Security

What and How

Password Strength

- *There are only two types of companies: Those that have been hacked and those that will be hacked.* – Robert S. Mueller III, former Director of the FBI.
- How security is your password? https://www.passwordmonster.com/

- US president's nuclear briefcase passcode.
- Marine password policy: at least 12 characters long, mix of number, special chars, change it every 3 months. Most write the passcode in a note and attach it to the device.

Security

- Privacy
- Authentication
- Authorization
- Integrity
- Non-repudiation
- Availability

Privacy

- Privacy is the right of individuals to control their personal information and to ensure that it is not disclosed to unauthorized parties.
- Information security measures, such as encryption and access controls, help to protect individual privacy and prevent data breaches.

Authentication

- Authentication is the process of verifying the identity of users, devices, or systems.
- This is achieved through various methods, including passwords, biometrics, and tokens.
- Authentication ensures that only authorized entities have access to sensitive information and systems.

Authorization

- Authorization is the process of determining what actions a user or system can perform once they have been authenticated.
- This includes access controls, such as role-based access control and mandatory access control, which ensure that users only have access to the resources and data they need to perform their tasks.

Integrity

- Integrity refers to the protection of data from unauthorized modification, deletion, or alteration.
- This is achieved through measures such as digital signatures, checksums, and data backups.

Non-repudiation

- Non-repudiation is the assurance that a sender of a message cannot deny having sent the message.
- This is achieved through digital signatures and certificates, which provide a tamper-evident record of transactions and communications.

Availability

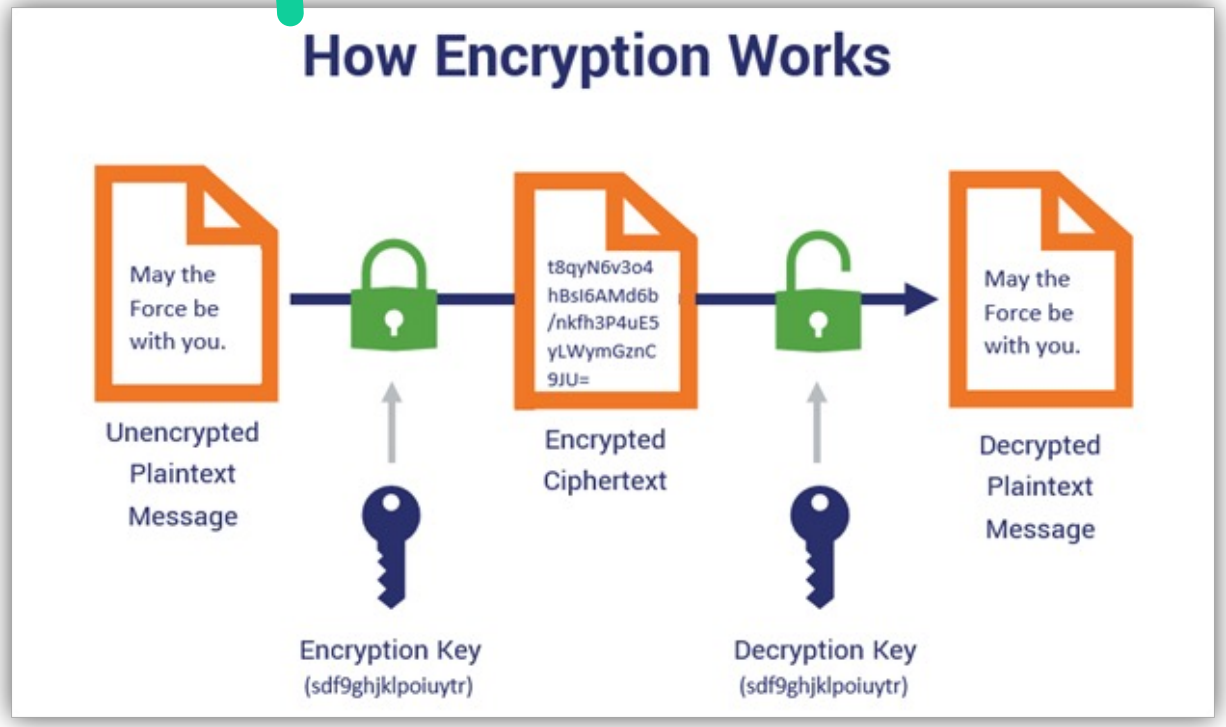
- Availability refers to the accessibility and usability of information and systems.
- This includes ensuring that systems are operational and accessible when needed, and that data is retrievable and usable.

Example: Messages Between Alice and Bob

- Privacy: Alice wants to ensure that only Bob can read the message, and no one else can access it. She uses encryption to protect the message, so even if an unauthorized party intercepts it, they won't be able to understand its contents.
- Authentication: Before sending the message, Alice verifies Bob's identity through a digital certificate or password to ensure she's sending it to the right person.
- Authorization: Alice checks Bob's access level and ensures he has the necessary clearance to receive the message.
- Integrity: Alice uses a digital signature or checksum to ensure the message isn't tampered with or altered during transmission. When Bob receives the message, he can verify its integrity using the same digital signature or checksum.
- Non-repudiation: Alice uses a digital signature that includes a timestamp and her unique identity, so Bob can verify the message came from her and when it was sent. This prevents Alice from denying she sent the message.
- Availability: Alice ensures the message is stored on a reliable server and transmitted through a secure channel, so Bob can access it when needed.

