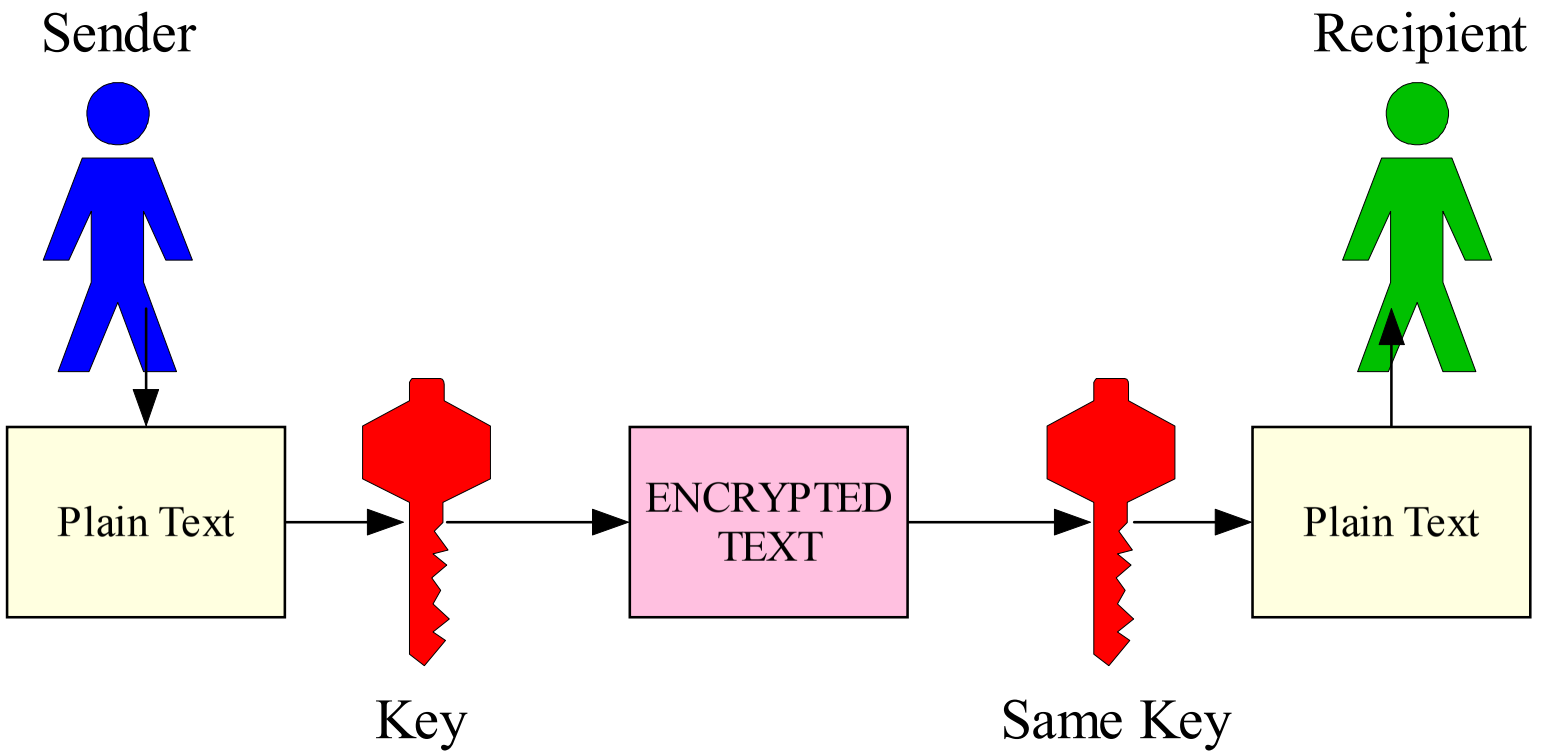
Why Security?

