UNIT-2

intro to cryptography

```
science of protecting information by transforming it into a secure format,
known as encryption, so that only those for whom the information is
intended can read and process it.

objectives
    confidentiality - Ensuring that information is accessible only to those
authorized to have access
    integrity - Assuring that the information is accurate and unchanged
from its original form
    authentication - Verifying the identity of the parties involved in the
communication
    non-repudiation - Preventing any party from denying the authenticity of
their signature on a document or a message they sent
```

symmetric and asymmetric enc

```
symmetric enc
    symmetric encryption, the same key is used for both encryption and
decryption. This method is efficient and fast, making it suitable for
encrypting large volumes of data. However, the key distribution process
poses a significant challenge because the key must be shared between the
sender and recipient in a secure manner. If the key is intercepted, the
encrypted data can be compromised.
    Common symmetric encryption algorithms include AES (Advanced Encryption
Standard), DES (Data Encryption Standard), and 3DES (Triple DES).

asymmetric enc
    public-key cryptography, uses two different keys: a public key and a
private key. The public key is shared openly and is used for encrypting
messages, while the private key is kept secret by the owner and is used for
decryption. This method solves the key distribution problem of symmetric
encryption, as the public key can be shared with anyone without
compromising security.
    Asymmetric encryption is generally used for securing small amounts of
data due to its computational complexity and slower performance compared to
symmetric encryption. It is often used for secure key exchange, digital
signatures, and encrypting small pieces of data such as passwords
    Common asymmetric encryption algorithms include RSA (Rivest-Shamir-
Adleman), ECC (Elliptic Curve Cryptography), and DH (Diffie-Hellman).
```

hash functions and digi signs

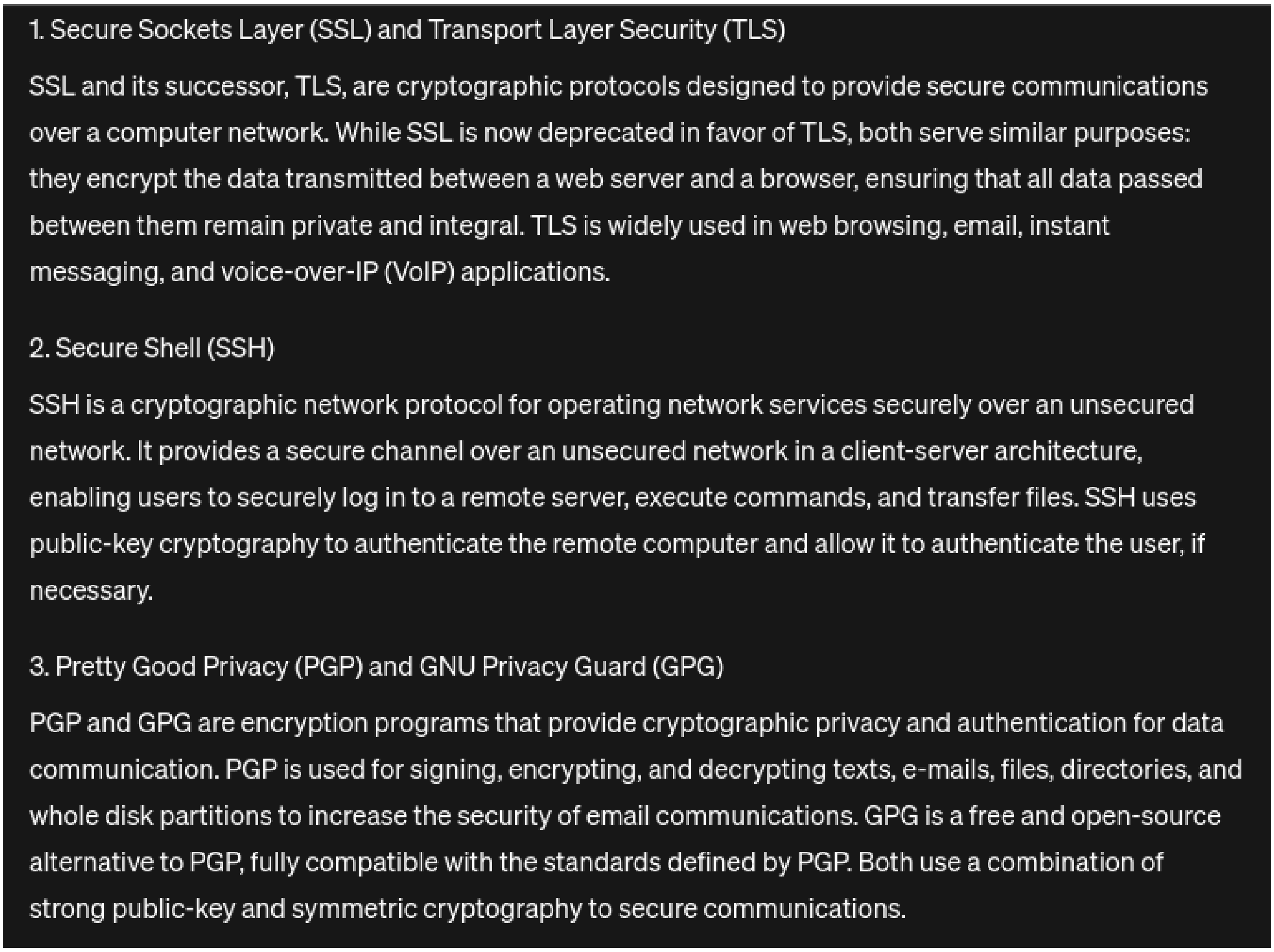
```
hash
    cryptographic algorithm that takes an input (or 'message') and returns a fixed-size string of bytes, typically a digest that appears to be random. The output, or hash value, represents the original string in a way that any alteration to the data will result in a different hash
    verifying data integrity, as it's computationally infeasible to find two different inputs that produce the same output (a property known as collision resistance)
    SHA-256 (Secure Hash Algorithm 256-bit) and MD5 (Message-Digest Algorithm 5), though MD5 is now considered insecure against collision attacks

digi sign
    verify the authenticity and integrity of a message, software, or digital document
    using a signer's private key (from asymmetric cryptography) to generate a signature that can be verified by anyone who has the signer's corresponding public key, confirming that the message was created by the known sender (authentication) and has not been altered in transit (integrity)
```

