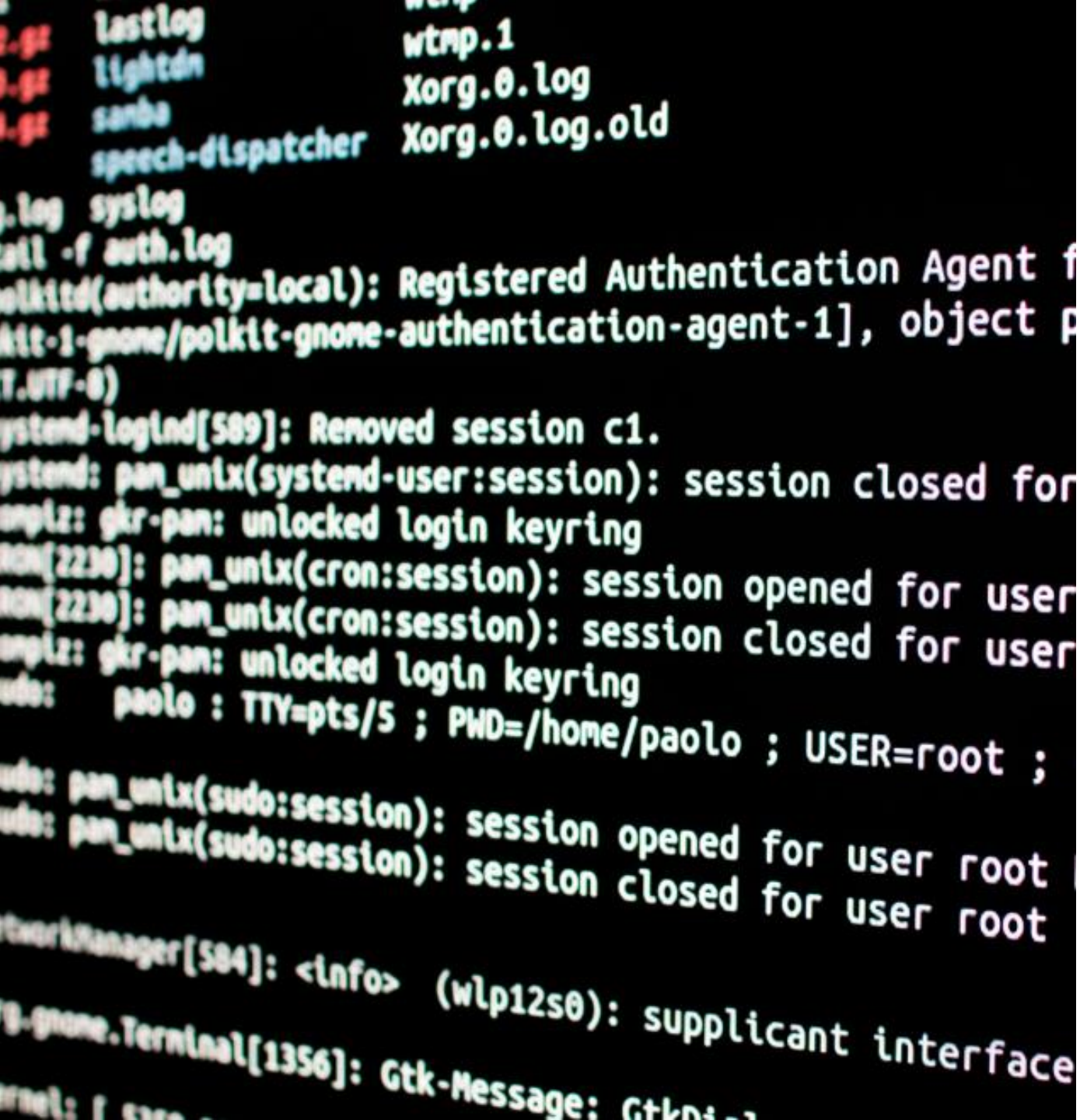
PRACTICAL CRYPTOGRAPHY

Objectives

- Compare symmetric and asymmetric cryptography
- Learn about encryption levels as in full disk, partition, file, volume, database, and record
- Examine hashing, salting, HMACs, and key exchange
- Explore digital signatures, certificates, and PKI
- Observe various cryptographic tools
- Understand blockchain technology



CRYPTOGRAPHIC SERVICES

- **Confidentiality**
  - Hiding the data at rest, in transit, and/or in use from unauthorized principals
  - It typically involves a system or algorithm that converts plaintext data into ciphertext
- **Integrity**
  - Ensures the data has not been altered while at rest or in transit
- **Non-repudiation**
  - Ensures the original sender cannot deny sending data or engaging in a digital transaction

SYMMETRIC KEY CRYPTOSYSTEMS

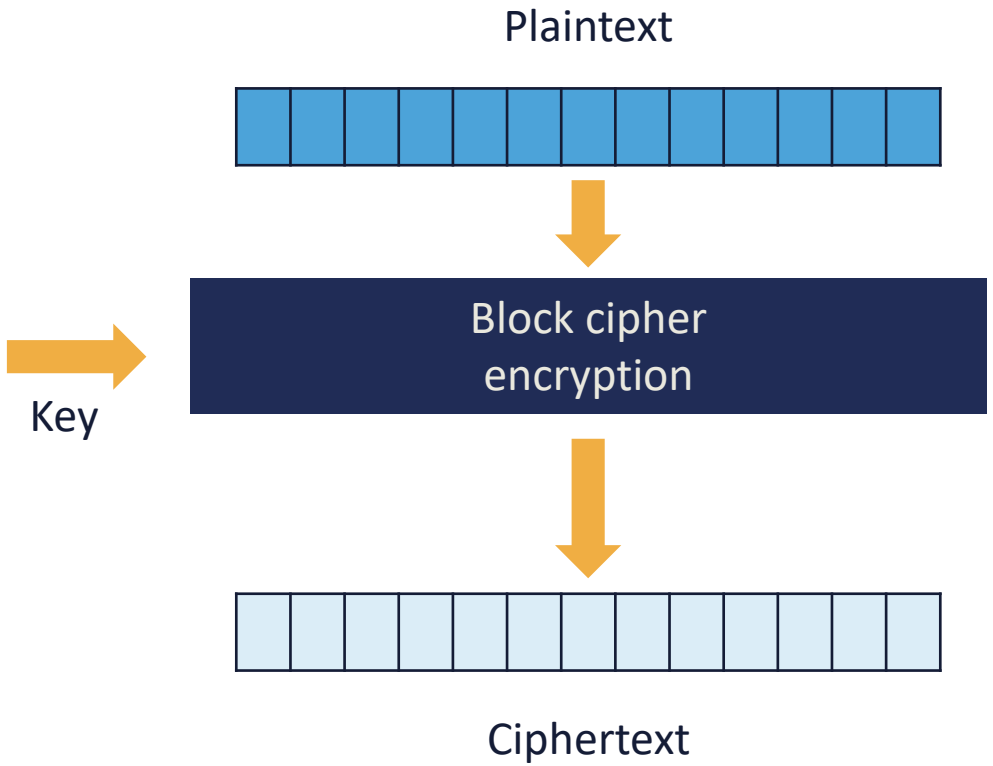
- This historic form uses the same key to encrypt and decrypt
- Efficient, fast, and handles high data rates of throughput
- Computationally inexpensive
- Deploys shorter key lengths (40 to 512 bits)
- Primarily used to protect data at rest

SYMMETRIC KEY CRYPTOSYSTEMS

- Key management is more complex unless using hardware security modules (HSMs) or cloud key management services
- There is no built-in origin authentication
- Symmetric systems do not scale well unless a cloud key management service is used
- Most popular algorithms are AES-CBC-128/256 and AES-GCM-128/256

BLOCK CIPHERS

- Operates on fixed blocks of data (bits) based on key size
- 64, 128, and 256-bit keyspaces are common
- Messages bigger than the key size are broken into blocks the size of the key and must include padding
- Common block ciphers:
  - DES
  - 3DES-EDE
  - AES-CBC
  - AES-GCM
  - Blowfish



STREAM CIPHERS

- Operate on a continuous stream of plaintext data by encrypting one bit or byte at a time
- Plaintext bits are typically XORed with keystream bits
- Keystream = random bits, bytes, numbers, characters
- Faster and less complex than block ciphers
- Modern ciphers can work in a block or stream mode or both:
  - FISH
  - CryptMT
  - Scream
  - Cryptographic hashing

STREAM CIPHER EXAMPLE

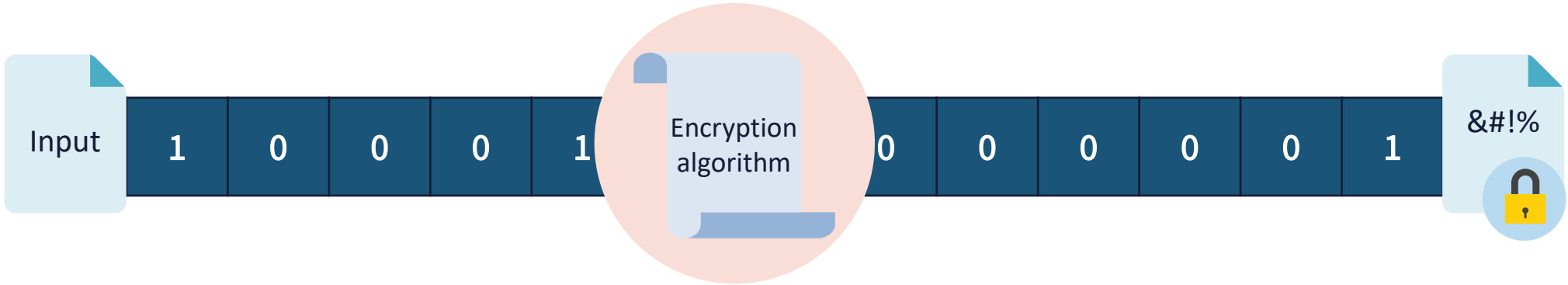
- Alice wants to use a stream cipher to encrypt the letter "A"
- In ASCII, the letter "A" has the value of 65 = 1000001
- The first cipher stream bits are 0101100
- We perform an XOR function (Modulo 2 addition)

  1000001 = A

  XOR

  0101100

  1101101 is the result
- The letter "A" becomes ciphertext "m" (ASCII value 109)

