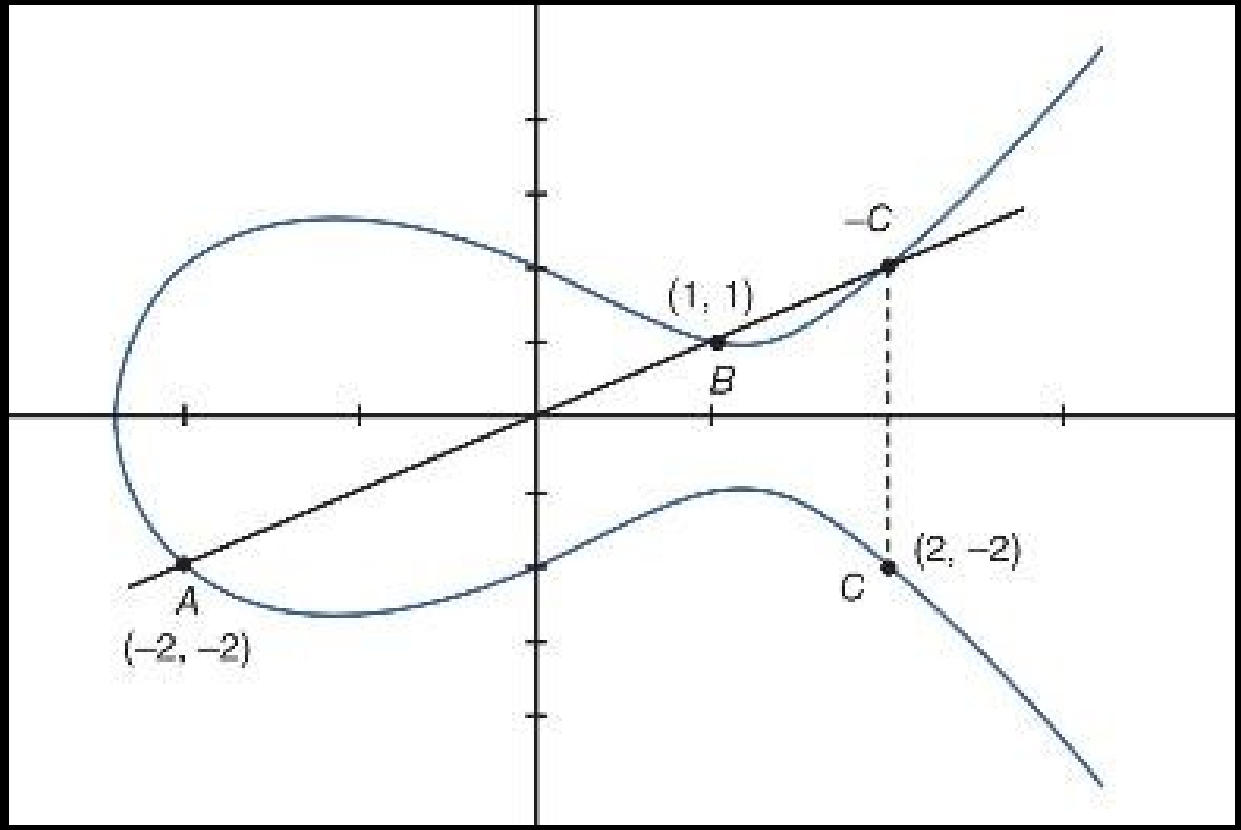
Asymmetric Cryptographic Algorithms



Asymmetric Cryptographic Algorithms

- **RSA** asymmetric algorithm was published in 1977
  - It multiplies two large prime numbers
  - The basis of RSA encryption security is factoring
- With **elliptic curve cryptography (ECC)**, users share one elliptic curve and one point on the curve
  - It uses less computing power than prime number-based asymmetric cryptography because the key sizes are smaller
  - All modern OSs and web browsers rely on ECC

Asymmetric Cryptographic Algorithms



Asymmetric Cryptographic Algorithms

- **Digital Signature Algorithm (DSA)** creates a digital signature which can do the following:
  - Verify the sender, prevent the sender from disowning the message, and prove message integrity
- **Key Exchange**
  - There are different solutions for a key exchange that occurs within the normal communications channel (in-band) of cryptography:
    - **Diffie-Hellman (DH), Diffie-Hellman Ephemeral (DHE), Elliptic Curve Diffie-Hellman (ECDH),** and **Perfect forward secrecy**

Question?