PKI

```
framework that supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks and verify the identity of the other party.
```

crypto protocols

```
structured sequences of operations that ensure secure electronic communications or data exchange. These protocols utilize the principles of cryptography to achieve various security goals, including confidentiality, integrity, authentication, and non-repudiation. They are essential for securing internet communications, electronic transactions, and data exchanges in an increasingly digital world
```



1. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

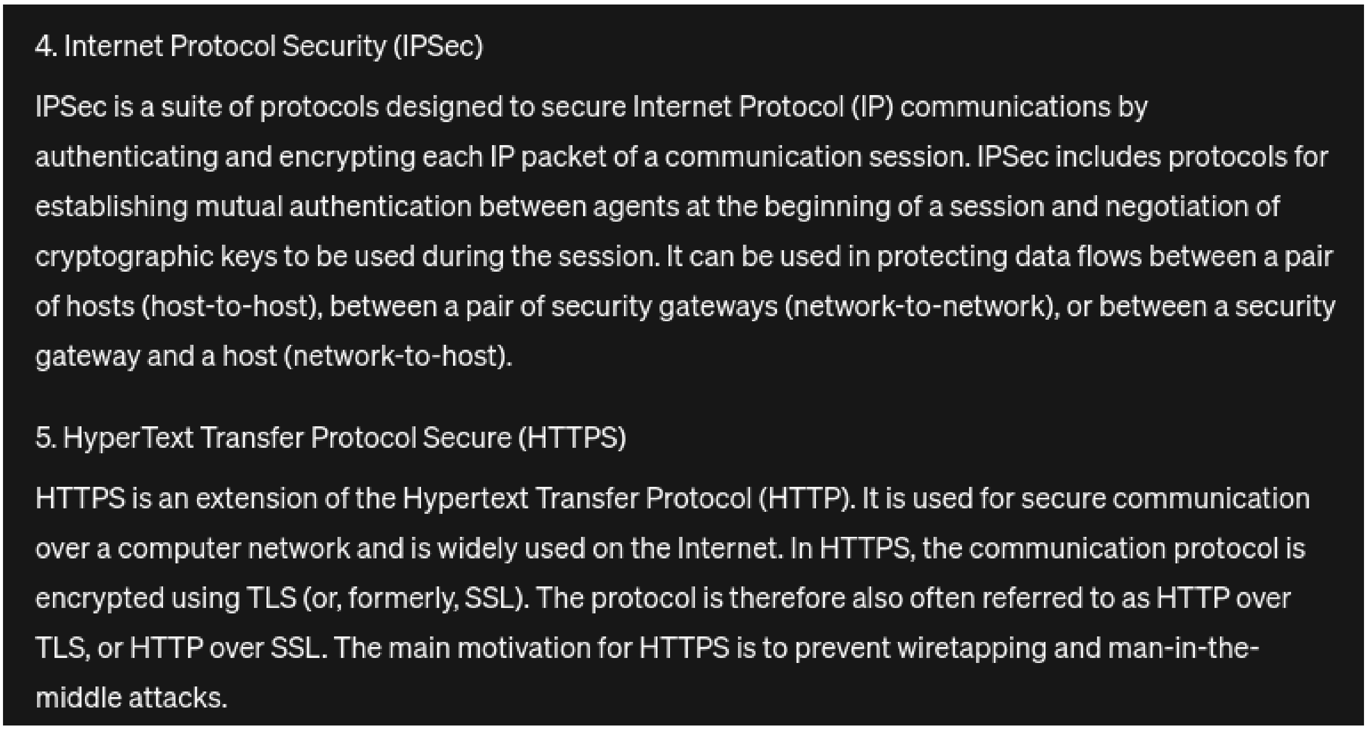
SSL and its successor, TLS, are cryptographic protocols designed to provide secure communications over a computer network. While SSL is now deprecated in favor of TLS, both serve similar purposes: they encrypt the data transmitted between a web server and a browser, ensuring that all data passed between them remain private and integral. TLS is widely used in web browsing, email, instant messaging, and voice-over-IP (VoIP) applications.

2. Secure Shell (SSH)

SSH is a cryptographic network protocol for operating network services securely over an unsecured network. It provides a secure channel over an unsecured network in a client-server architecture, enabling users to securely log in to a remote server, execute commands, and transfer files. SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary.

3. Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG)

PGP and GPG are encryption programs that provide cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions to increase the security of email communications. GPG is a free and open-source alternative to PGP, fully compatible with the standards defined by PGP. Both use a combination of strong public-key and symmetric cryptography to secure communications.



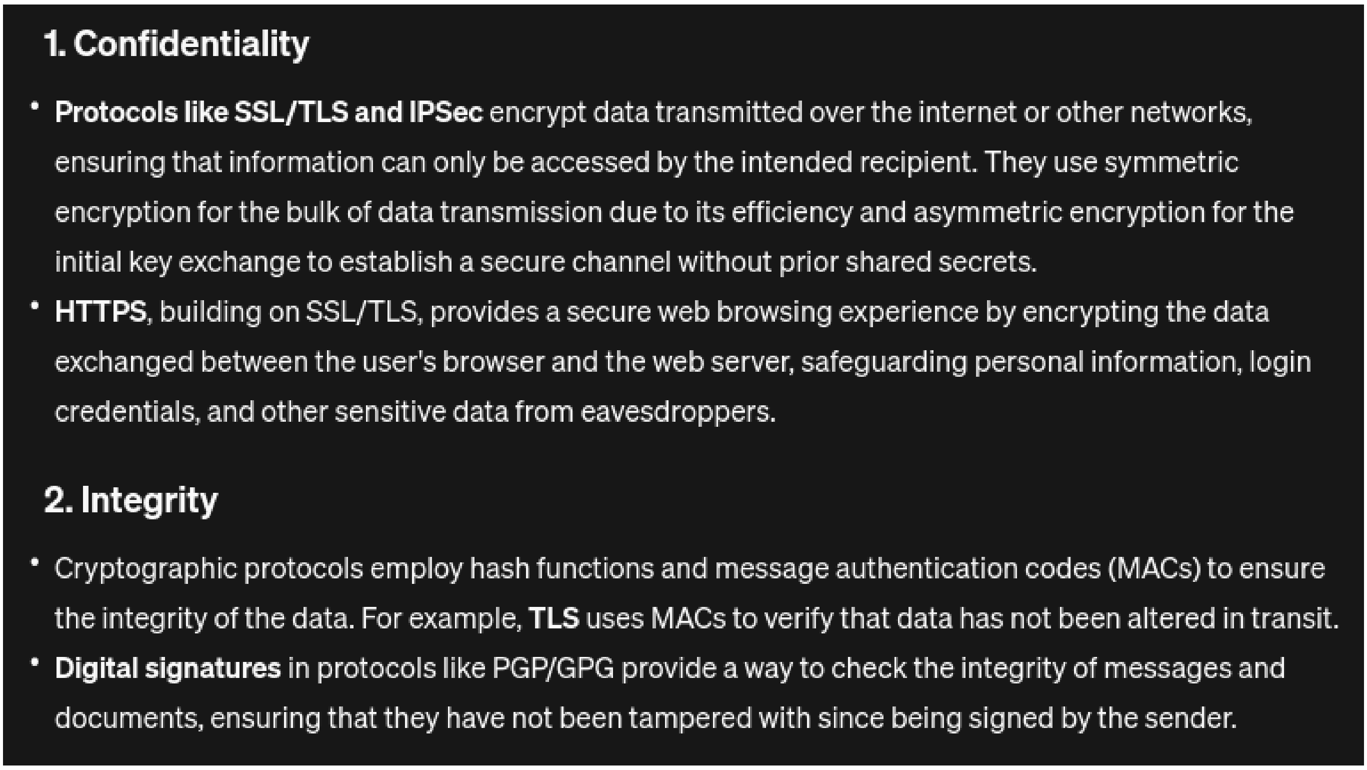
4. Internet Protocol Security (IPSec)