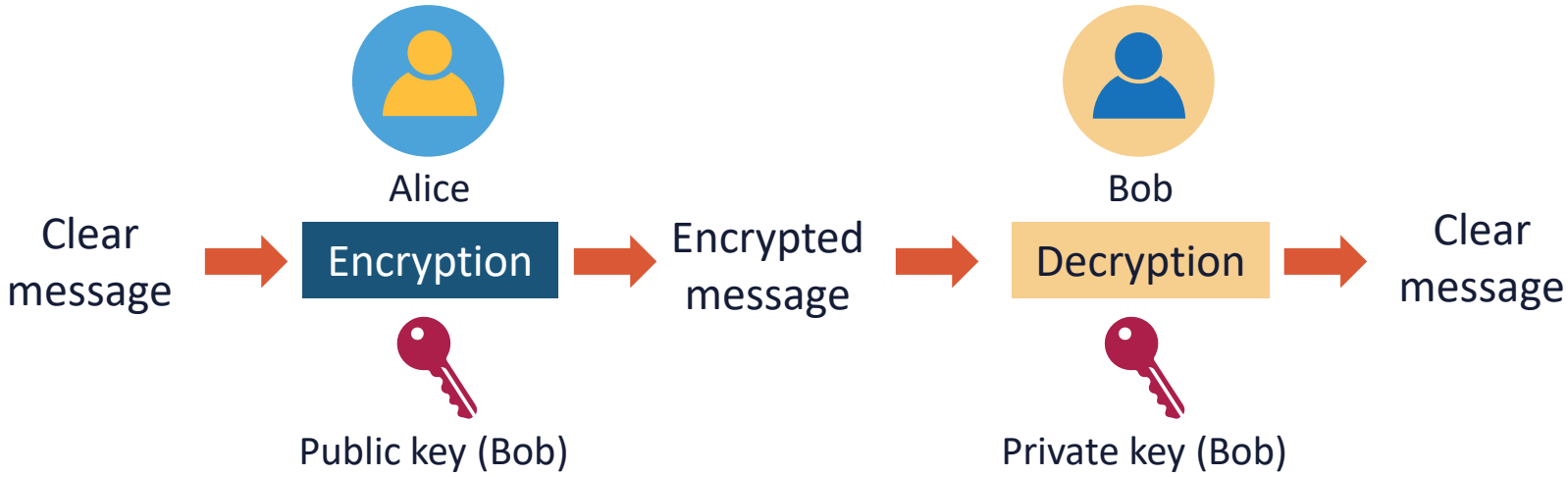


ASYMMETRIC KEY CRYPTOSYSTEMS

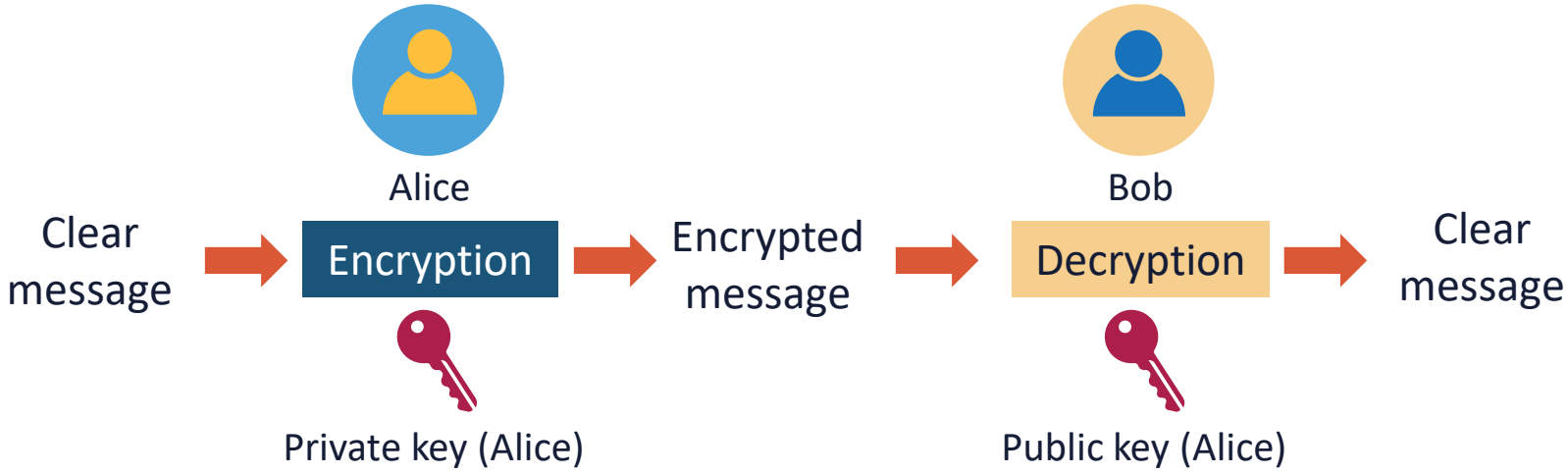
- Uses a mathematically related pair of a public and private key
  - If one is used to encrypt, the other is used to decrypt
- Public key infrastructure (PKI) enables efficient key management and scalability
- Often used for digital signatures and key exchange
- Employs longer key lengths than symmetric (up to 4096)
- Slower and more computationally expensive

ASYMMETRIC KEY CRYPTOSYSTEMS

- Confidentiality
  - Encrypt with public key
  - Decrypt with private key



- Origin authentication
  - Encrypt with private key
  - Decrypt with public key



POPULAR ASYMMETRic (PUBLIC KEY) ALGORITHMS

- RSA (Rivest–Shamir–Adleman) – the most widely used algorithm for securing communication and data encryption
- Diffie-Hellman key exchange – a protocol for securely exchanging cryptographic keys over an untrusted network
- Elliptic curve cryptography (ECC) – an algorithm based on the algebraic structure of elliptic curves over finite fields
- Digital signature algorithm (DSA) – a standard based on the mathematical concept of modular exponentiation and discrete logarithm problem

FULL DISK ENCRYPTION

- Full disk encryption (FDE) is the process of encoding all user data on a device using an encrypted key
- Also called whole disk encryption – the master boot record (MBR) (or comparable) that includes code that loads the operating system is not encrypted
- Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk

PARTITION ENCRYPTION

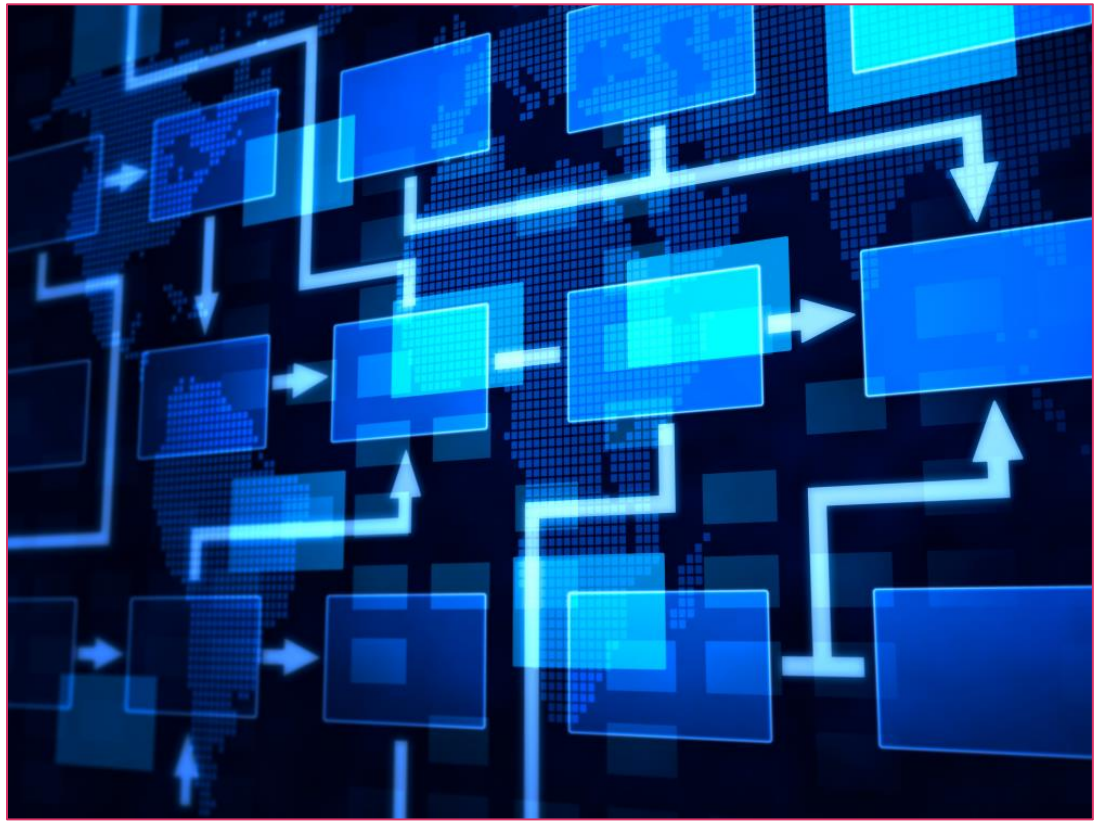
- Encrypted partitions are disk partitions that are protected with encryption keys to prevent unauthorized access to the data on the drive
- One advantage of encrypting only a partition instead of the whole drive is that you can encrypt/decrypt the partition while using the system for other tasks
- If one only encrypts a data partition, however, sensitive data can remain in temporary files or swap files in a non-encrypted partition

FILE ENCRYPTION

- File-level encryption enables the protection of individual files by encrypting them
- This technique is often utilized when there are specific files that need an extra degree of security or contain very sensitive information
- Encrypting individual files offers more control over access and assures that even if one file is cracked, the others will still be safe

VOLUME (BLOCK) ENCRYPTION

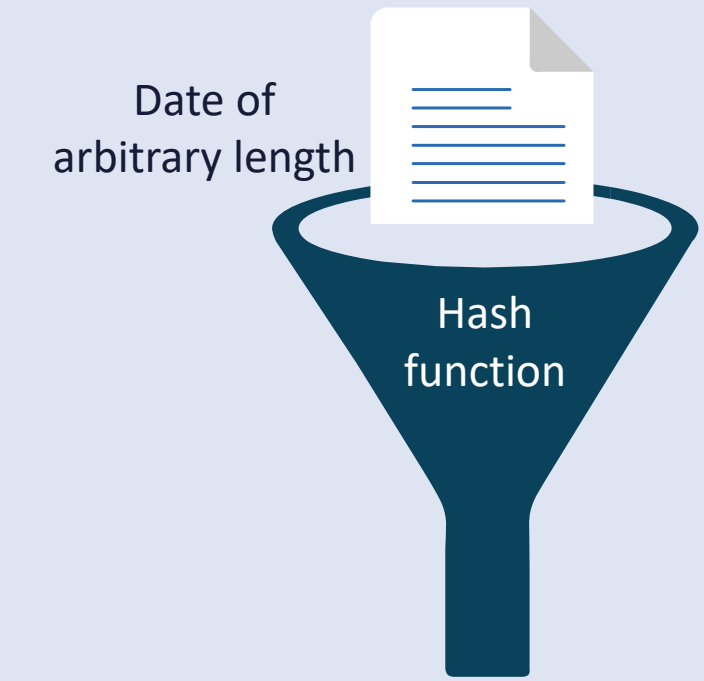
- Volume encryption targets a section of the physical drive, which is defined as a separate partition or "volume"
- It provides a choice to encrypt different volumes, whereas with disk encryption, you can only encrypt everything
  - Volume encryption can help save time and provide greater flexibility
- If a single volume occupies the entire hard drive, then volume encryption will function the same way as full disk encryption