- eBusiness relies on services such as online purchasing, banking and trading.
- All these services consist of transactions involving the transfer of confidential data (e.g. Social Security Numbers) and authentication.
  - **Privacy** (need to maintain confidentiality).
  - **Integrity** (ensure info is not compromised or altered).
  - **Authentication** (sender/receiver proving their identities).
  - **Non-repudiation** (legally prove that a transaction was effected)

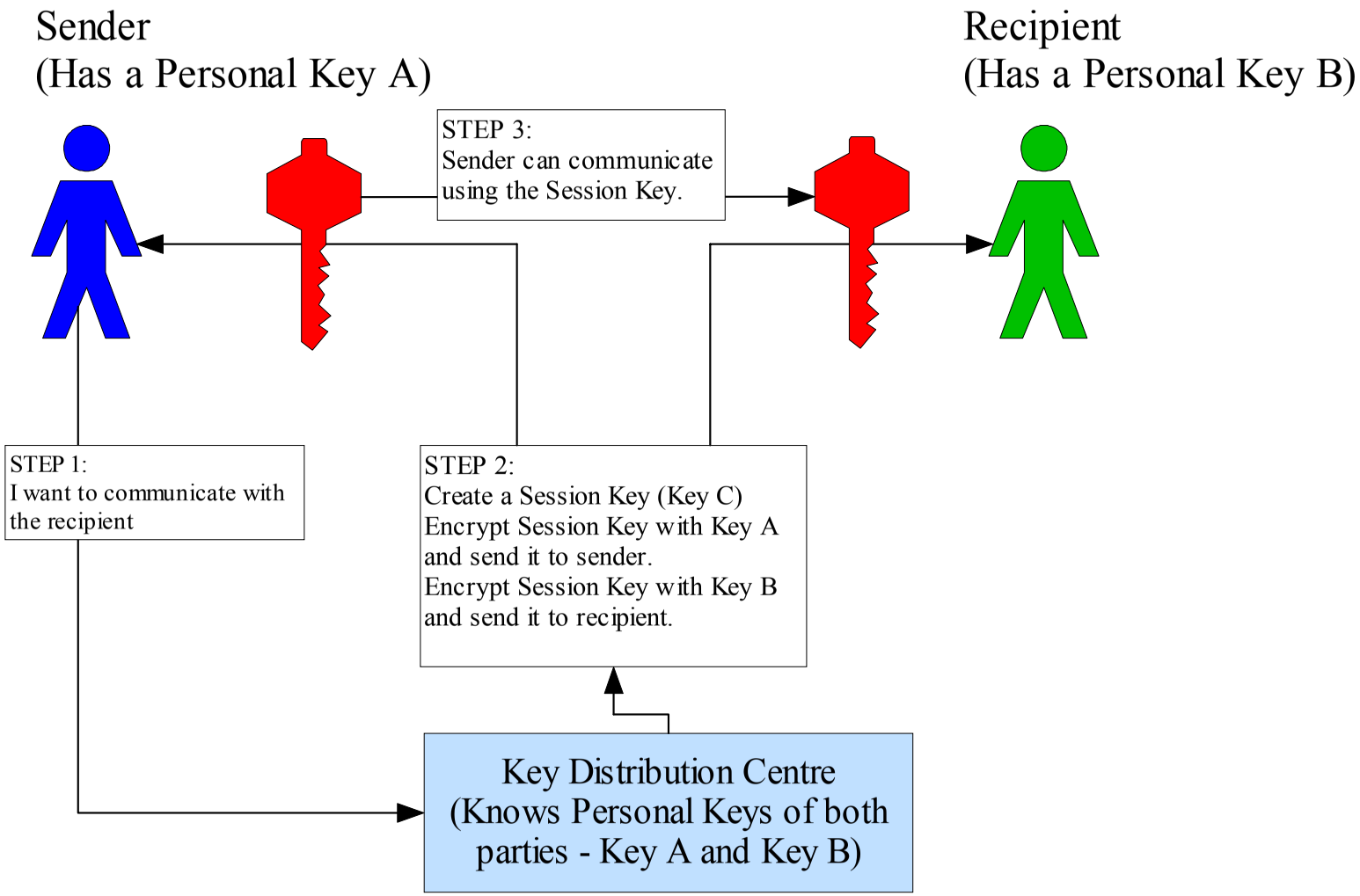
Early days of Cryptography

- Traditionally, secure communication was established using **symmetric** cryptography:
  - A secret key was used to encrypt and decrypt (hence symmetric) data being transmitted.
  - The problem is how the two entities exchange the keys securely
  - One approach was to use a courier – very inefficient.
  - Alternatively there could be a central authority to manage the key.
  - Example: DES is a commonly used encryption algorithm.