Symmetric Encryption

- Symmetric encryption is a type of cryptography that uses the same secret key for both encryption and decryption.
- This means that the key used to lock the information is the same key used to unlock it. Symmetric encryption algorithms are fast, efficient, and widely used in various applications, including secure web browsing, email encryption, and digital signatures.



Symmetric Encryption Algorithms

- Data Encryption Standard (DES): introduced in 1976, DES was the first widely adopted symmetric encryption algorithm. DES uses a 56-bit key and operates on 64-bit blocks. Its short key length and vulnerability to brute-force attacks led to its eventual deprecation.
- Triple Data Encryption Algorithm (Triple DES): introduced in the late 1990s, aimed to address DES's security concerns. It uses three separate 56-bit keys, effectively increasing the key length to 168 bits.
- Advanced Encryption Standard (AES): introduced in 2001, revolutionized symmetric encryption. AES uses a variable key length (128, 192, or 256 bits) and operates on 128-bit blocks.

Symmetric Encryption Drawbacks

- Key distribution: A major challenge with symmetric encryption is securely distributing the secret key to all parties involved. If the key is intercepted during transmission, the security of the encrypted data is compromised.
- Key Management: Managing the keys becomes increasingly complex as the number of users grows. Each pair of users needs a unique key, leading to many keys that must be securely stored and managed.
- Lack of Non-repudiation: Symmetric encryption does not provide non-repudiation. Since the same key is used for both encryption and decryption, it is impossible to prove which party encrypted the message, making it unsuitable for scenarios where proof of origin is required.

Key Sharing Among 10 People

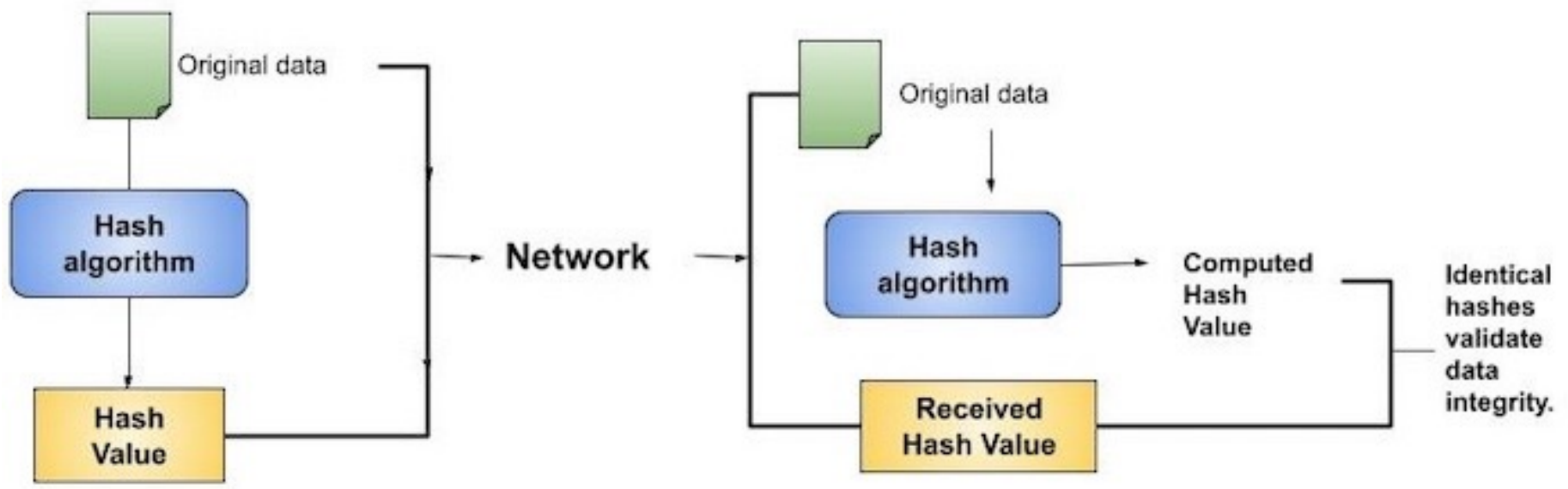
- Meet in person: This would require each person to meet with every other person individually, resulting in 45 separate meetings (10 people x 9 others = 90, but since each meeting involves two people, we divide by 2).
- Share via email or messaging: This would require each person to send the key to every other person, resulting in 90 separate key transmissions (10 people x 9 others = 90). However, this method is insecure since the keys could be intercepted or compromised during transmission.
- Use a central key server: This would require each person to trust the key server and connect to it to retrieve the shared key. However, this creates a single point of failure and a potential target for attacks.

Mission Impossible

- As the number of users increases, the complexity of sharing symmetric keys grows exponentially. In a larger group, managing and securing the key exchange process becomes impractical.
- For example, with 100 users, each person would need to share the key with 99 others, resulting in 4,950 separate key exchanges (100 people x 99 others = 9,900, but since each exchange involves two people, we divide by 2).
- In Internet that has millions of businesses and billions of users, sharing symmetric key is an impossible mission.