DATABASE AND RECORD ENCRYPTION

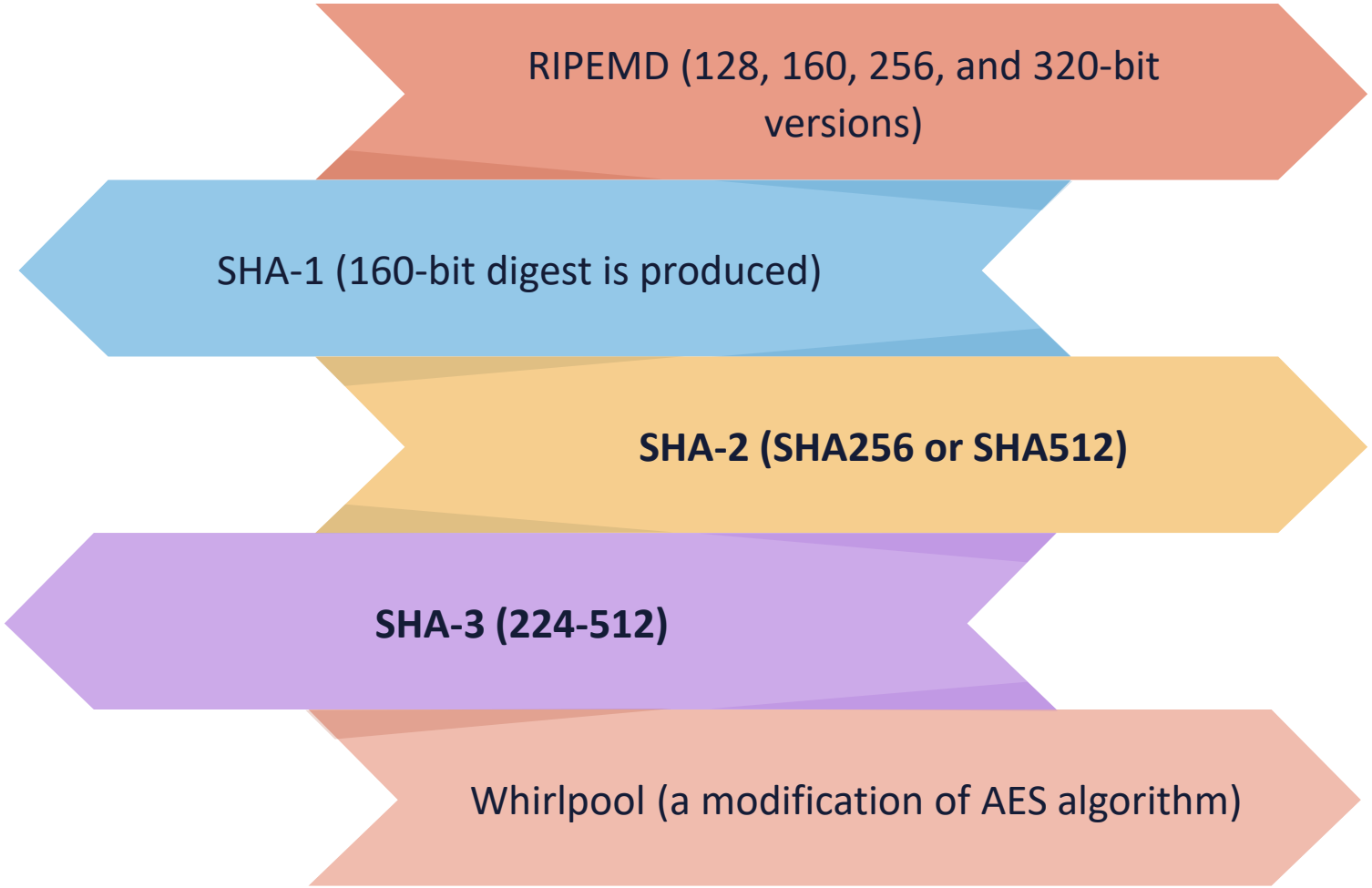
- Database encryption is the process of using an algorithm to transform data stored in a database into unreadable cipher text
- The purpose is to protect the data stored in various platforms from being accessed by external attackers or even compromised privileged insiders
- When using a cloud database service, key management services are often used
- Record encryption will encrypt and decrypt the individual records in a database systems

CRYPTOGRAPHIC HASHING



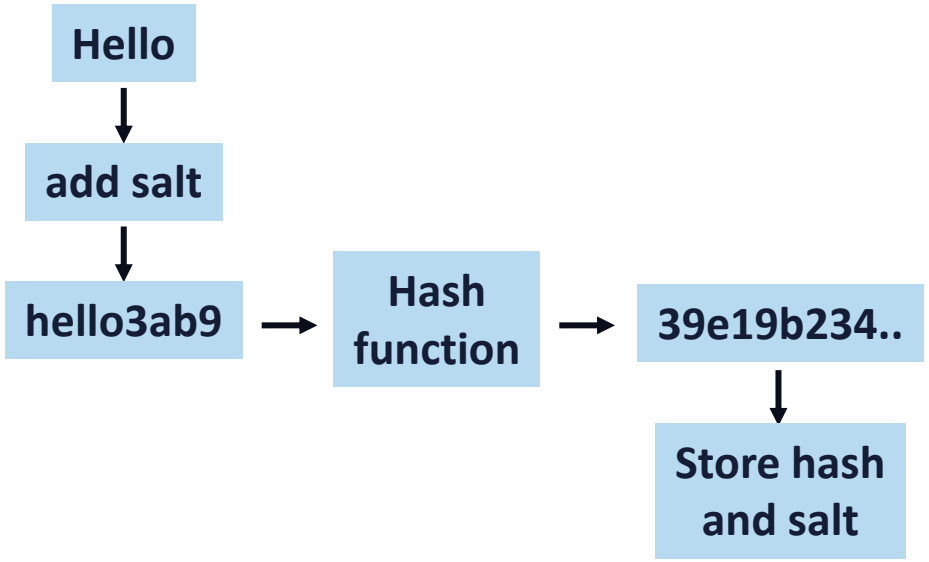
- A one-way mathematical function that produces a digest of 128 to 512 bit
- Converts data of any input size to a fixed-length string called a hash value, message digest, or fingerprint
- An advanced version of a simple checksum
- Birthday paradox, avalanche effect
- Used in authentication, data integrity, non-repudiation, fingerprinting, password storage, database indexing
- Must be collision resistant (no MD5)

COMMON HASH FUNCTIONS

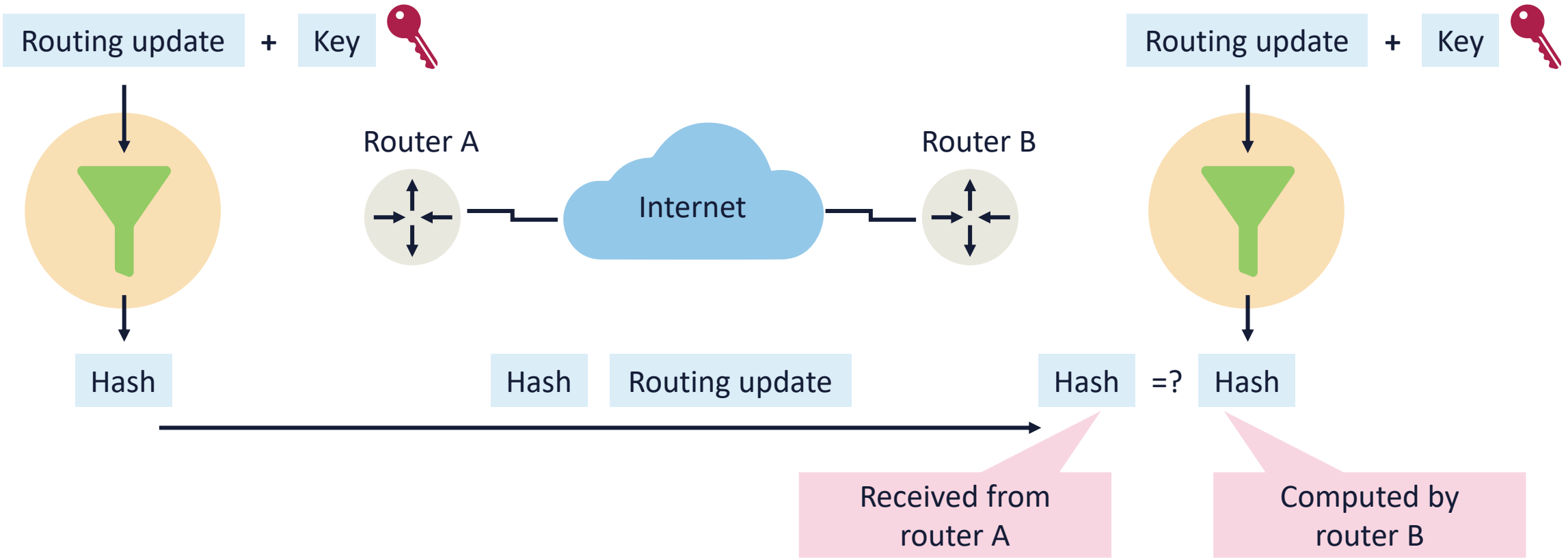


SALTING

- Salting is the technique of adding pseudorandom data to a cryptographic hash function
- The goal is to make it less deterministic for cracking tools
  - When an attacker can access a database of password hashes, they can use either hash tables or rainbow tables to look up matching hashes, which they can use to discover the passwords or other hashed data
- Two weaknesses are salts that are too short or if they aren't unique for each password



HASH-BASED MESSAGE AUTHENTICATION CODES (HMACS) FOR INTEGRITY AND ORIGIN AUTHENTICATION



KEY EXCHANGE

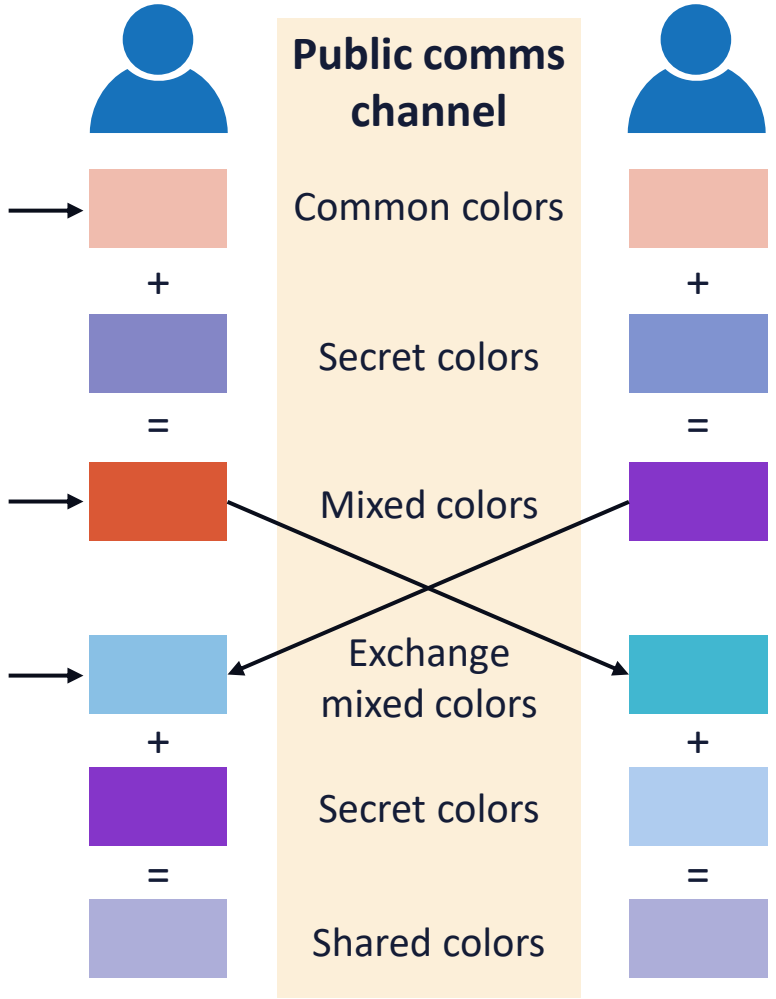
- There are several ways for parties to exchange keys:
  - Phone or text
  - Secured email
  - Couriers
  - Diplomatic bags
- Alternatively, a more effective method is using an asymmetric key exchange algorithm, such as:
  - RSA key exchange
  - Diffie-Hellman key exchange
  - Elliptic Curve Diffie-Hellman
  - Elliptic Curve Diffie-Hellman Ephemeral