- Which algorithm uses the same key to both encrypt and decrypt data?

Answer

- Which algorithm uses the same key to both encrypt and decrypt data?
- Symmetric cryptographic algorithms use the same key to encrypt and decrypt the data.

Encryption through Software

- **File and File System Cryptography**
  - Encryption software can be used to encrypt or decrypt files one-by-one (file-level encryption)
  - Protecting groups of files can take advantage of the OS's file system
  - Third-party software tools available for encryption include GNU Privacy Guard (GnuPG), AxCrypt, Folder Lock, and VeraCrypt
  - Microsoft Windows Encrypting File System (EFS) is a cryptography system for Windows that is tightly integrated with the file system
  - Encryption and decryption are transparent to the user

Encryption through Software

- **Disk Encryption**
  - **Full-disk encryption** (**FDE**) protects all data on a hard drive
  - An example: *BitLocker* drive encryption software that is included in Microsoft Windows
  - BitLocker encrypts the entire disk, including the Windows Registry
  - **Volume-level encryption** protects a volume, which is a section of a drive that is accessible by a user and has a file system associated with it

Encryption through Software

- **Database Encryption**
  - **Database-level encryption** occurs in one of two ways
  - The plug-in method requires attaching an encryption module onto the DBMS
  - Transparent data encryption (TDE) executes encryption and decryption within the database engine itself
  - TDE does not require any additional packages or code modification of the database, engine, or DBMS and is easier to manage

Hardware Encryption

- Cryptography can be embedded in hardware, which provides a higher degree of security
  - It can be applied to USB devices and standard hard drives
- Cryptographic features can be built into the hardware of a USB device which allows for all data written to be automatically encrypted
- Some hardware-based USBs allow administrators to remotely prohibit accessing the data, lock out a user, or even instruct the drive to initiate a self-destruct sequence to destroy all data

Hardware Encryption

- **Self-encrypting drives** (**SEDs**) are drives that can protect all data written to them
  - The drive and host device perform authentication process during initial power up
  - If authentication fails, the drive can be configured to deny access or even delete encryption keys so all data is permanently unreadable
- A **hardware security model** (**HSM**) is a removable external cryptographic device that includes an onboard key generator and key storage facility
  - It performs accelerated symmetric and asymmetric encryption