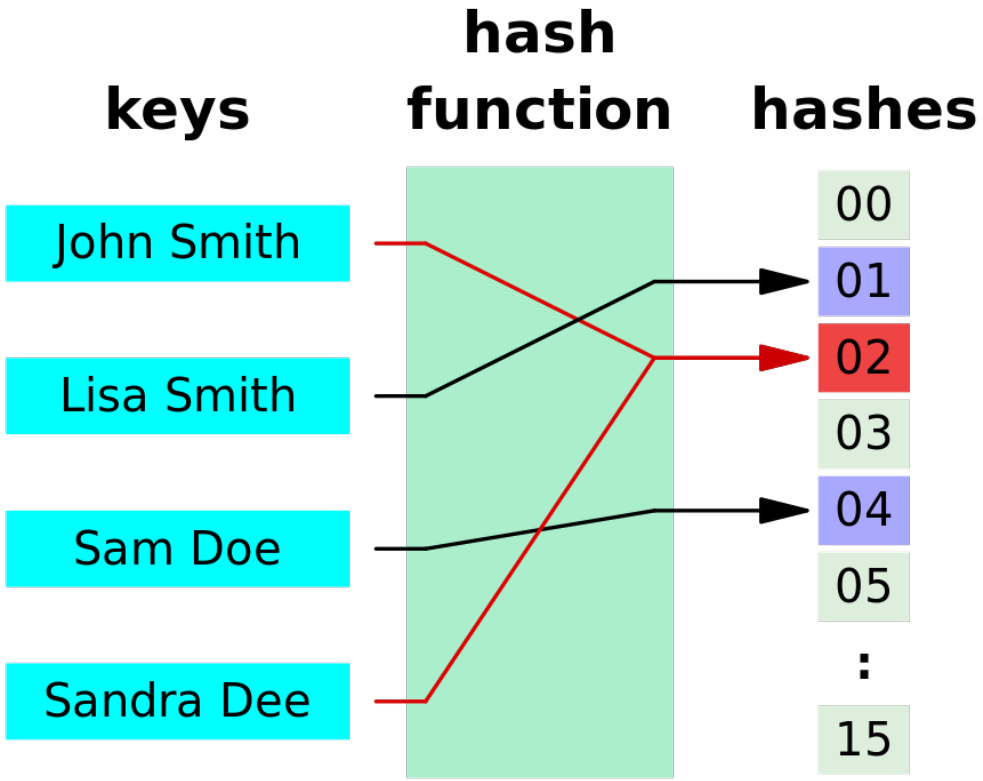
Hashing Algorithm

- A hashing algorithm is a mathematical function that takes input data of any size and generates a fixed-size output, known as a hash value or digest.
- The key characteristic of a hashing function is that it is a one-way function, meaning it is:
  - Deterministic: Given the same input, it always produces the same output.
  - Non-invertible: It is computationally infeasible to reverse-engineer the original input from the output hash value.



Hashing For Data Integrity

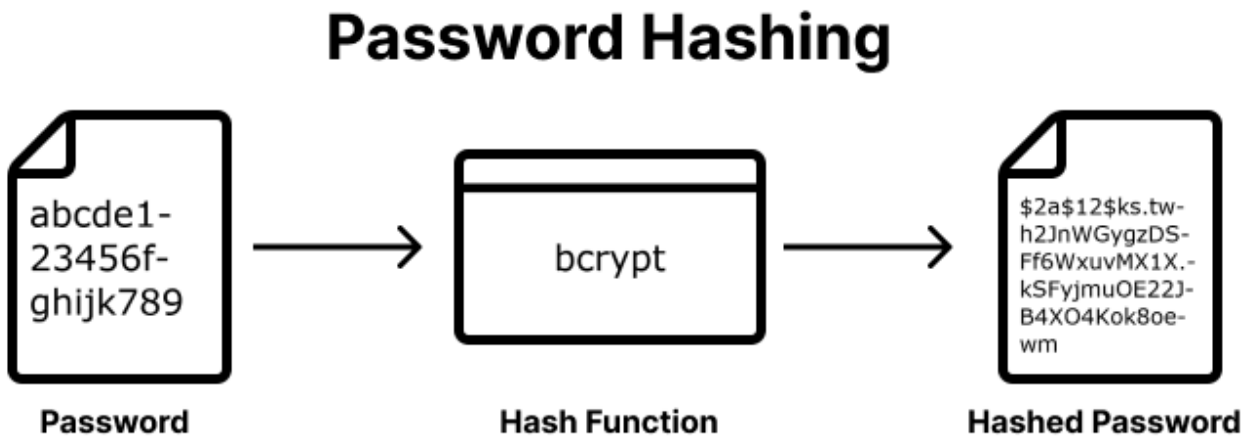
- Data Integrity: Hashing ensures that data is not tampered with or altered during transmission or storage.
- Software Download: Apache Web server: https://httpd.apache.org/download.cgi



Hashing for Data Indexing

- Data Indexing: Hashing enables efficient data indexing and retrieval, as hash values can be used to quickly identify and locate specific data records.