Using a Symmetric Key



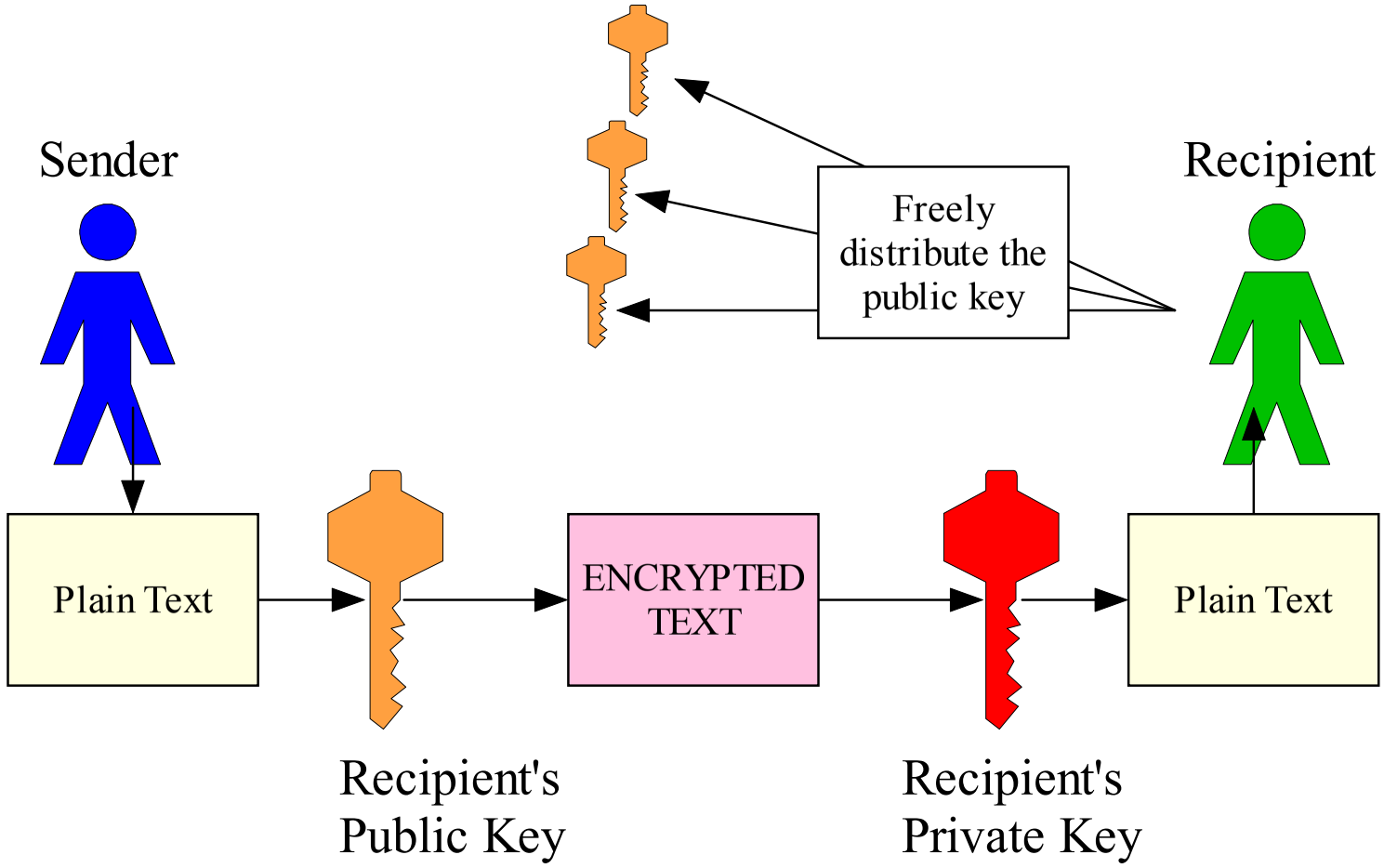
Using a Key Distribution Centre



Public Key Cryptography (1)

- Public Keys are **Asymmetric** (i.e. different keys to encrypt and decrypt the data).
- A **Private Key** is kept secret by the owner.
- The owner also has a **Public Key** which can be freely distributed.