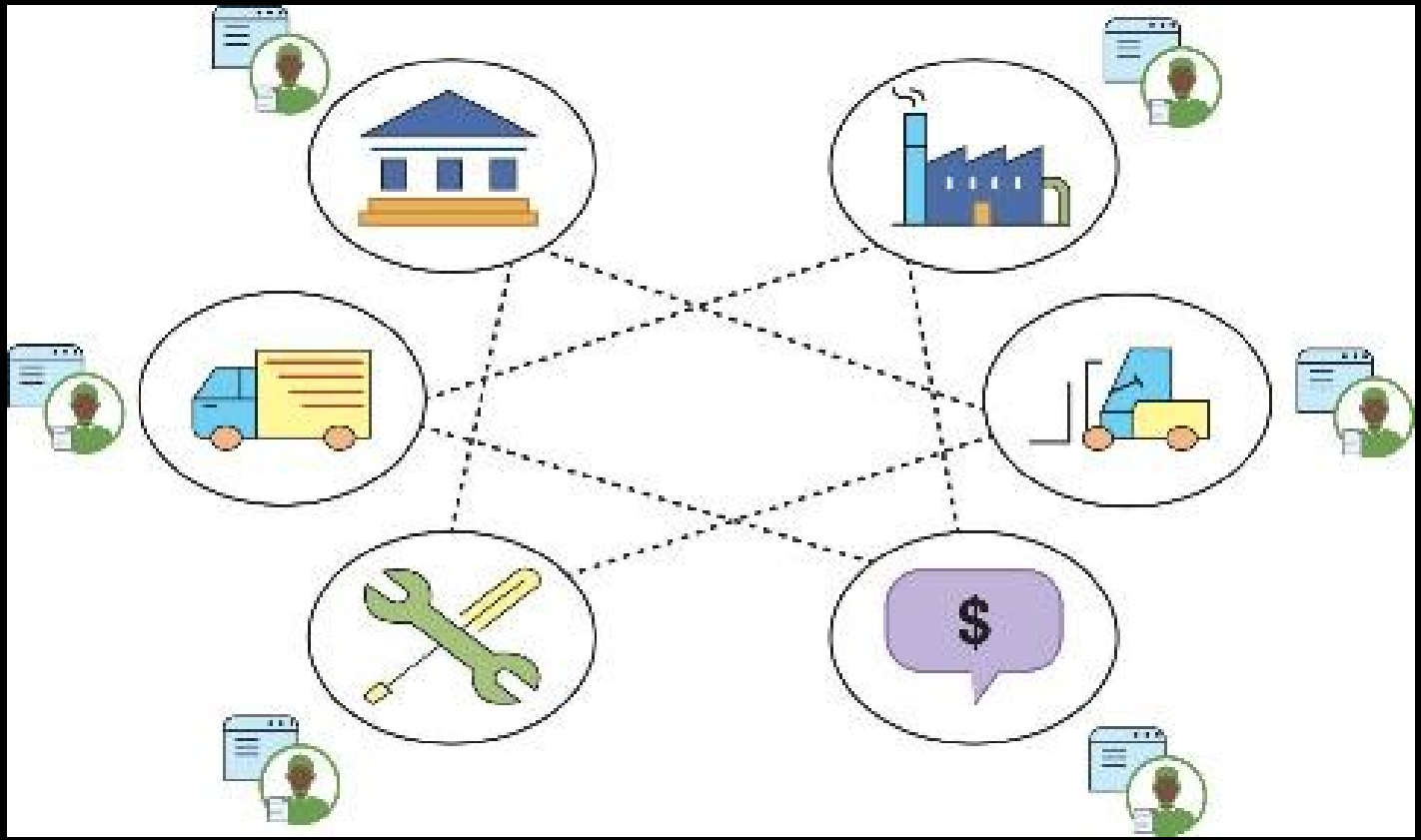
Hardware Encryption

- A **trusted execution environment** (**TEE**) is a secure cryptoprocessor that is internal to the computer itself
  - It protects the confidentiality and integrity of the code and data stored on it
- The **Trusted Platform Module** (**TPM**) is an international standard for cryptoprocessors that provides cryptographic services
- A TPM includes a random number generator and full support for asymmetric encryption and can also generate public and private keys
  - On Apple and Android devices it is called a **secure enclave**

