Message Digests and Digital Signatures

Dr Rosanne English

Secure Hashes

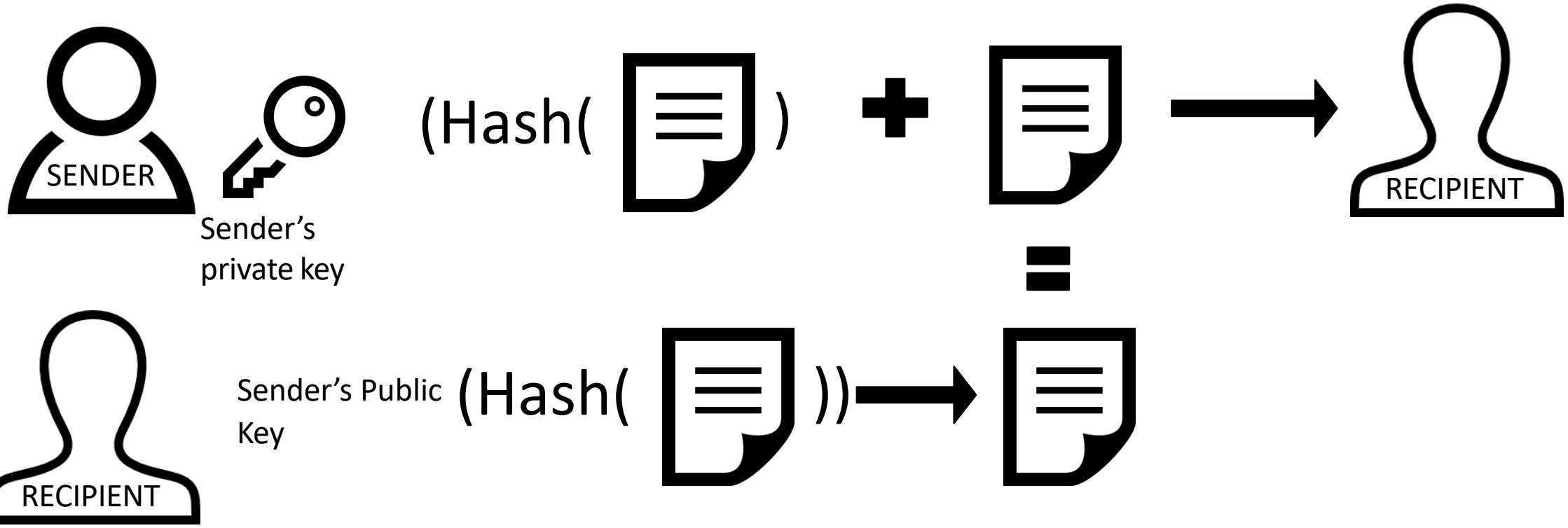
- **One-way property**
  - It is computationally infeasible to find a message that corresponds to a given hash code
- **Strong Collision Resistance**
  - It is computationally infeasible to find two different messages that hash to the same hash value.

Dr Rosanne English

Digital Signature

- Hash of a document encrypted with the sender's private key
- Sent to the recipient with the original document
- They can decrypt the encrypted hash using the sender's public key, and check it against the hash of the document sent

Digital Signature



Real world applications

AUTHENTICATED KEY EXCHANGES:

- in key exchanges we currently could have an attacker impersonate Alice or Bob and send their public key instead of Alice or Bob's public key
- Consider the situation where Bob knows Alice's verify signature if Alice digitally signs the key and sends it with the key then Eve could not replace the key as she is unable to change the signature
- What if Bob doesn't know the verifying key in advance? We'll explore digital certificates which can help

Digital Signature Standards

- Digital signatures can be implemented with RSA, using padding standard PKCS#1 v1.5 but it is INADVISABLE TO DO SO, as this can be susceptible to a Bleichenbacher attack
- Better: **RSA-PSS** updated PKCS#1 v2.1
- Encode the message using the PSS encoding algorithm before signing as before- adds a random salt, and masking
- CURRENT BEST Edwards-curve digital signature algorithm (EdDSA), details are out of scope for this module