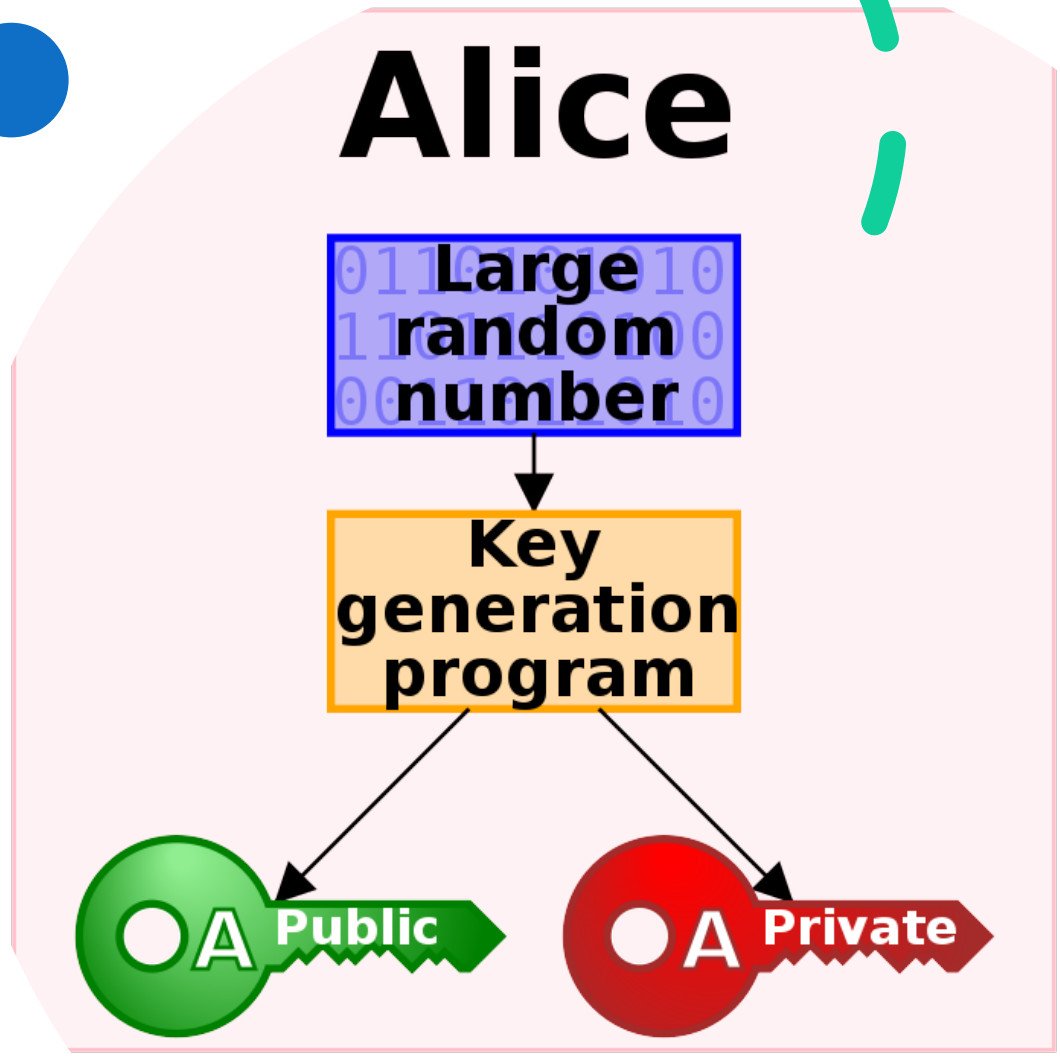
Hashing for Password Storage



- Password Storage: Hashing is used to store passwords securely, making it difficult for attackers to obtain the original password.
- When a user creates a password, a hash value is generated and stored instead of the actual password. When the user logs in, the input password is hashed and compared with the stored hash value to authenticate the user.
- This way, even if an attacker gains access to the stored hash values, they cannot obtain the original passwords.
- bcrypt in the above picture is a popular password hashing function because it allows the computational cost to be increased as computational power grows, enhancing security.

Asymmetric Encryption Concepts

- A pair of keys: a public key and a private key.
- It is generated from a large random number.