IPSec is a suite of protocols designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to be used during the session. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

5. HyperText Transfer Protocol Secure (HTTPS)

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using TLS (or, formerly, SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL. The main motivation for HTTPS is to prevent wiretapping and man-in-the-middle attacks.

```
wrt to basic principles of cryptography
```

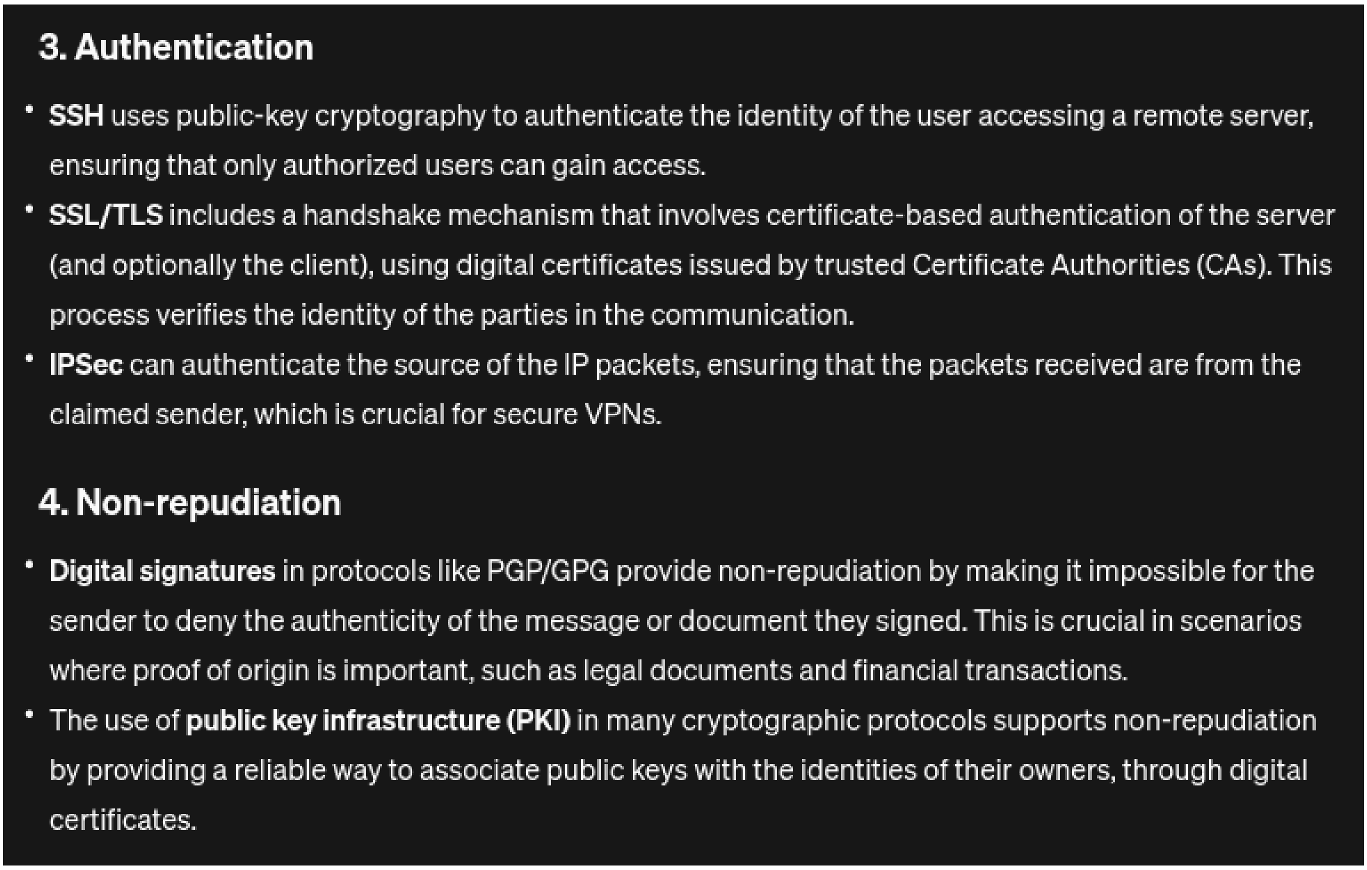


1. Confidentiality

- **Protocols like SSL/TLS and IPSec** encrypt data transmitted over the internet or other networks, ensuring that information can only be accessed by the intended recipient. They use symmetric encryption for the bulk of data transmission due to its efficiency and asymmetric encryption for the initial key exchange to establish a secure channel without prior shared secrets.
- **HTTPS**, building on SSL/TLS, provides a secure web browsing experience by encrypting the data exchanged between the user's browser and the web server, safeguarding personal information, login credentials, and other sensitive data from eavesdroppers.