- A sender wishing to send data to a recipient will encrypt the data using the recipient's public key. Only the private key can decrypt it.
- Although the public and private keys are mathematically related, it is computationally infeasible to deduce one from the other.

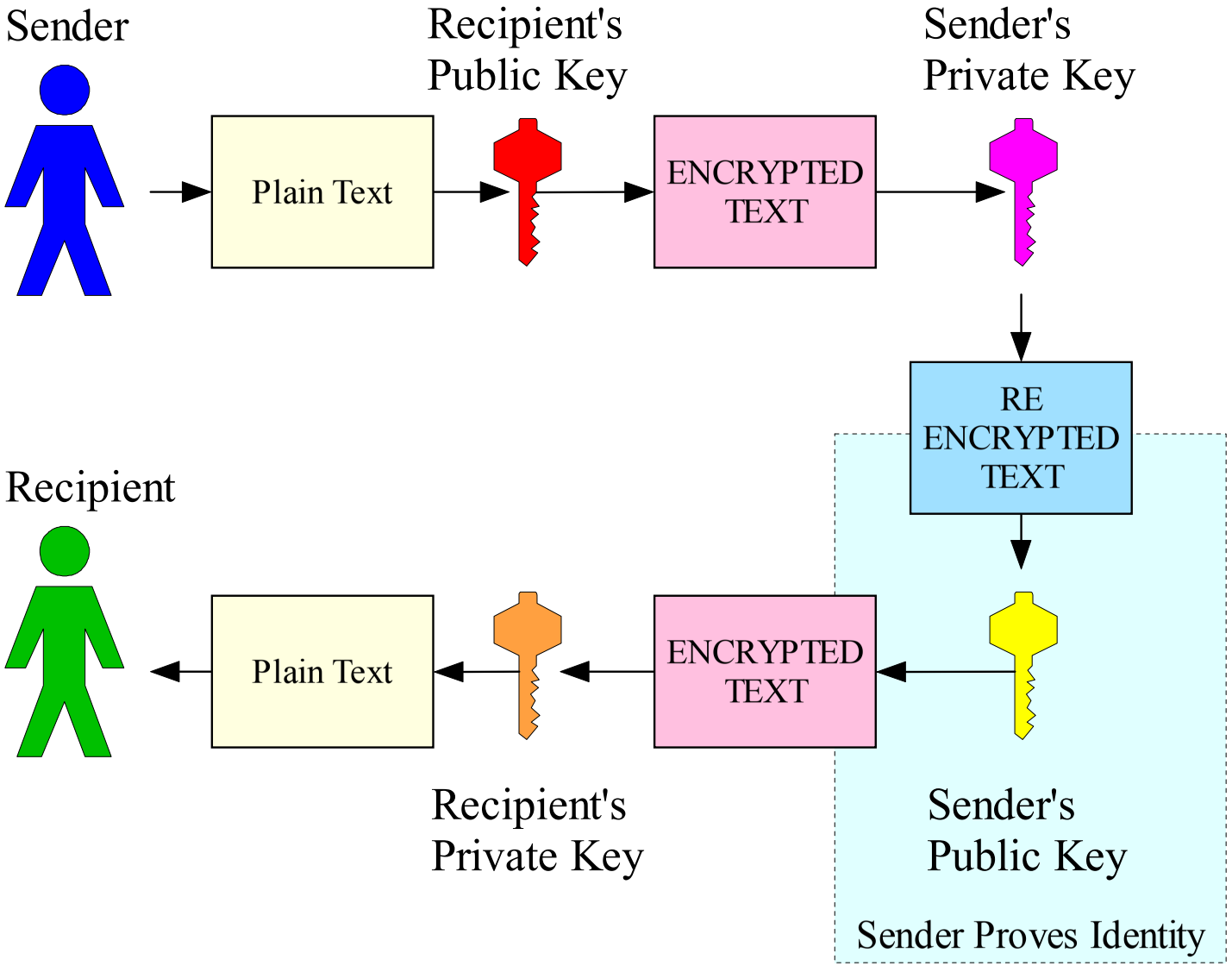
Public Key Cryptography (2)