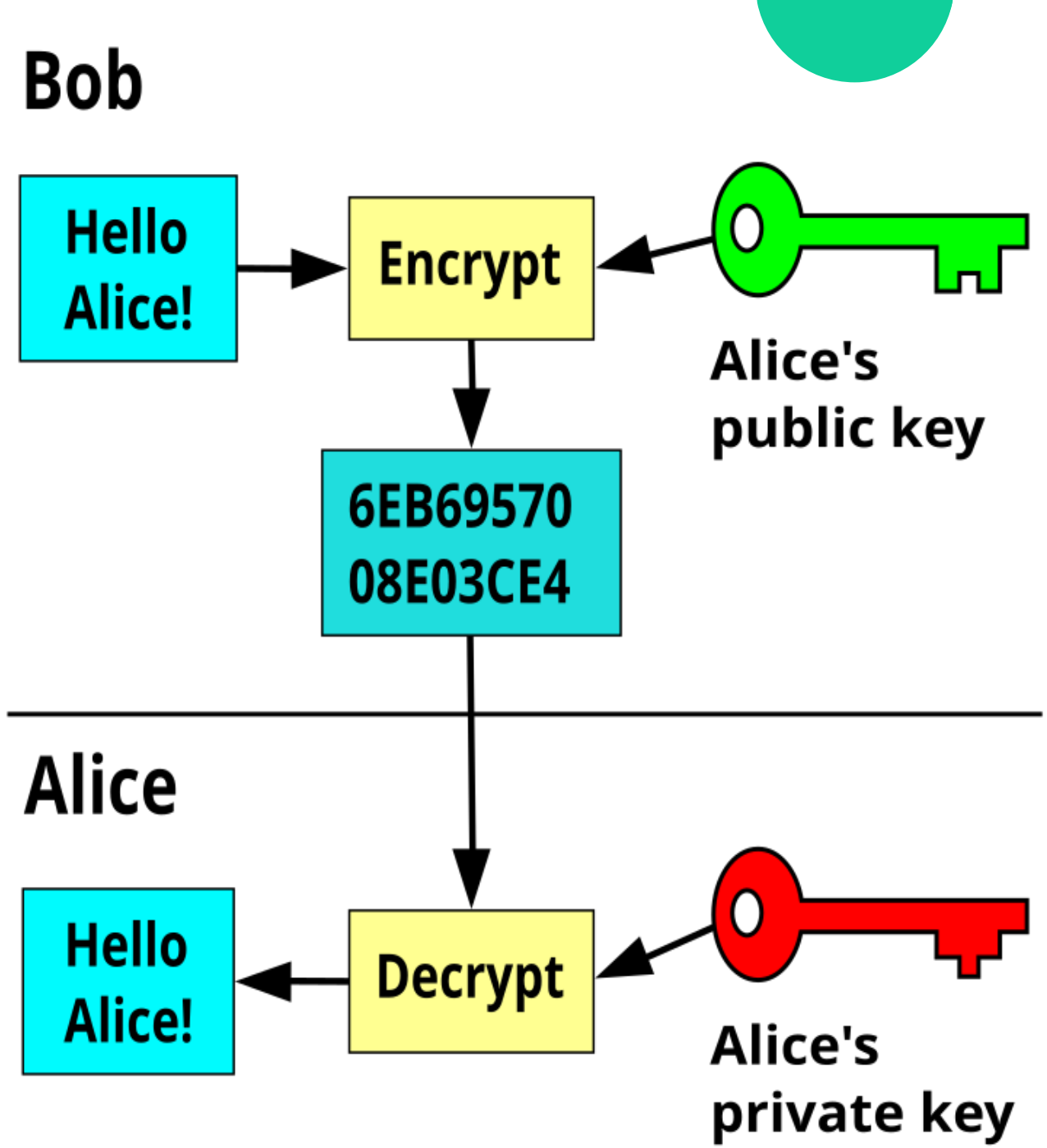
Public Key

- Publicly available
- Used for encryption
- Not sensitive, shared openly

Private Key

- Kept confidential: it is computationally impossible to find out the private key from its public key
- Used for decryption, digital signature, and key exchange
- Sensitive, not shared publicly