2. Integrity

- Cryptographic protocols employ hash functions and message authentication codes (MACs) to ensure the integrity of the data. For example, **TLS** uses MACs to verify that data has not been altered in transit.
- **Digital signatures** in protocols like PGP/GPG provide a way to check the integrity of messages and documents, ensuring that they have not been tampered with since being signed by the sender.



3. Authentication

- **SSH** uses public-key cryptography to authenticate the identity of the user accessing a remote server, ensuring that only authorized users can gain access.
- **SSL/TLS** includes a handshake mechanism that involves certificate-based authentication of the server (and optionally the client), using digital certificates issued by trusted Certificate Authorities (CAs). This process verifies the identity of the parties in the communication.
- **IPSec** can authenticate the source of the IP packets, ensuring that the packets received are from the claimed sender, which is crucial for secure VPNs.

4. Non-repudiation

- **Digital signatures** in protocols like PGP/GPG provide non-repudiation by making it impossible for the sender to deny the authenticity of the message or document they signed. This is crucial in scenarios where proof of origin is important, such as legal documents and financial transactions.
- The use of **public key infrastructure (PKI)** in many cryptographic protocols supports non-repudiation by providing a reliable way to associate public keys with the identities of their owners, through digital certificates.

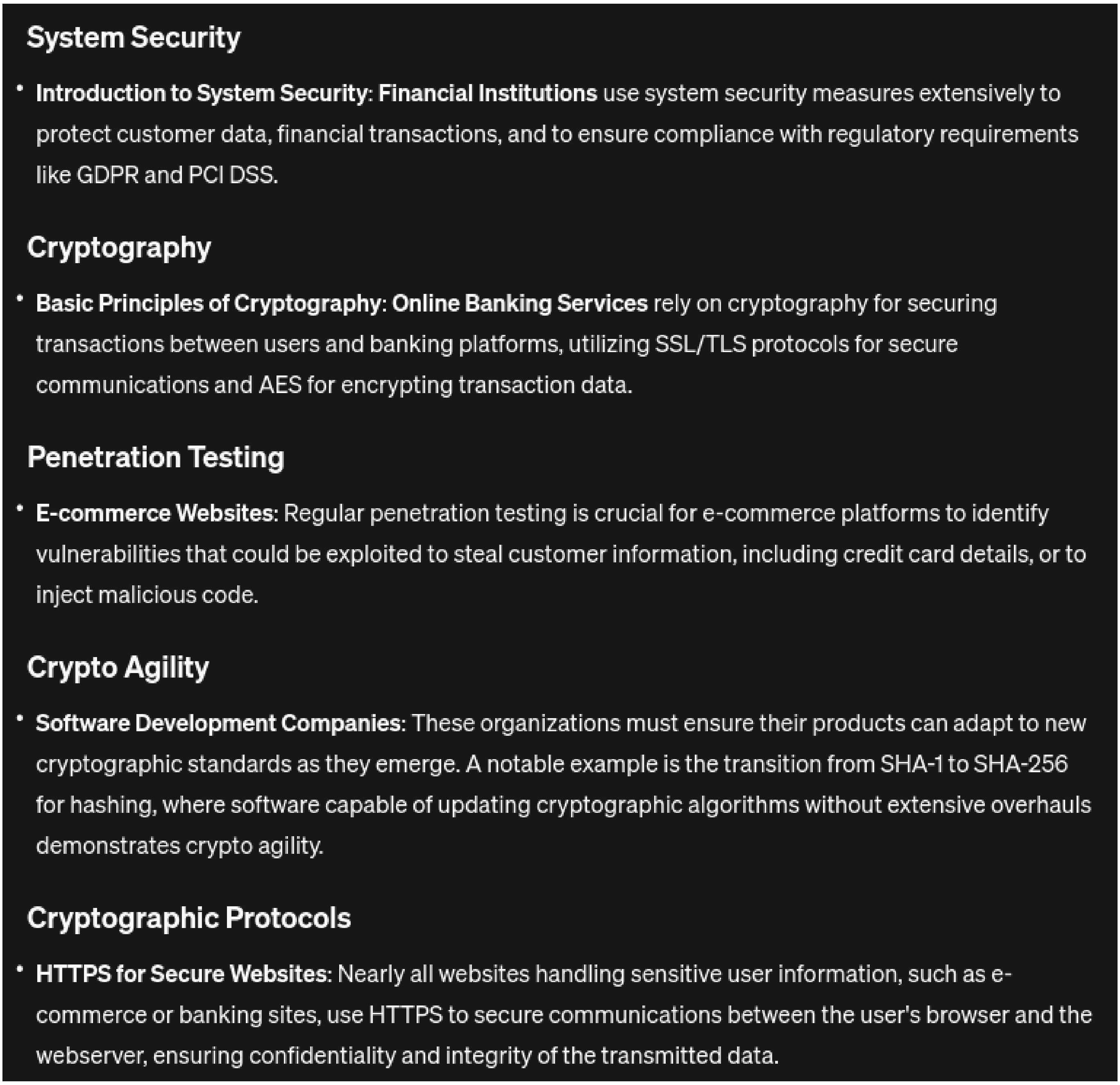
pen testing

crypto-agility

```
ability of a system to rapidly adapt to new cryptographic algorithms and
methods without requiring significant changes to the system's
infrastructure. This concept is increasingly important in the context of
system security, cryptography, and even penetration testing, given the
```

```
fast-paced evolution of cyber threats and the potential for current
cryptographic standards to be compromised or become obsolete.

importance
    adapting to advanced cryptographic standards
    responding to vulnerabilities
    compliance and pen testing

implementing - key considerations during design
    modular crypto
    standardized algos and protocols
    config and policy management
    future-proofing

challenges
    complexity of system
    potential misoconfig of sys
```

real-world applications



System Security

- **Introduction to System Security: Financial Institutions** use system security measures extensively to protect customer data, financial transactions, and to ensure compliance with regulatory requirements like GDPR and PCI DSS.

Cryptography

- **Basic Principles of Cryptography: Online Banking Services** rely on cryptography for securing transactions between users and banking platforms, utilizing SSL/TLS protocols for secure communications and AES for encrypting transaction data.