DIFFIE-HELMAN KEY EXCHANGE

- Diffie-Hellman key exchange (DHKE) and RSA key transport are original protocols created for establishing secret keys between two parties over an unsecure channel
- Diffie-Helman is a widely used asymmetric cryptosystem found in SSH2, TLS, and IPsec
- It represents an impressive application of the discrete logarithm problem
- The RSA algorithm can sign public-key certificates, whereas the Diffie-Hellman key exchange cannot

BASIC CONCEPT OF DHKE

Note: Attacker only sees these colors and thus cannot arrive at the shared secret

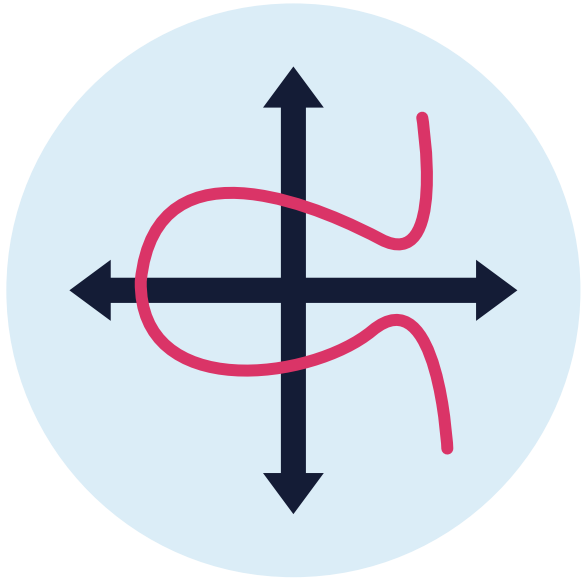


Note: Assume colors are hard to unmix, which means the secret colors are secure

DIFFIE-HELMAN MODES

- DH (Diffie-Hellman)
  - The same shared secret is used all the time between parties
- DHE/EDH (Ephemeral Diffie-Hellman)
  - A different shared secret is used each time between parties
- ECDH (Elliptic Curve Diffie-Hellman)
  - Uses EC public/private key pair
  - The same shared secret is used all the time between parties
- **ECDHE/ECEDH (Elliptic Curve Ephemeral Diffie-Hellman)**
  - Uses EC public/private key pair
  - A different shared secret is used each time

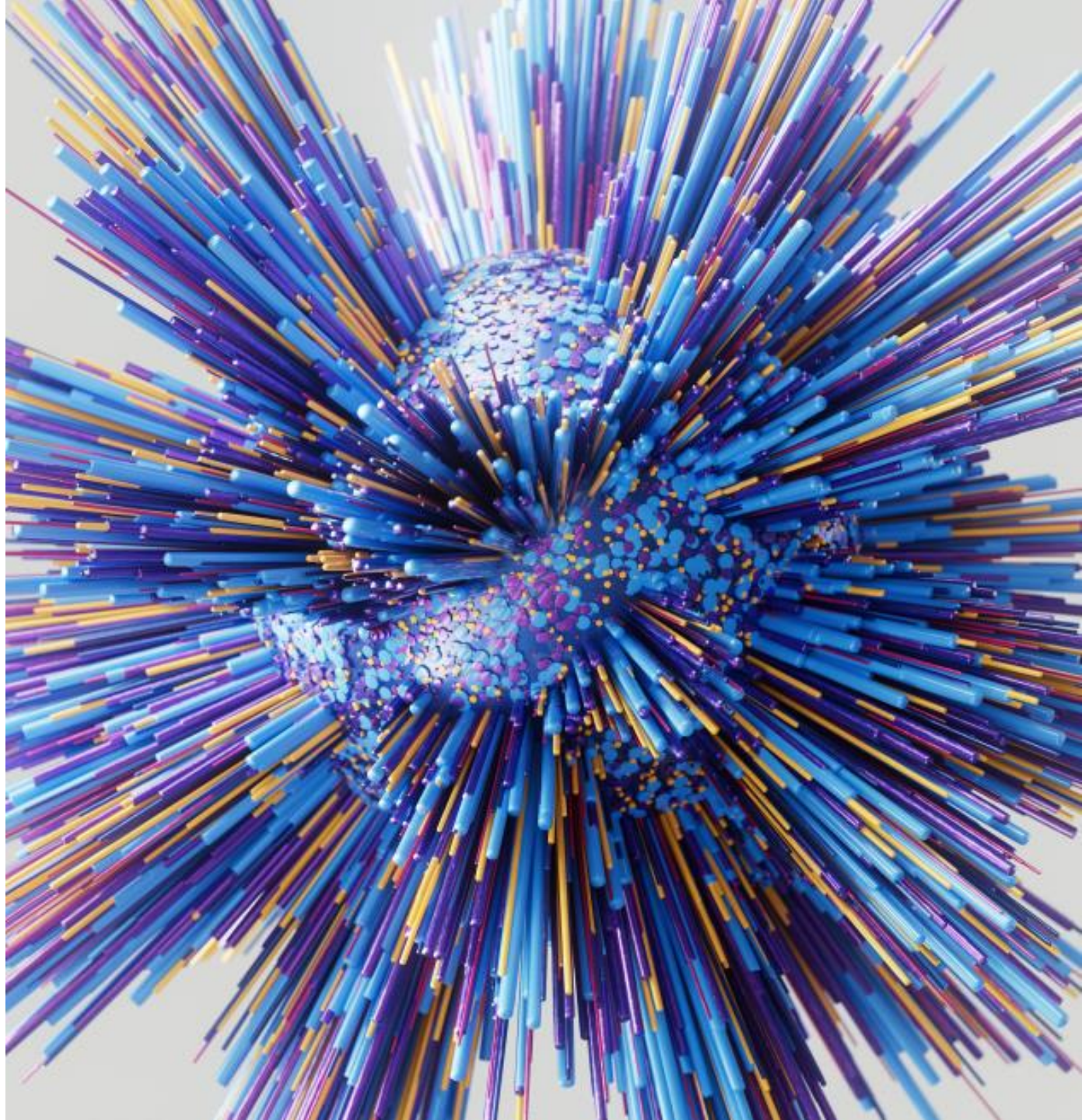
ECDHE/ECEDH (ELLIPTIC CURVE DIFFIE-HELLMAN EPHEMERAL)



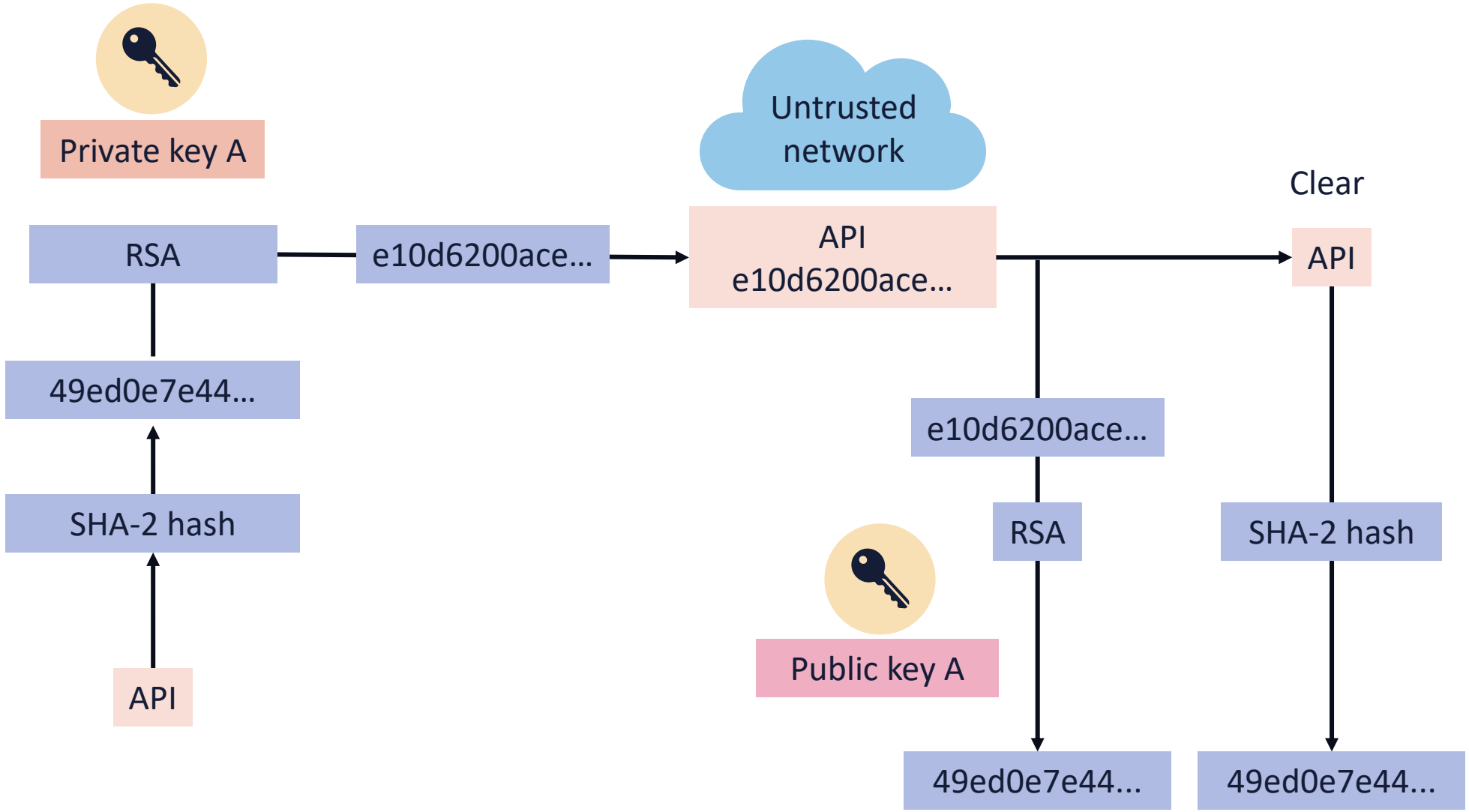
- Based on rich math functions of values plotted on an elliptic curve
- Uses smaller keyspaces while offering superior strength
- 256-bit elliptic key = 3072-bit standard key
- Excellent for mobile devices and IoT with limited memory and processing power
- Common use cases:
  - Key exchange
  - IPsec and TLS
  - Digital signatures