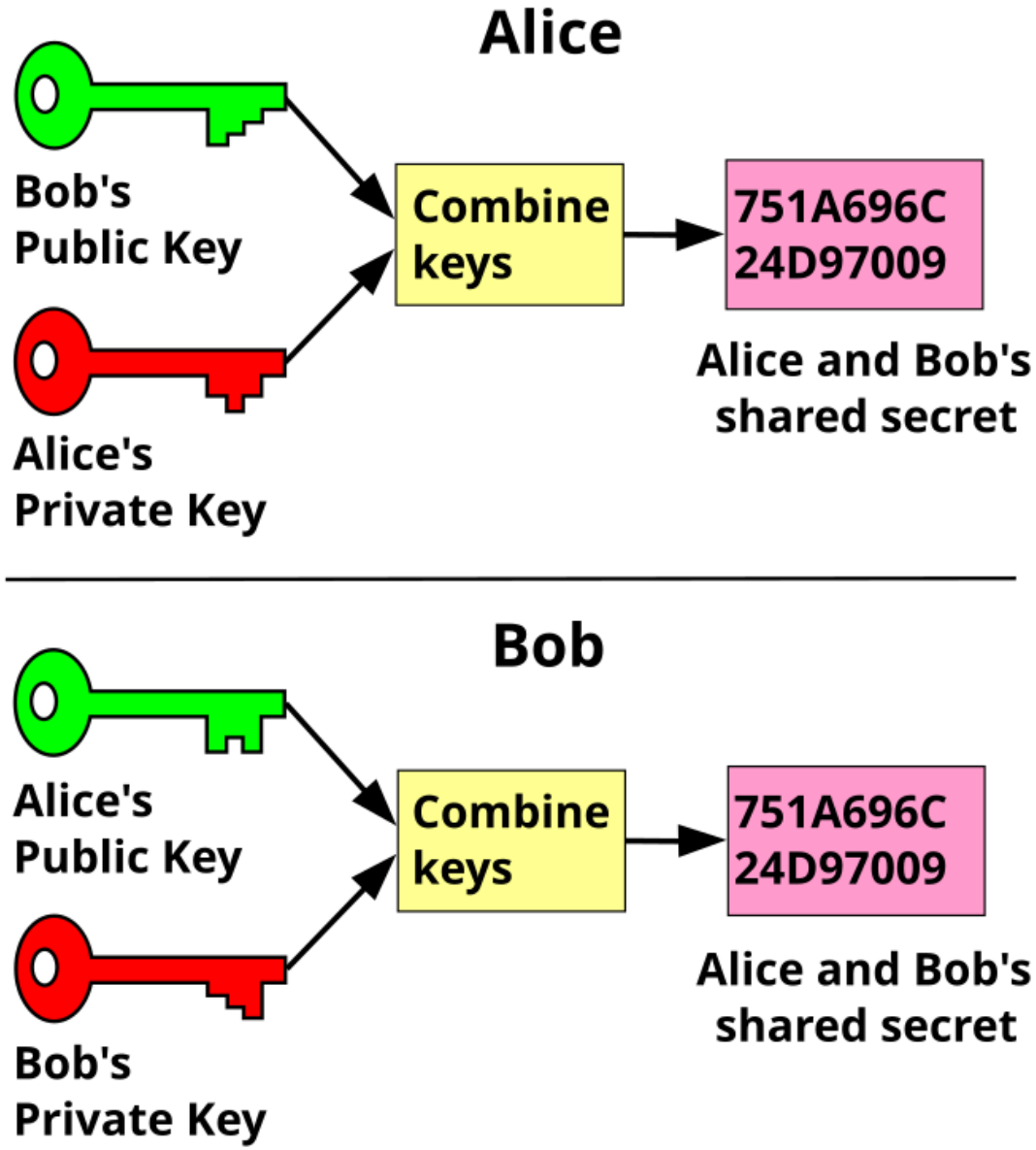
Public Key Encryption



Public Key for Authentication

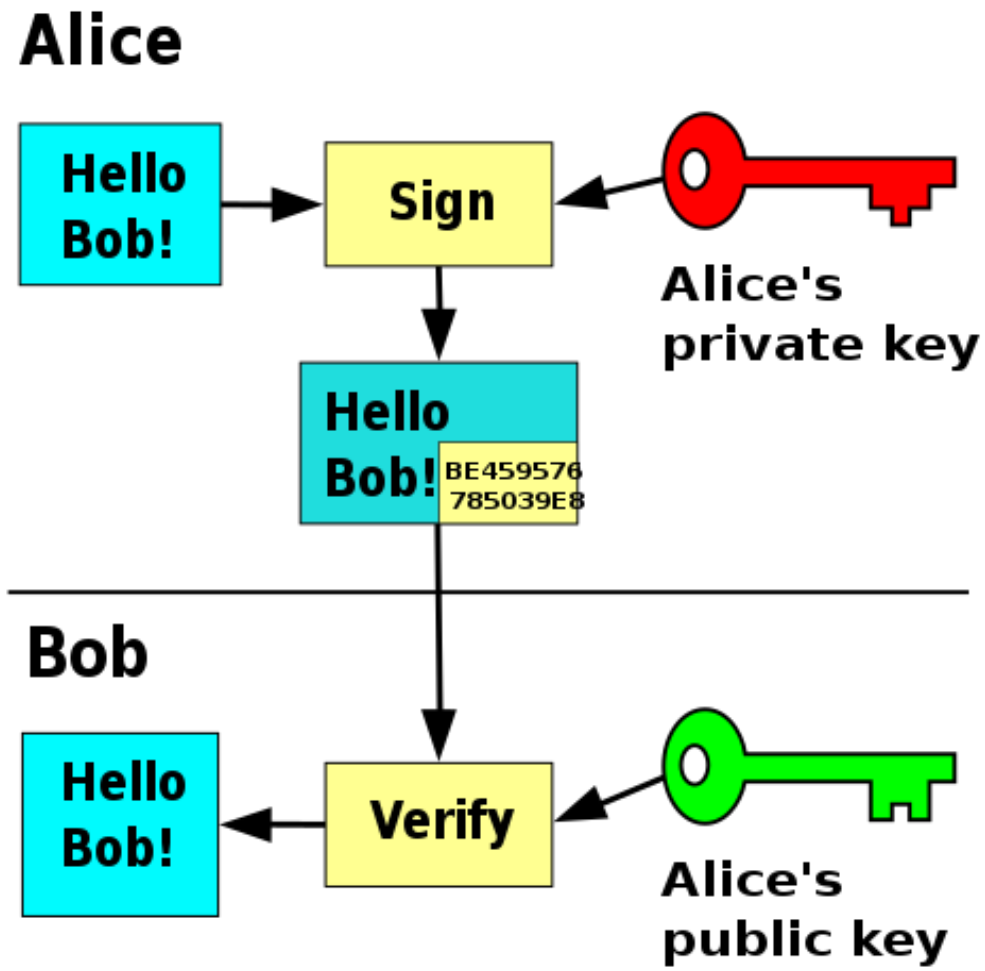
1. **Generate Key Pair:** Create a linked public and private key pair for the user.
2. **Bind Identity:** Associate the public key with the user's identity (e.g., username, email) and store this information in the service provider's database.
3. **Send Challenge:** When the user requests access, the server sends a random challenge (nonce) to the user.
4. **Sign and Verify:** The user signs the challenge with their private key and sends the signature to the server. The server verifies the signature with the public key. If valid, the user is authenticated and granted access.