Penetration Testing

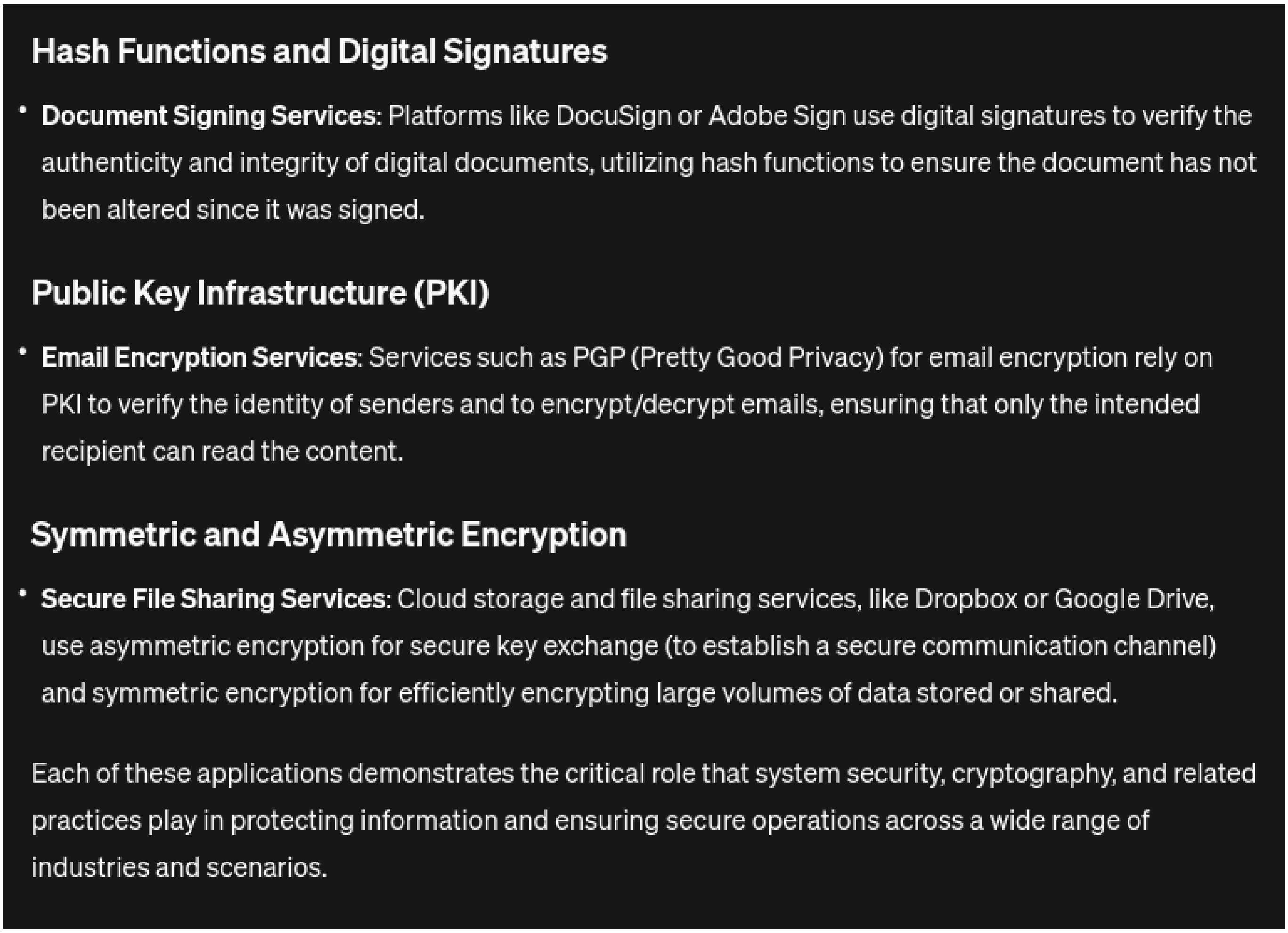
- **E-commerce Websites**: Regular penetration testing is crucial for e-commerce platforms to identify vulnerabilities that could be exploited to steal customer information, including credit card details, or to inject malicious code.

Crypto Agility

- **Software Development Companies:** These organizations must ensure their products can adapt to new cryptographic standards as they emerge. A notable example is the transition from SHA-1 to SHA-256 for hashing, where software capable of updating cryptographic algorithms without extensive overhauls demonstrates crypto agility.

Cryptographic Protocols

- **HTTPS for Secure Websites**: Nearly all websites handling sensitive user information, such as e-commerce or banking sites, use HTTPS to secure communications between the user's browser and the webserver, ensuring confidentiality and integrity of the transmitted data.



Hash Functions and Digital Signatures

- **Document Signing Services:** Platforms like DocuSign or Adobe Sign use digital signatures to verify the authenticity and integrity of digital documents, utilizing hash functions to ensure the document has not been altered since it was signed.

Public Key Infrastructure (PKI)

- **Email Encryption Services:** Services such as PGP (Pretty Good Privacy) for email encryption rely on PKI to verify the identity of senders and to encrypt/decrypt emails, ensuring that only the intended recipient can read the content.

Symmetric and Asymmetric Encryption

- **Secure File Sharing Services:** Cloud storage and file sharing services, like Dropbox or Google Drive, use asymmetric encryption for secure key exchange (to establish a secure communication channel) and symmetric encryption for efficiently encrypting large volumes of data stored or shared.

Each of these applications demonstrates the critical role that system security, cryptography, and related practices play in protecting information and ensuring secure operations across a wide range of industries and scenarios.

Cryptography

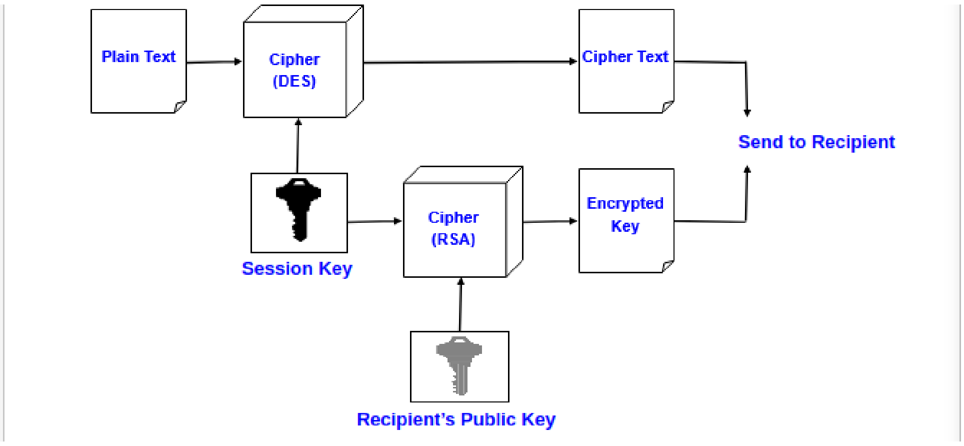
components

- encryption
  - symmetric
    - same key for encryption and decryption
    - types
      - block cipher - in blocks of data
      - stream cipher - 1 byte/bit at a time
    - strength of algo depends on key length
      - key space - set of possible keys for a cipher
    - substitution ciphers
      - caesar cipher
      - monoalphabetic cipher
        - each letter is substituted for any other unique letter
        - briute force too time consuming; statistical analysis would make it feasible to crack the key
      - polyalphabetic cipher
        - use a sequence of monoalphabetic ciphers in tandem
        - obtain a key and shift the letters by the key and remove the key
        - mapping must be one-to-one
      - columnar transposition
        - rearrangement of chars in the plain text into columns