DIGITAL SIGNATURES

- These are a scalable mechanism for providing authenticity, integrity, and non-repudiation using random public/private key pairs
  - Does not offer confidentiality
- Digital signatures are legally equivalent to a handwritten signature in many countries
- SHA1/2/3 hash algorithms are commonly used
- Signing algorithms:
  - Rivest-Shamir-Adelman (RSA)
  - Digital Signature Algorithm (DSA)
  - Elliptic Curve Digital Signature Algorithm (ECDSA)



DIGITALLY SIGNING AN API CALL



DIGITAL CERTIFICATES

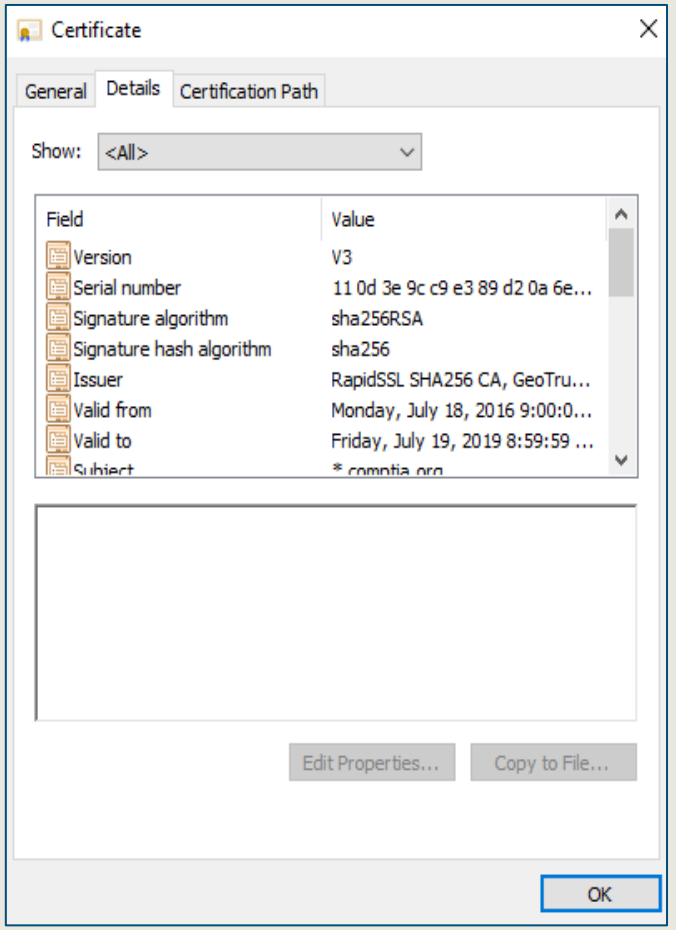
- A digital certificate is a form of file used to bind cryptographic key pairs to entities such as individuals, websites, devices, or organizations
- If validity affirmation and/or public trust is needed, then a trusted certificate authority (CA) will assume the role of a third party to validate, identify, and associate them with cryptographic pairs using the digital certificates

DIGITAL CERTIFICATES

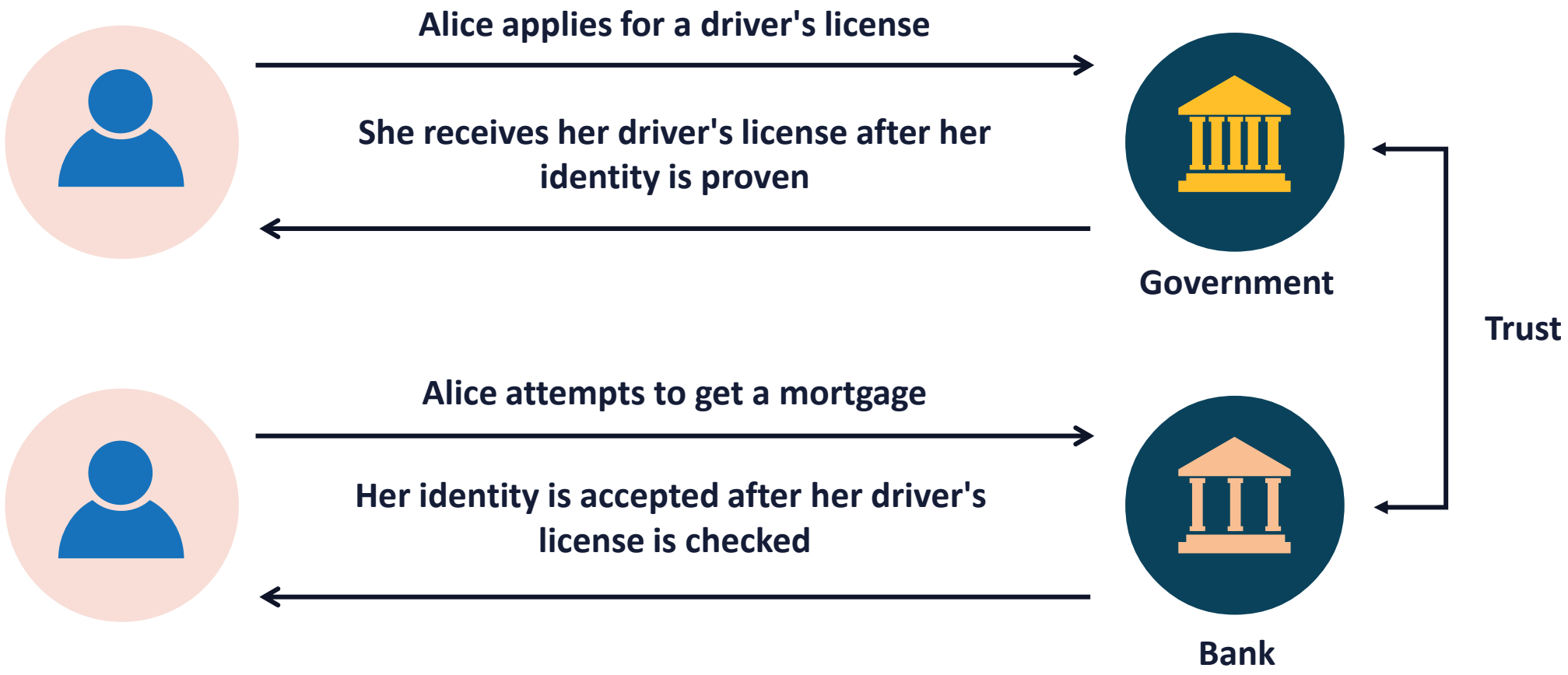
- The key pair consists of a public key and a private key
- The public key is included in the certificate, while the private key is stored in a secure fashion
- The owner of the private key can then use it to sign documents, and the public key can be used to verify the validity of those signatures
- A common format for digital certificates is based on the X.509 standard

X.509V3 DIGITAL CERTIFICATES

- Version number
- Serial number
- Signature algorithm ID
- Issuer name
- Validity period
- Not before
- Not after
- Subject name*
- Subject alternative name (SAN)
- Subject public key info
- Public key algorithm
- Subject public key
- Issuer unique identifier
- Subject unique identifier
- Extensions
- Certificate signature algorithm
- Certificate signature