Public Keys to Authenticate (1)

- If a customer uses a merchant's public key to encrypt credit card info to send, only the merchant would know the private key to decrypt it. So essentially the merchant's identity is proving.
- So far the client's identity is not proven (i.e. the sender is not authenticated)
- but…

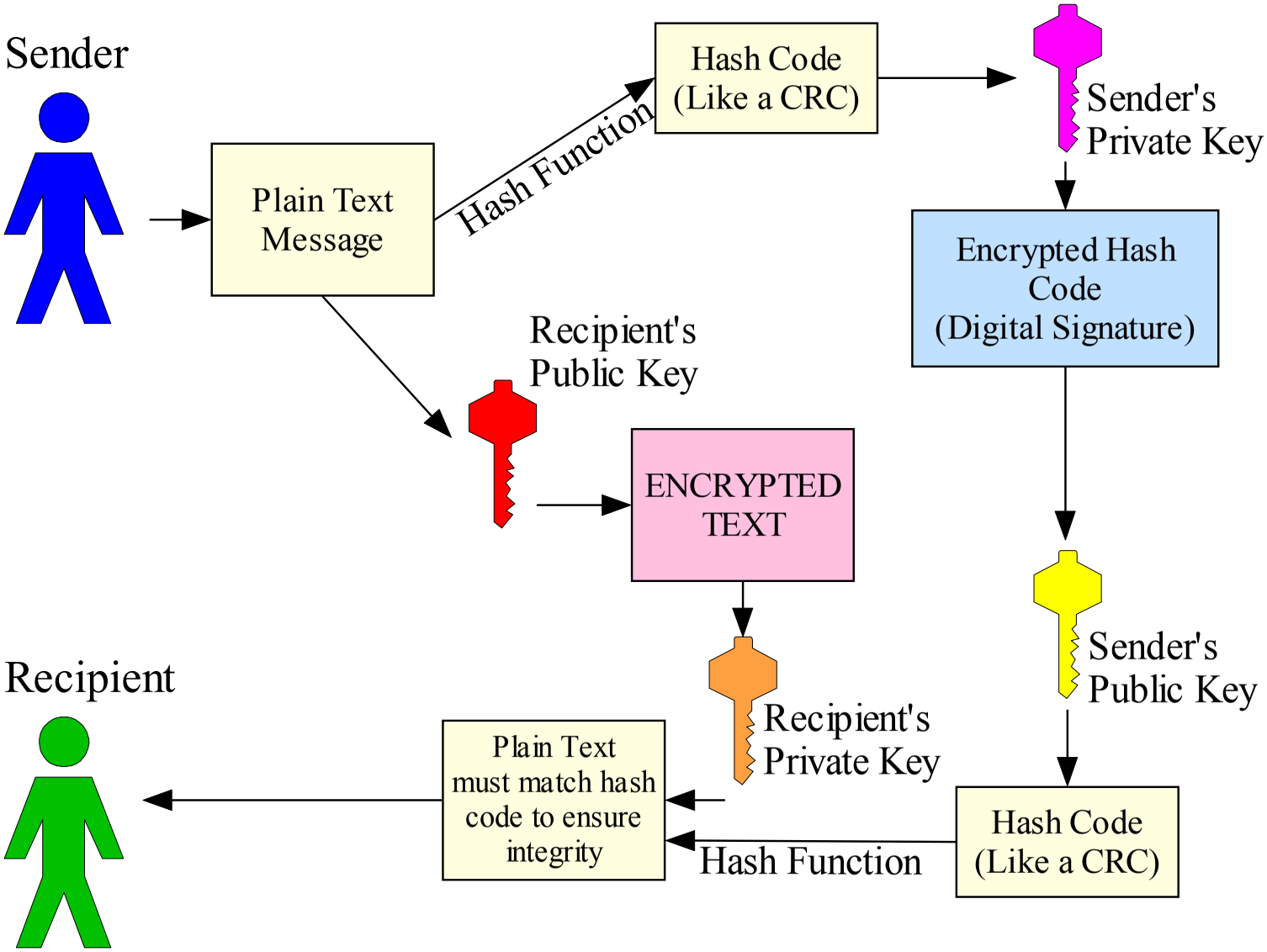
Public Keys to Authenticate (2)