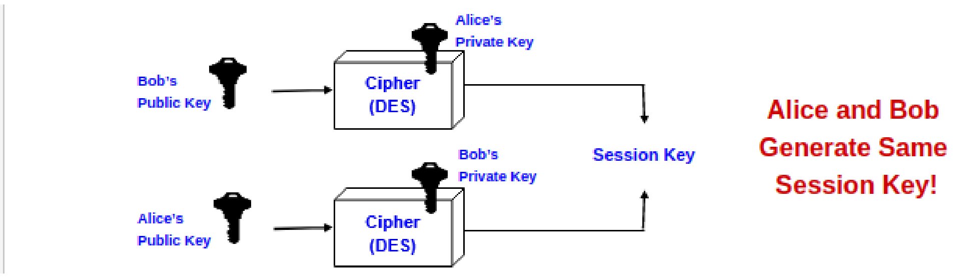
        - if letters are insufficient, pad with x or y(say)

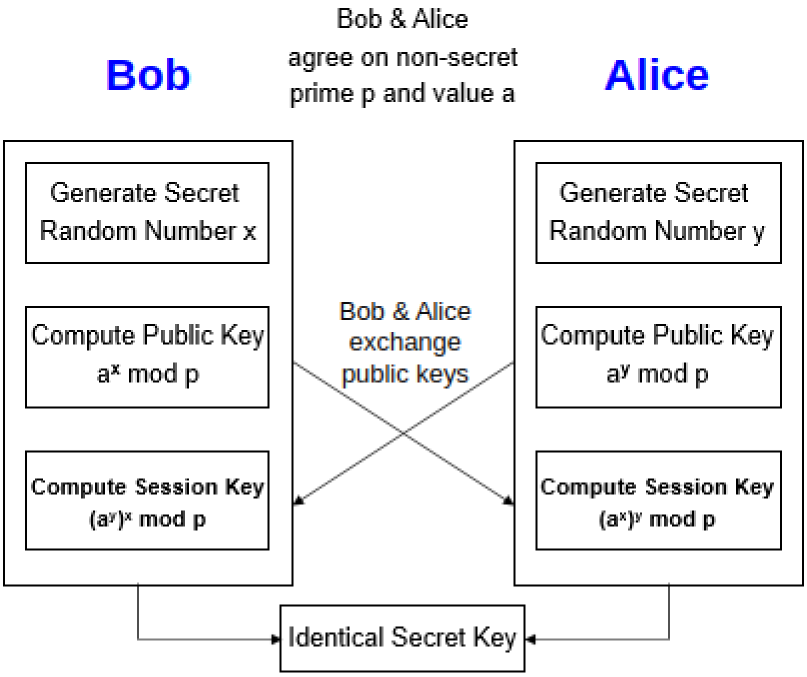
      - shannon's characteristics of good encryption
        - amt of secrecy should determine labour needed for enc and dec
        - keys and algo should be free of complexity
        - err in cipher must not propagate and corrupy further info in the message
        - size of enc text <= size of plain text
      - properties of trustworthy sys
        - based on sound math
        - tested by competent experts
        - stood the test of time
    - limitations
      - exposure to secret key compromises secrecy
      - key must be delivered to recepient for decryption
        - susceptible to eavesdropping attacks
  - asymmetric
    - pair of keys
      - public key - encryption
      - private key - decryption
    - secret transmission of key not required
    - types
      - RSA(Rivest-Shamir-Adleman)
        - public and private keys interchangeable
        - variable key size
      - El Gamal
        - variable key size
    - limitations
      - less efficient than symmetric
      - susceptible to MITM attacks
        - hacker gens key pair and gives public key away claiming it belongs to someone else
        - users use this key and hacker will be able to decrypt it
      - problematic to gen key pair
    - session key enc
      - improve efficiency
        - symmetric key for encrypting key

- asymmetic key to encrypt symmetric key



- encryption protocols
  - PGP(pretty good privacy)
    - email encryption using session key encryption
    - cobines RSA, 3DES and other algos
  - S/MIME(secure/multipurpose internet mail extension)
    - to secure email
    - backed bby MS, RSA
  - SSL and TLS
    - securing TCP/IP traffic
    - mainly for web use
    - for any kind of internet traffic
- key agreement
  - create secret key only by exchanging public keys
  - key agreement algo uses exchanged public keys and their own private keys to gen a common session key
  - no need to exhange keys



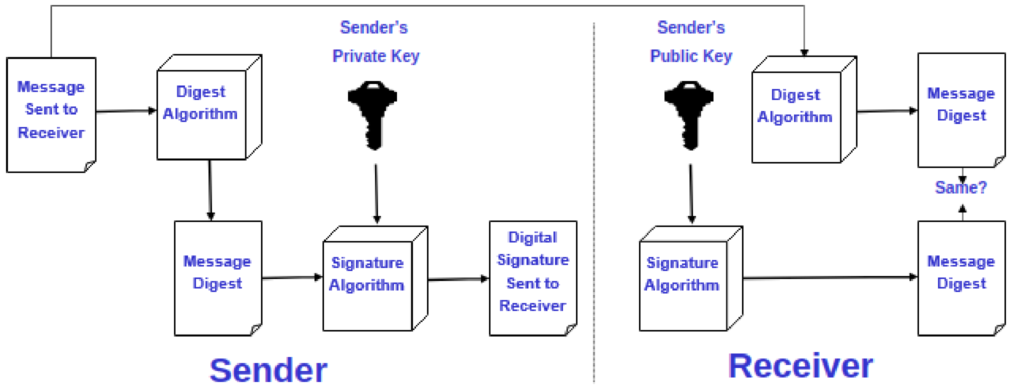

Bob
Bob & Alice agree on non-secret prime p and value a
Alice
Generate Secret Random Number x
Compute Public Key a^x mod p
Compute Session Key $(a^y)^x$ mod p
Bob & Alice exchange public keys
Generate Secret Random Number y
Compute Public Key a^y mod p
Compute Session Key $(a^x)^y$ mod p
Identical Secret Key