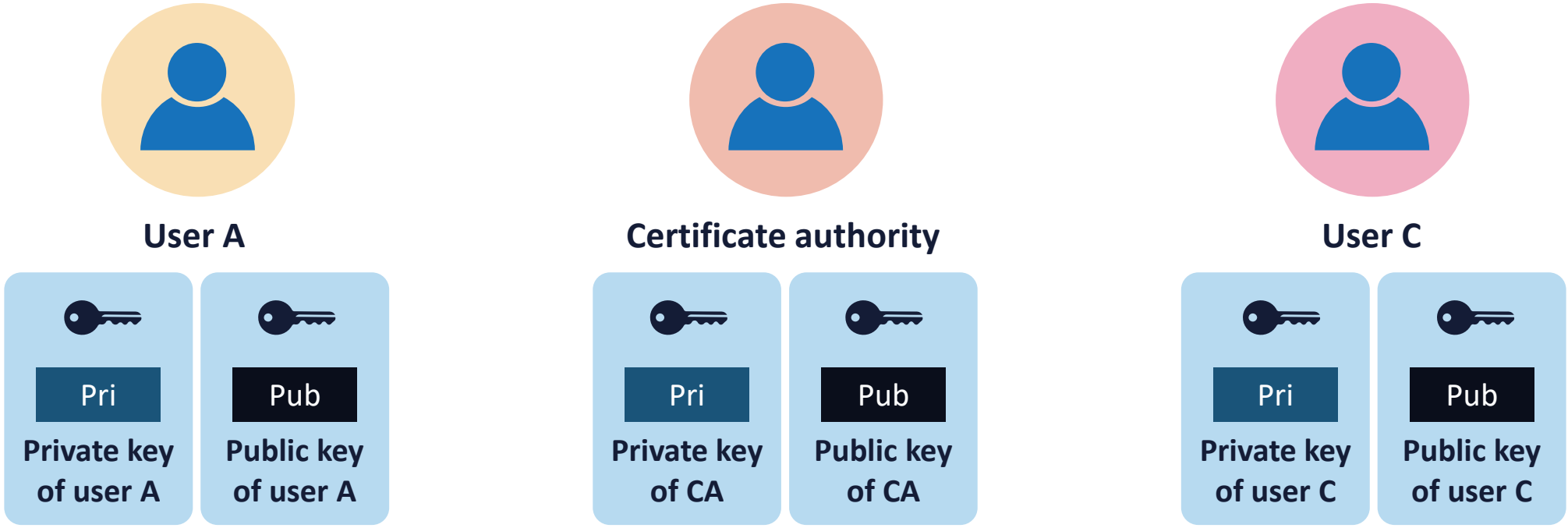


TRUSTED THIRD PARTIES



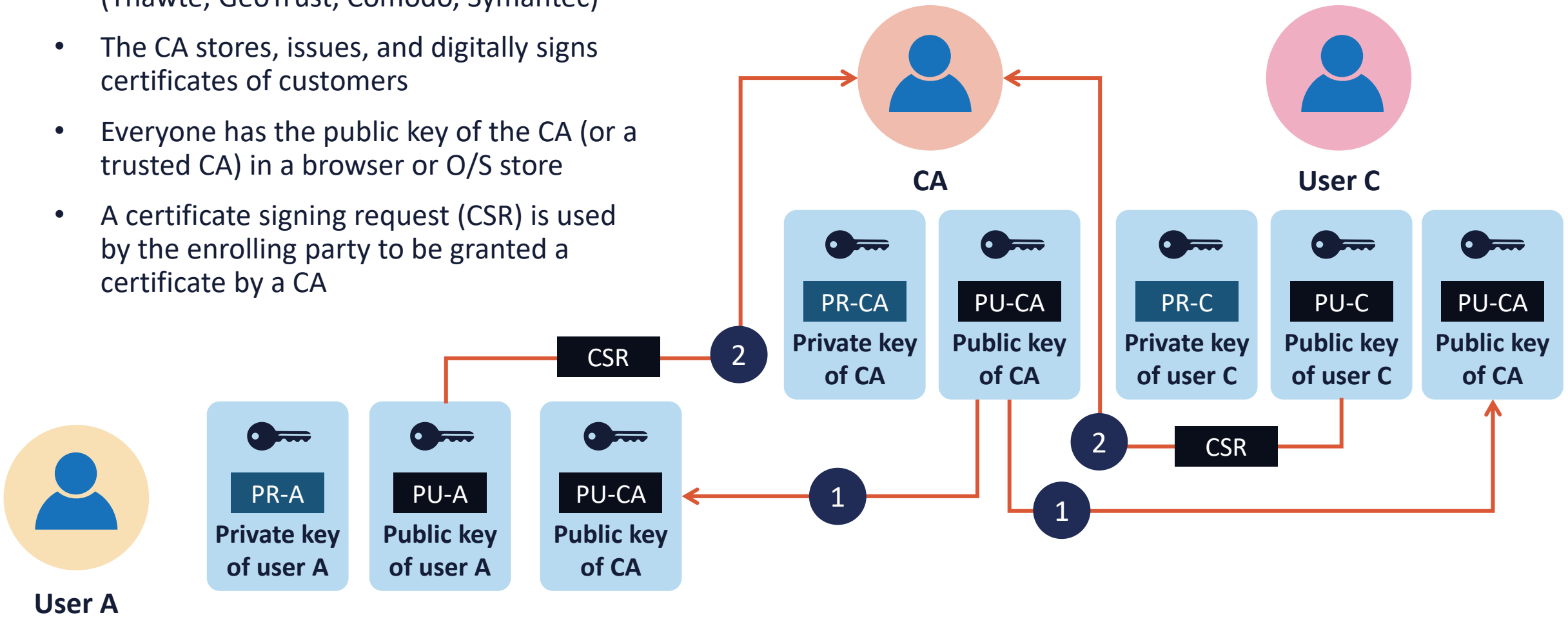
PUBLIC KEY INFRASTRUCTURE (PKI)

- PKI is a scalable binding of a public key with an entity identity
  - A person, system, or organization
- Digital certificates are registered and issued by a certificate authority (CA)
  - Can be automated or manual
- The CA may also generate the key pair (usually RSA) for the requesting party



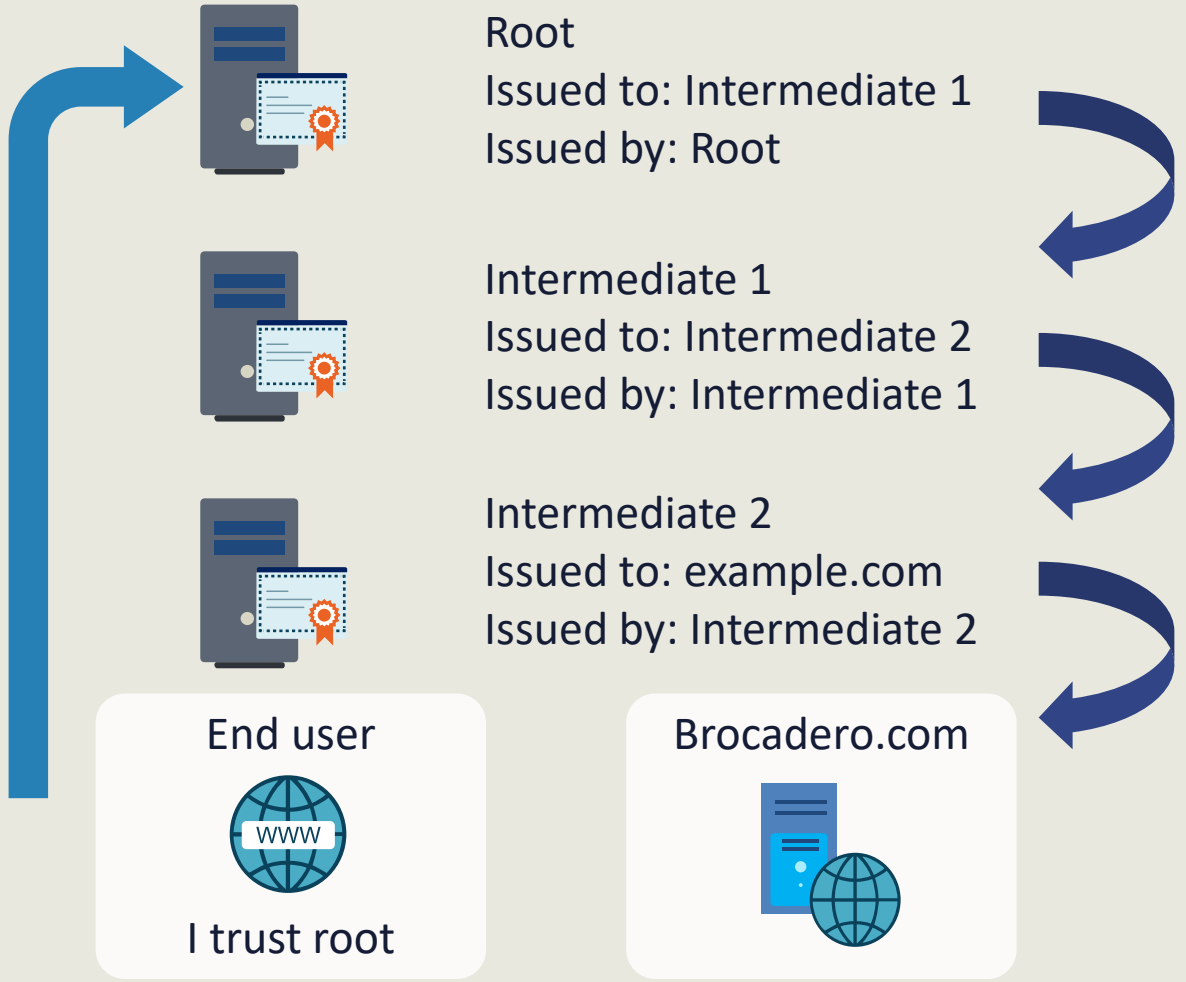
PUBLIC KEY INFRASTRUCTURE (PKI)

- The CA is the central trusted introducer (Thawte, GeoTrust, Comodo, Symantec)
- The CA stores, issues, and digitally signs certificates of customers
- Everyone has the public key of the CA (or a trusted CA) in a browser or O/S store
- A certificate signing request (CSR) is used by the enrolling party to be granted a certificate by a CA



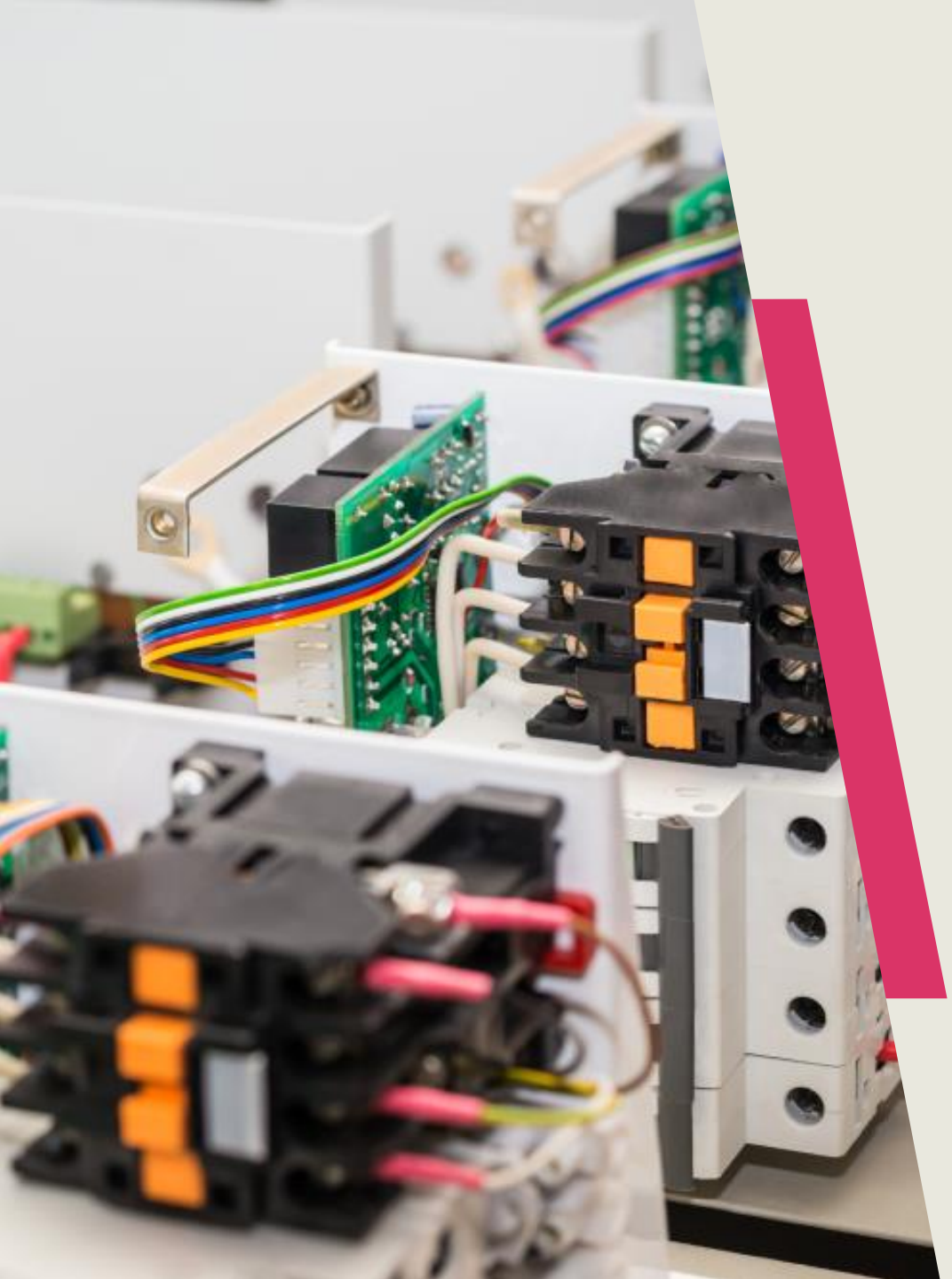
CA TRUST MODELS

- Single CA:
  - Responsible for directly providing certificates to everyone (enterprise PKI)
  - Must always be online
- Hierarchical CA:
  - Combination of root CA and intermediate CAs
  - Root sends certificates to intermediates
  - Intermediate CAs provide certificates and the "chain" to users or other intermediate CAs
  - Root can be online or offline
- Online – connected to the network and issues certificates over the network
- Offline – not connected to the network and issues certificates on removable media