Key Exchange



Key Exchange is Everywhere

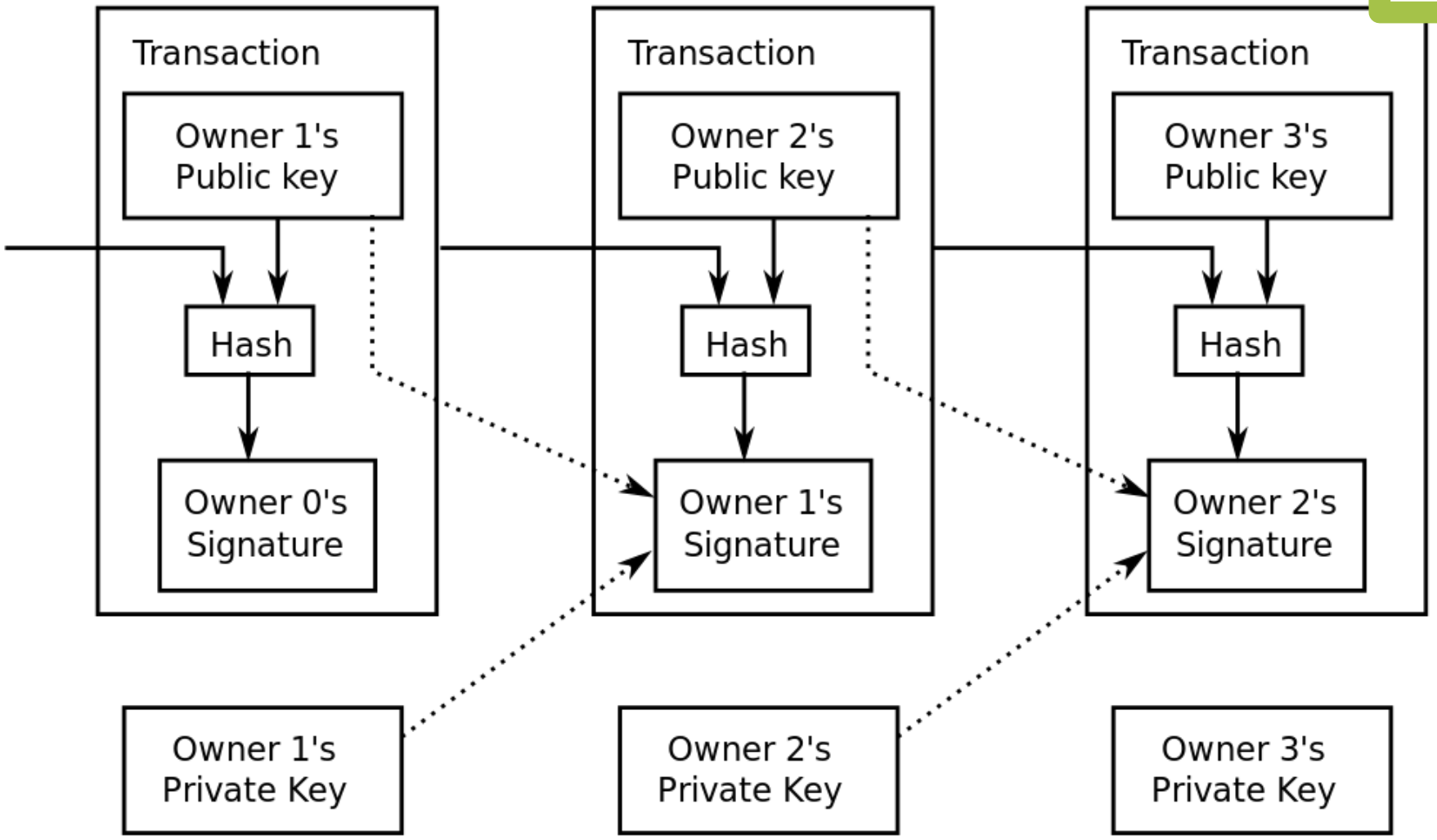
- TLS/SSL used by HTTPS
- SSL for secure login
- VPN
- WIFI
- SSH for remote secure shell