        - diffie-hellman
- authentication and integrity
    - authentication
        - validating identity of a user or the integrity of a piece of data
            - MD/MAC
                - MD
                    - provide proof that data has not been altered
                    - hashing
                        - hash functions - one way functions
                            - irreversible
                            - infeasible to construct 2 messages which hash to the same digest
                    - MD5(128 bit), SHA(162 bit)
                - MAC
                    - MD created with a key
                    - secret key possessed by both parties to retrieve the mssg
            - digi sign
            - PKI
        - types of user authentication
            - identity presented by app in a session
            - sender's identity presented along with a message

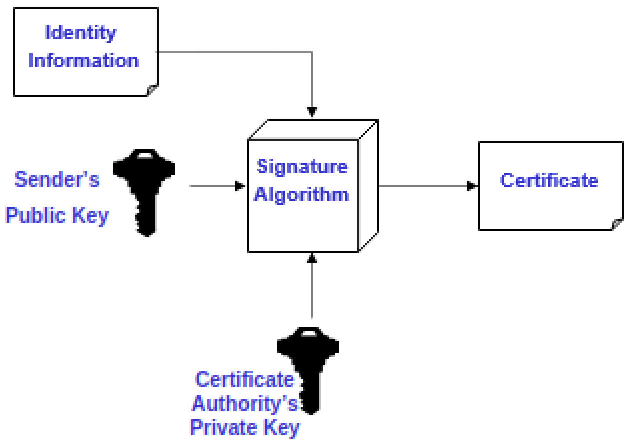
---

        - personal tokens
            - H/W devices that gen unique strings used in conjunction with psswd for auth
            - types
                - storage token
                    - secret val stored on a token available after it is unlocked with a pin
                - synch one-time psswd
                    - gen psswd periodically based on time and a secret code stored on token
                - challenge response

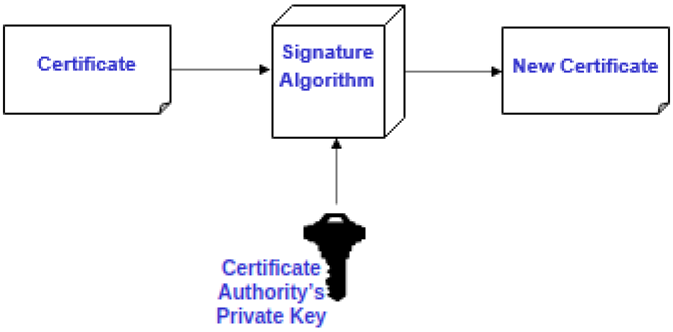
      - token computes num based on challenge sent by server
    - digi sign token
      - contains the digi siggn private key and computes a digi sign on a supplied val
  - variety of physical forms
    - hand held devices
    - smart cards
    - USB tokens
- biometrics
  - bio chars for authentication
    - fingerprint
    - iris
    - voice recog
    - handwriting
- digi sign
  - digital stamp on digital info like email and e-docs
  - assures that the info originated from the sender and hasn't been tampered with



- digi cert
  - signed statement by a trusted party that another party's public key belongs to them
    - allows one CA to be authorized by another(root CA)
  - authenticates the identity of the ord, individual, etc.
  - top level CA must be self-signed



  - anyone can start a CA
- cert chaining
  - signing cert with another priv key that has a cert for its public key



      - belongs to a CA

cryptanalysis

- breaking enc code
    - recog patterns in enc msgs
    - infer meaning without breaking code; analyzing frequency of comm
    - deduce key
    - id weaknesses in algo

DES(Data encryption standard)

- every bit of enc text depends on every bit of inp data and every bit of key
- block cipher
    - 64 bit blocks = 58 + 8(parity bits)
    - 64 bits -> 56 bit key
- runs in reverse to decrypt
- 3DES - 3 DES in tandem; output of one DES is the input to another

AES(advanced encryption standard)

- symmetric
- in blocks of 126/192/256 bits

Password authentication

- psswd is secret char string only known to user and server
- MD common for psswd auth
- store hash of psswd to reduce of risk
- probs
    - attacker learns psswd via
        - social eng
        - brute force
        - eavesdropping
        - by replaying enc psswd back to auth server
            - replaying - capturing a valid net transmission and retransmitting it later

Authentication protocols

- set of rules governing comm of data related to auth b/w server and user
- techniques to build protocol
    - transformed psswd

        - tranform psswd using one way func before transmission
        - prevents eavesdropping but not replay
    - challenge response
        - server send challenge along with auth request; must be included in response
        - prevents replay
    - time stamp
        - auth from client to server must have time stamp embedded; server check if time is reasonable
        - prevents against replay
    - OTP
        - new psswd obtiained by passing through one-way func n times
        - protects against replay and eavesdropping

- kerberos
    - auth service using symm key enc and key distro center
    - auth server contains symm keys of all users and info on which user has access privilege to which services on the network

PKI(public key infrastructure)

key exchange with key server

key server

- creates and transmits secure session keys to users
- takes care of the initial validation of user's identities