CERTIFICATE REVOCATION AND SUSPENSION

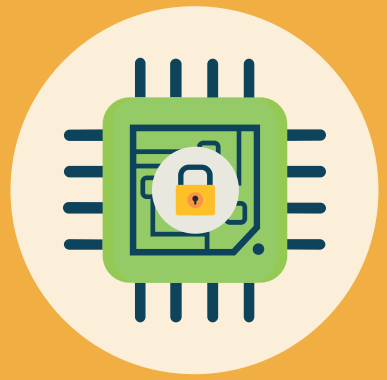
- Certificates are stamped with non-deterministic serial numbers and validity dates
- For security reasons, all keys must have a finite life due to brute-force attacks
- Certificate can be
  - Revoked (permanent) – never used again
  - Suspended/held (temporary) – can be reactivated
- The certificate revocation list (CRL) is the original method for revoking certificates
- Online Certificate Status Protocol (OCSP) is an Internet-enabled transactional database that CA's and web servers utilize for suspension and revocation



TRUSTED PLATFORM MODULES (TPM)

- A TPM is used to improve the security of various systems, such as servers and PCs
- Microsoft uses services like BitLocker Drive Encryption, Windows Hello, and others to securely create and store cryptographic keys
- It is often a separate chip on the motherboard (TPM 2.0) that allows manufacturers to build the capability into their chipsets rather than requiring a separate chip
- Google employees store X.509v3 certificates in TPMs in devices as part of zero trust

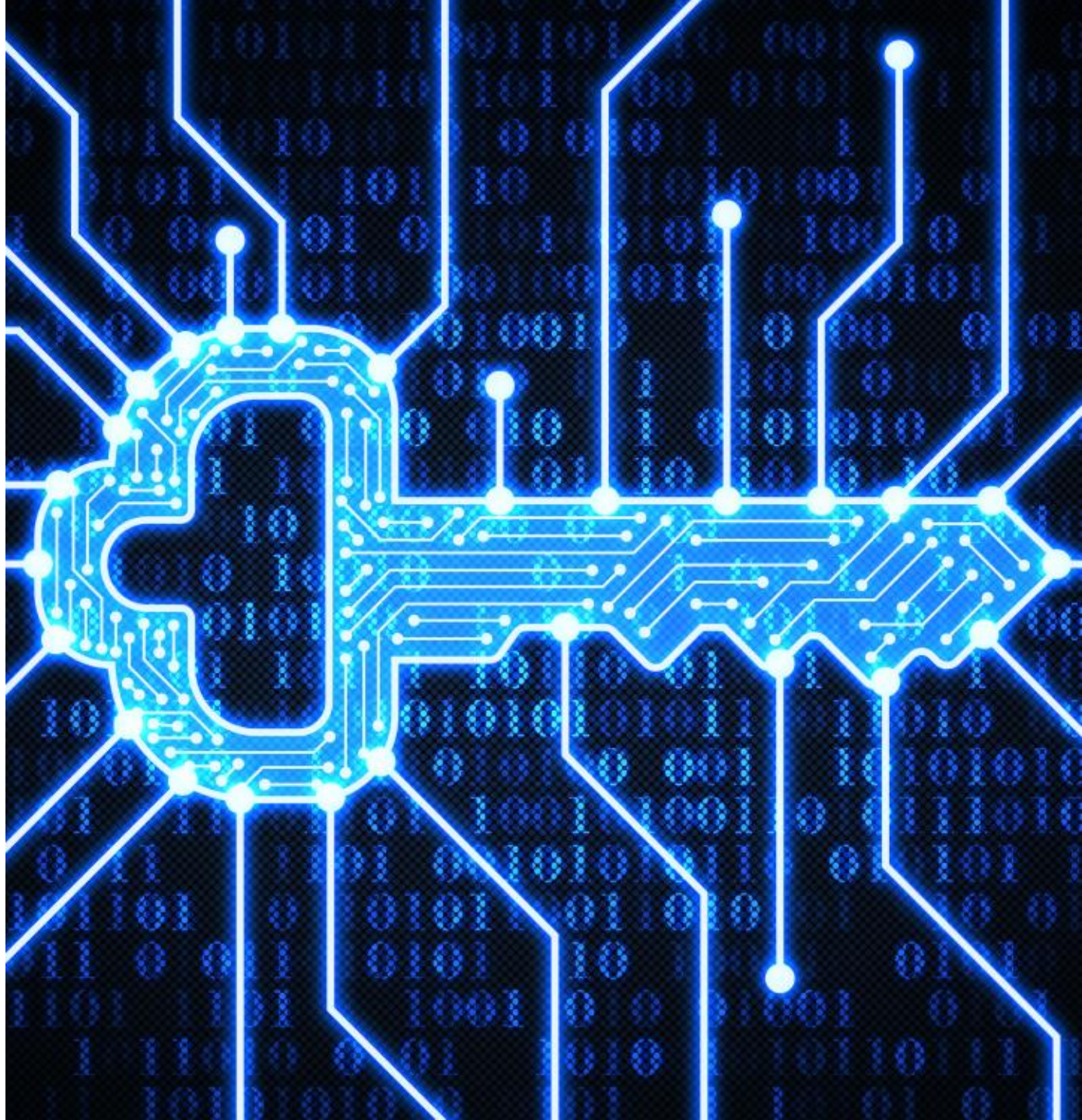
HARDWARE SECURITY MODULES (HSMs)



- These are hardened, tamper-resistant dedicated appliances or integrated modules in a PC/server
  - HSMs can be physical or virtualized
- A SmartCard-HSM is a lightweight hardware security module in a smart card, MicroSD, or USB form factor providing a remotely manageable secure RSA and ECC keys
- Responsibilities include:
  - Managing, processing, generating, and storing keys
  - Verifying digital certificates
  - SSL connection accelerator
  - Encrypting sensitive data
  - Verifying the integrity of stored data

KEY MANAGEMENT SERVICES

- A cloud-based key management service (such as AWS KMS) is a managed service that enables the creation and control of customer-managed symmetric and asymmetric cryptographic keys to protect various types of data at rest
- These key services integrate with many other cloud services, such as block storage, object (blob) storage, applications, and databases to facilitate the encryption of critical data