Notes on PKs

- A drawback of PKs is that they require a lot of computing power to encrypt/decrypt and thus slow down communication.
- So it is inefficient to use PKs to transmit large amounts of data.
- An idea is to use PK technology to transmit a symmetric key to be used for subsequent communication.

Digital Signatures (1)



PK Infrastructure, Certificates and Authorities

- A problem with PK technology, is that anyone with a pair of keys can claim to be say Amazon.com to steal your credit card details.
- How do you know that the public key you are using to encrypt data REALLY belongs to Amazon.com?
- A **Digital Certificate** is a digital document issued by a **Certification Authority - CA** (e.g. Verisign).
- The certificate of a merchant is bound its public key.
- Since the CA is responsible for issuing the certificate to the real merchant, one can check the certificate to see that the public key is the legitimate one.

Setting the Scene

1. Client uses web browser opens a **socket** to **request a page** on a site.
2. The request is transmitted over **TCP/IP**.
3. The TCP/IP message is broken down into a number of **packets** (numbered sequentially).
4. Each packet may be **routed** via different paths over the internet to avoid traffic.
5. At the site, all packets are received on the receiving **socket**.
6. They are **concatenated** into the original message and sent to the application (e.g. web server).

Secure Sockets Layer (SSL)

- SSL uses PK's and certificates to authenticate a server and protect private information in a session.
- On the client side SSL is built into almost all web browsers.
  - A client sends a request for a page.
  - The server responds with a certificate.
  - Using PK technology, the server and browser negotiate symmetric session keys.
  - These keys will be used for subsequent comminication.

Network Security – Firewall

- The purpose of a **firewall** is to protect a machine or LAN connected to the internet from an outside attack or theft of data.
- Firewalls can prohibit certain types of communication in and out of the LAN (or individual PC) unless explicitly allowed.
- A simple packet-filtering firewall examines TCP packets and (unless specified) rejects those not originating from the local network. This prevents hackers fro getting inside.

Kerberos (1)

- Firewalls protect from external attack but internal attacks (e.g. naughty employees, unauthorised network access) can be very damaging.
- Kerberos is an protocol used to authenticate users on a network, maintain privacy and integrity.
- Authentication is handled by a main Kerberos System and a Ticket Granting Service (TGS).
- The main Kerberos System authenticates the user on the network and the TGS authenticates the users rights to perform actions on the network.

Kerberos (2)

- Each client has a symmetric key with the Main Kerberos System.
- The client logs on and is authenticated by the Main Kerberos System.
- If logon is successful the client is given a Ticket Granting Ticket (TGT) encrypted with the client's symmetric key.
- Since only the client can decrypt the TGT, the client's identity is proven.
- The client sends the decrypted TGT to the TGS to request a Service Ticket that grants network rights.