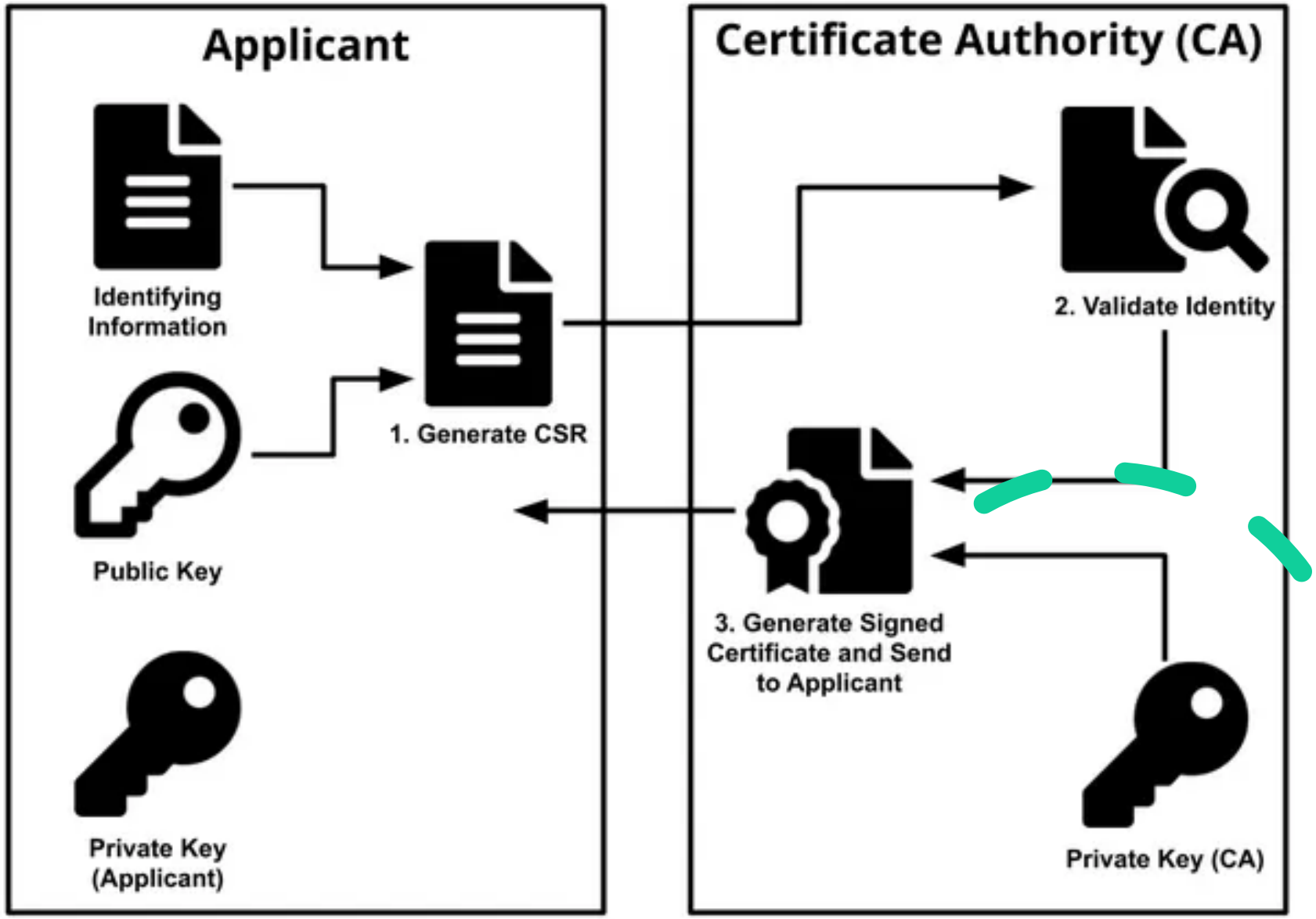
Digital Signature

- Alice encrypts the hash of the message to create a digital signature.
- The digital signature is then sent along with the original message.
- On the receiving end, Bob uses Alice's public key to decrypt the digital signature.
- Bob also hashes the received message using the same algorithm as Alice.
- He then compares the decrypted digital signature with the newly generated hash.

Bitcoin


Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key

PKI


Applicant
Certificate Authority (CA)
Identifying Information
Public Key
Private Key (Applicant)
1. Generate CSR
2. Validate Identity
3. Generate Signed Certificate and Send to Applicant
Private Key (CA)

Malware: Malicious Software

- Virus: A self-replicating program that attaches itself to a file or program on a computer.
- Worm: A self-replicating program that can travel from computer to computer without needing to be sent as an attachment.

More Forms…

- Trojan: A program that appears to be legitimate but contains malicious code.
- Spyware: A program that secretly monitors and collects personal information about a user.
- Adware: A program that displays unwanted advertisements on a computer, often in the form of pop-ups or banners.
- Ransomware: A program that encrypts a user's files and demands payment in exchange for the decryption key.
- …

How Can Malware Break Into?

- Vulnerable System: Security bugs vulnerabilities in software or operating systems, or outdate systems allowing malware to gain access.
- Download and Install Infected Software: Downloading software from untrusted sources, which may bundle malware.
- Social Engineering (Phishing): Tricking users into revealing login credentials or installing malware through emails, messages, or social media.
- Weak Passwords: Using easily guessable passwords, allowing hackers to gain access.

Antivirus? No for Me

- It cannot prevent malware from infecting your system because it cannot detect any **NEW** malware (virus or worms)
- And it comes with the cost of anti virus software to provide real time protection. Two big costs are
  - Subscription fee
  - Resource utilization: 20% performance lose

How to Protect

- Keep your system and software up-to-date - simply turn on auto system updates.
- Don't download software from untrusted sources. Be cautious with emails and messages, and avoid suspicious links or attachments.
- Use strong, unique passwords and enable two-factor authentication.
- Don't leak your password to untrusted ones.
- Have multiple data copies.

DOS and DDOS

- A DOS (Denial of Service) attack is a type of cyberattack where an attacker attempts to make a computer or network resource unavailable by flooding it with traffic or exploiting a vulnerability.
- A DDOS (Distributed Denial of Service) attack is a type of DOS attack where the traffic or requests come from multiple sources, often compromised devices or bots.
- Protection
  - Network infrastructure: Firewalls and Intrusion Prevention Systems (IPS)
  - Content Delivery Networks (CDNs)
  - Network monitoring
  - Auditing.

Security Policies

- Can you play video games on a company computer?
- Is your email on a company computer private?
- Computer security policies outline the rules and guidelines for employees to follow.
- It is not uncommon for companies to monitor and inspect employee computers and email accounts.