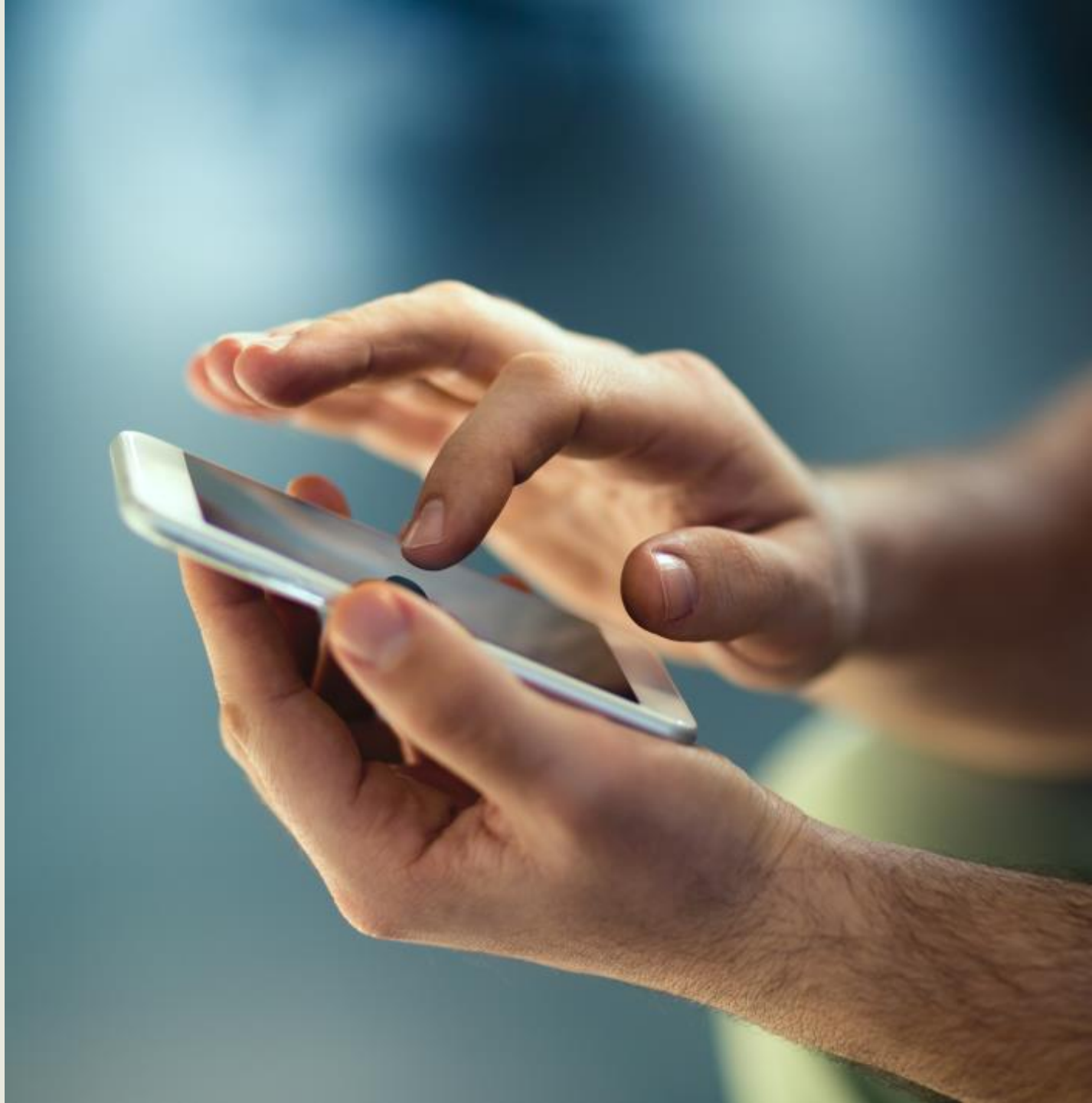


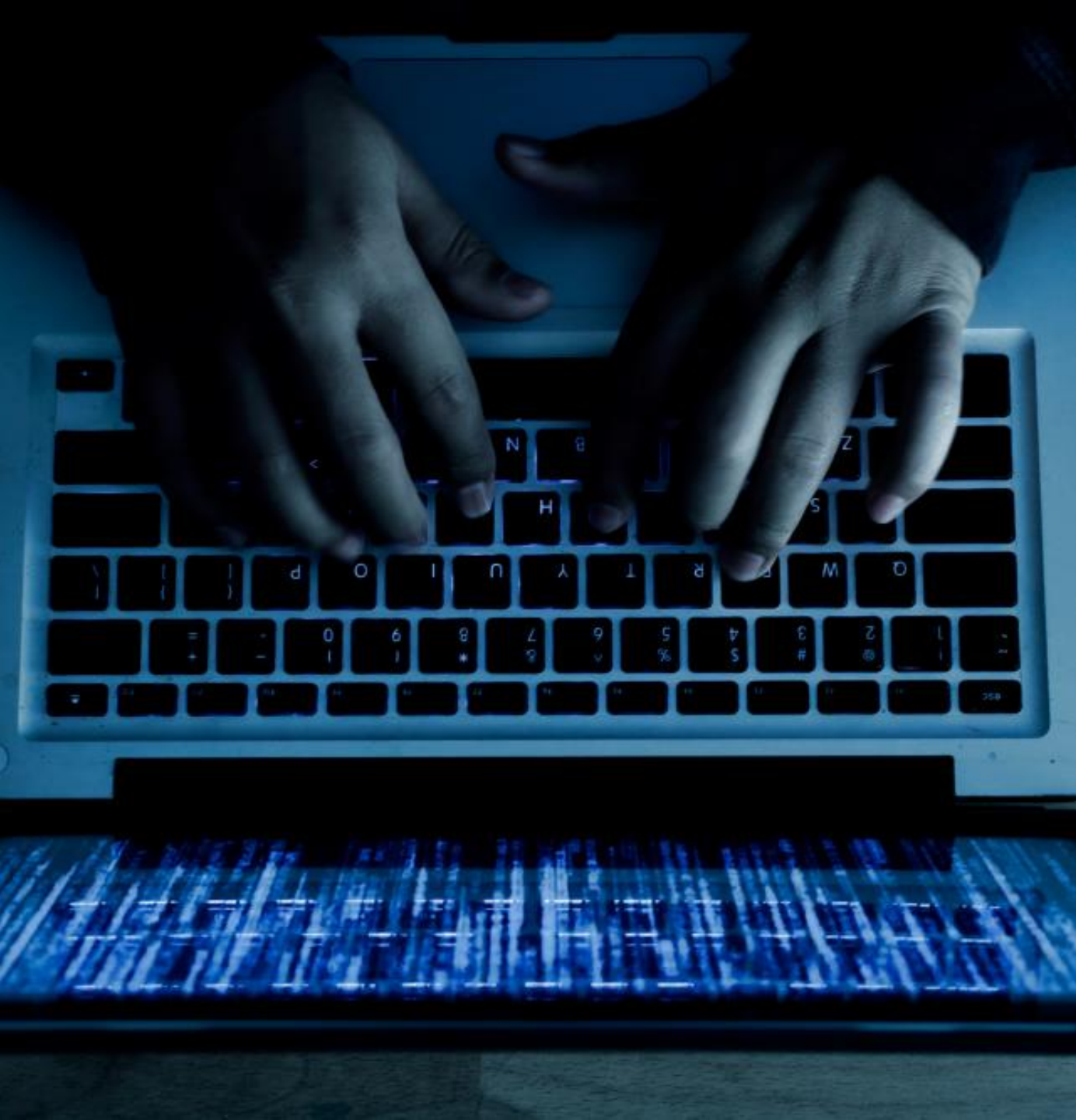
KEY STRETCHING

- Tools such as PBKDF2 apply a pseudorandom function, such as an HMAC, to the input password or passphrase along with a salt value
- PBKDF2 then repeats the process many times (1000 iterations) to produce a derived key, which can then be used as a cryptographic key in further operations
- The stretching process makes password cracking much more difficult
- Today, programs will use hundreds of thousands of iterations due to fast processors

SECURE ENCLAVES

- A secure enclave delivers CPU hardware-level isolation and memory encryption on a server, workstation, or mobile device by isolating application code and data from anyone with privileges and encrypting its memory
- With additional software, Secure Enclaves enable the encryption of both storage and network data for simple full-stack security
- Secure enclave hardware support is built into all new CPUs from Intel and AMD
- The Secure Enclave is a hardware feature of most versions of iPhone, iPad, Mac, Apple TV, and Apple Watch





STEGANOGRAPHY

- Steganography is the process of hiding a secret message inside of (or even on top of) something that is not secret
- Tools like Steghide often involve embedding a secret piece of text inside of a picture or hiding a secret message or script inside of a Word, Excel, or PDF document
- It is a form of covert communication but not a form of cryptography because it doesn’t involve scrambling data or using a key
- Steganography is a practice that enables secrecy and deceit

DATA MASKING

- Masking often involves using characters like "X" to hide some or all data
- For example, only displaying the last four digits of:
  - Social Security numbers
  - Credit card numbers
  - National ID numbers
  - Bank account numbers
  - Usernames or email addresses
- Methods to obfuscate data should prevent inference, and therefore, masking is suboptimal when compared to other methods like tokenization

TOKENIZATION

- Tokenization involves sending sensitive data through an API call (or batch file) to a provider that replaces the data with non-sensitive placeholders called tokens
- The practice involves two distinct databases:
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data
- Unlike encrypted data, tokenized data is irreversible and unintelligible

TOKENIZATION EXAMPLE

Sensitive data held by government

- Substance use in families
- Treatment cost and effectiveness

- Arrest and parole information
- Geographical crime data

Non-sensitive publicly available data

- Aggregated treatments data
- Aggregated prescriptions data

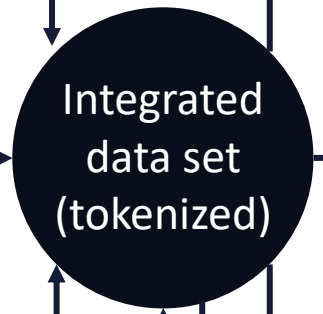
- Marketing data
- Spending and insurance information

Child welfare agencies

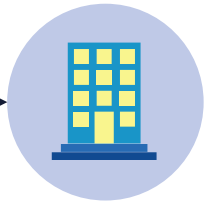
Law enforcement

Hospitals

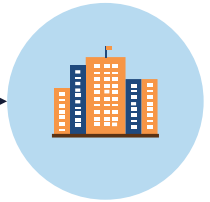
Third-party data



Enriched individualized insights



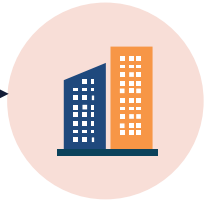
Child welfare agencies



Corrections department

Enriched aggregated insights

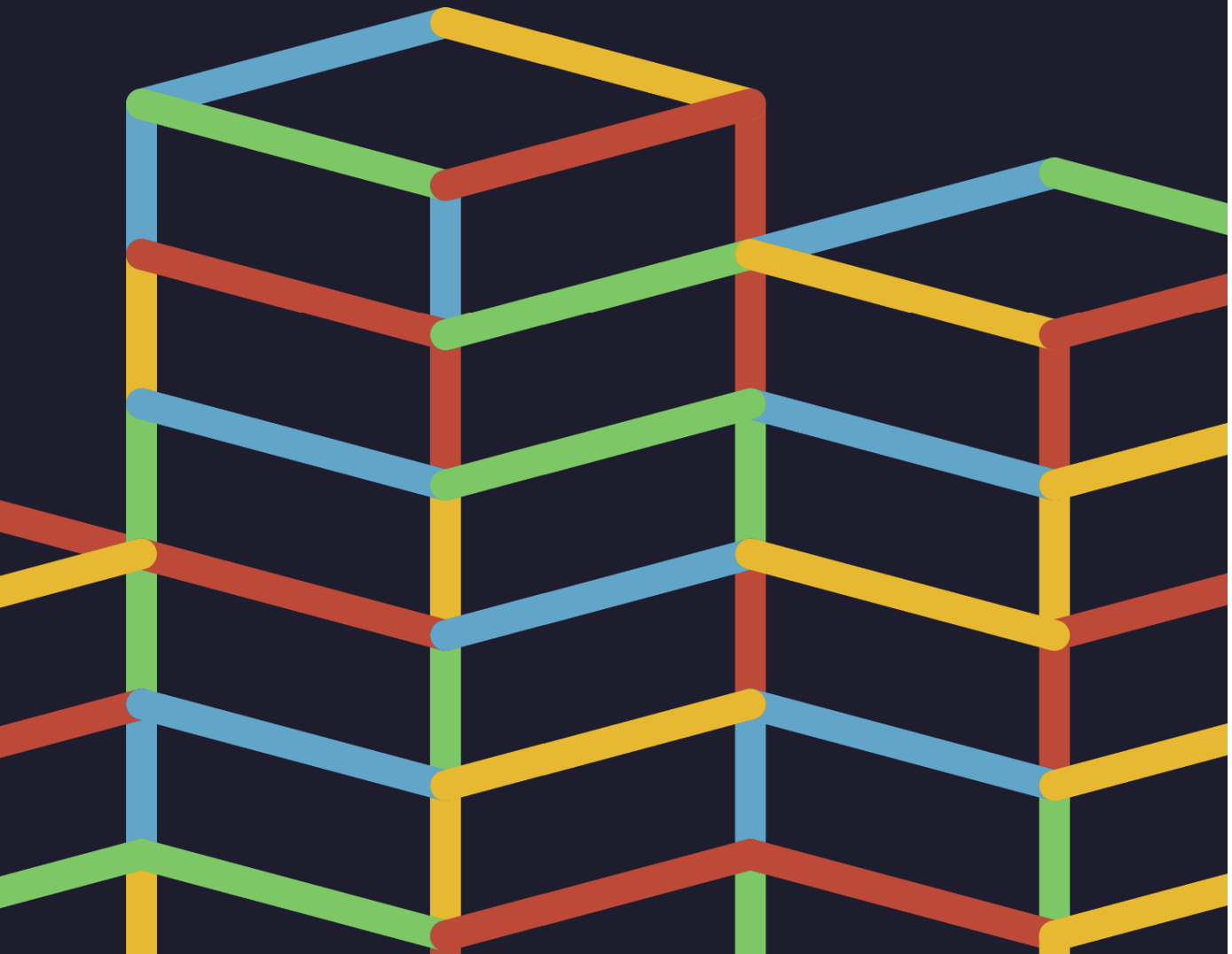
Hospitals



Third-party data

BLOCKCHAIN TECHNOLOGY

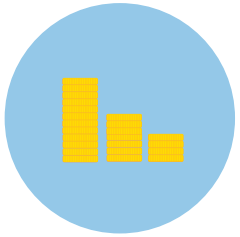
- A blockchain is a distributed database that leverages a constantly growing list of ordered records called blocks
- These blocks are linked using cryptographic mechanisms
- Each block stores a cryptographic hash of the previous block, a timestamp, and transaction data
- Blockchain may be deployed as a public ledger (or private smart contract) consisting of a digital "chain of blocks" storing information



BLOCKCHAIN TECHNOLOGY

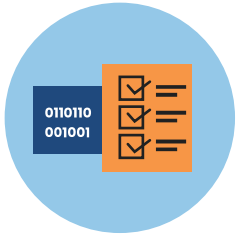
- Data can be read or written to the chain but not modified (immutability) – changes must be made to a subsequent block in the chain
- Transaction data such as date, time, and amount is verified with a consensus mechanism (proof of work [PoW], proof of stake [PoS], etc.)
- The transaction participant's identities are based on digital signatures
- Unique cryptographic hashes are used to distinguish the blocks from each other

BLOCKCHAIN USE CASES

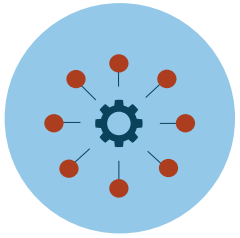


Cybercurrencies and tokens

Money and asset transfer ledgers



Smart contracts



Non-fungible tokens (NFTs)

Government services

Insurance claims (fraud prevention)

Securities (stocks, bonds)

Healthcare