building blocks

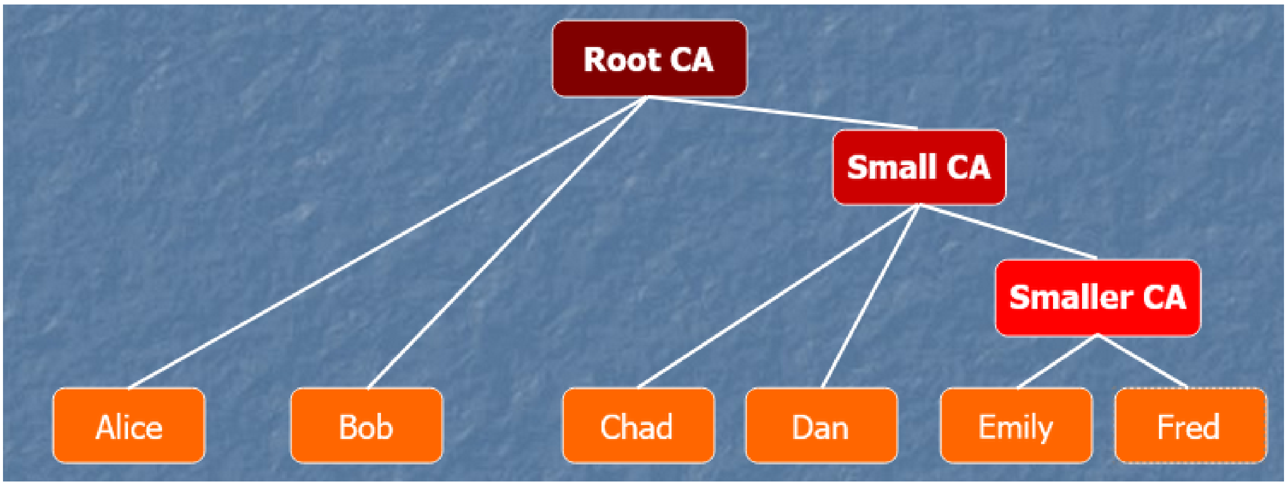
- crypto tools
    - symmetric enc - used for most comm
    - asymmetric enc(public key enc) - used for exchaning symmetric keys
    - digi sign -to validate public keys
- names
    - a name in a PKI must be unique to a user
- time
    - PKI must know current time
    - relies heavily on having an accurate clock
- secure comm session
    - use asymmetric cryptography to exchange symmetric key

certificates

- combo of user's public key, common name, start and expiration dates, etc.
- digitally signed by a trusted 3rd party(CA); sign attached to the rest of the cert
- CAs can delegate trust

models

- strict hierarchy



- networked
  - when 2 or more PKIs wish to merge
    - mesh - every root CA signs every other root CA's cert
    - hub-and-spoke - CAs combine to form super root CA; each root CA signs the super root CA's cert while super root CA signs each of theirs
- web browser
  - browser maintains a list of trusted CAs
- PGP
  - each user's cert digned by 0 or more other users
  - cert validity determined by levels of trust assigned by signers

Penetration testing

- test evaluating strengths of all sec controls on the comp sys
- evaluates procedural and operational controls as well as technological controls
- orgs stroing sensitive data requrie regular pen testing
- external vs internal
- overt vs covert(with and without the knowledge of the IT dept)

phases

- reconnaissance and info gathering
  - collect as much info as possible wihout making actual network contact with the target
  - methods
    - Google search
    - website browsing
- network enumeration and scanning
  - discover existing nets owned by a target as well as live hosts and services running on those hosts
  - methods
    - DNS querying - request info from a DNS server
    - route analysis - best route from one net to another
- vulnerability testing and exploitation
  - cehck hosts for known vulnerabilities and to see if they are exploitable
  - methods

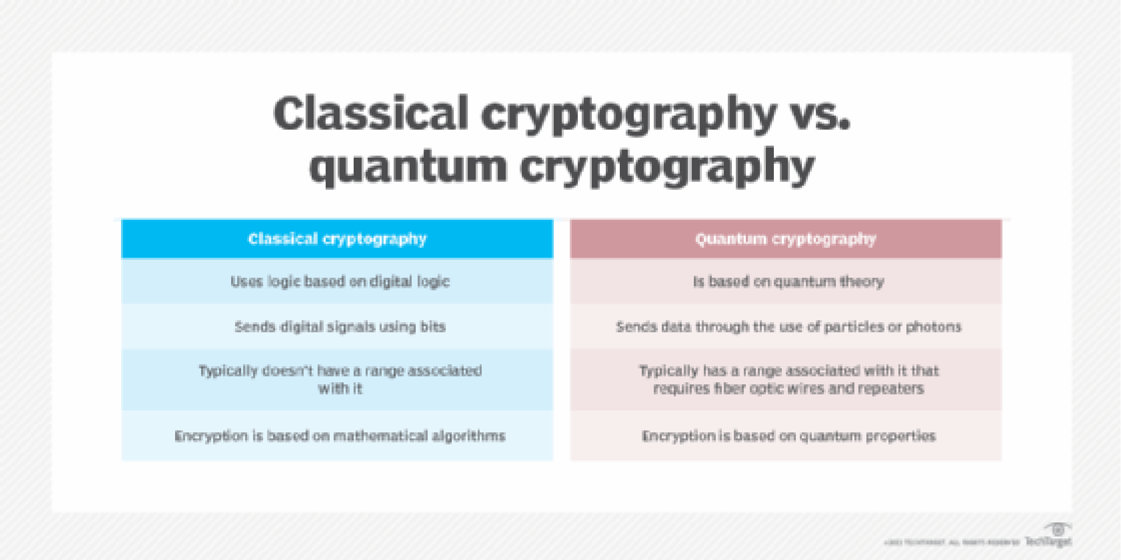
        - remote vulnerability scanning
- reporting
    - document info found and report to the org

Crypto-agility

- the ability to replace crypto primitives, algo and protocols with limtied impact on operations and with low overhead
- CARAF(crypto agility risk assessment framework)
    - identify threats
    - inventory of assets
    - risk estimation
    - secure assets through risk mitigation
    - roadmap

Quantum Cryptography

- quantum computing
  - computing that seeks to exploit properties of quantum mech to speed up computing
  - traditional computers use binary bits; quantum computers use qubits - can represent a diffrent composition of 0 and 1 at the same time
- quantum cryptography
  - quantum concepts only used in the distribution of keys while the actual transmission of data is down with classical algos
  - could still be hacked by methods such as tailored illumination
  - unconditionally secure; phy realisations of those sys violate some of the assumptions of the security proof
- post-quantum cryptography
  - develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks
- QKD(quantum key distibution)
  - use of quantum physics to distribute keys
- a quantum safe transition strategy
  - know your risks - assess your crypto agility maturity and readiness
  - focus of crypto agility



Classical cryptography vs. quantum cryptography

Classical cryptography	Quantum cryptography
Uses logic based on digital logic	Is based on quantum theory
Sends digital signals using bits	Sends data through the use of particles or photons
Typically doesn't have a range associated with it	Typically has a range associated with it that requires fiber optic wires and repeaters
Encryption is based on mathematical algorithms	Encryption is based on quantum properties