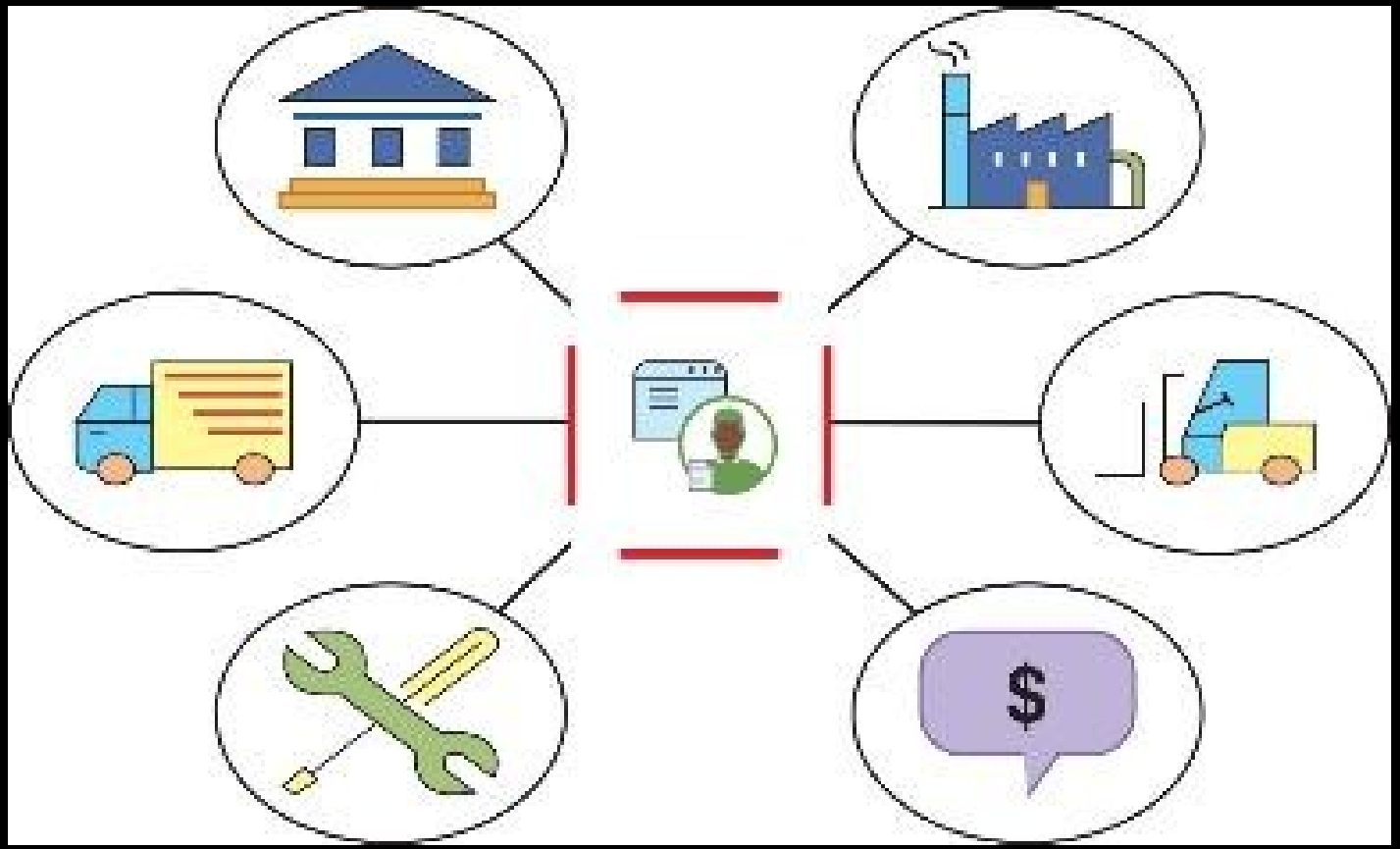
Blockchain

- A **blockchain** is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network
- Blockchain technology allows a network of computers to agree at regular intervals on the true state of a distributed ledger
- A **public blockchain** (open public ledger) is a blockchain network that anyone can join and become a part of
- A **private blockchain** operates in a closed network
- A **federated blockchain** (consortium blockchain) is typically used when organizations need both a public and private blockchain

Blockchain



Blockchain



Limitations of Cryptography

- Cryptography is a necessary feature to add to protect low-power devices and applications with fast response times to make them secure
- Adding cryptography to low-power devices or those that have fast response times can be difficult
  - Cryptographic algorithms require both time and energy, which results in a resource versus security constraint

Attacks on Cryptography

- Two of the most common cryptography attacks are algorithm attacks and collision attacks
- Methods attackers can use to circumvent strong algorithms include known ciphertext attacks and downgrade attacks
  - Statistical tools can be used to attempt to discover a pattern in the ciphertexts, which can then be used to reveal the plaintext or key
  - In a downgrade attack, an attacker forces the system to abandon the current higher security mode of operation and instead “fall back” to implementing an older and less secure mode

Attacks on Cryptography

- A **collision attack** is an attempt to find two input strings of a hash function that produce the same hash result
  - When two files have the same digest this is known as a **collision**
- A **birthday attack** is based on the *birthday paradox*, which says that for there to be a 50 percent chance that someone in a given room shares your birthday, 253 people would need to be in the room

Attacks on Cryptography

- **Quantum computing** relies on quantum physics using atomic-scale units (**qubits**) that can be both 0 and 1 at the same time
  - It is possible for one qubit to carry out two separate streams of calculations simultaneously
- Quantum computing also has a drawback for cybersecurity
  - A single quantum computer could perform factoring by using hundreds of atoms in parallel to quickly factor huge numbers, rendering all current asymmetric cryptographic algorithms useless
- Post-quantum cryptography algorithms are secure against an attack by a quantum computer