Digital Signatures

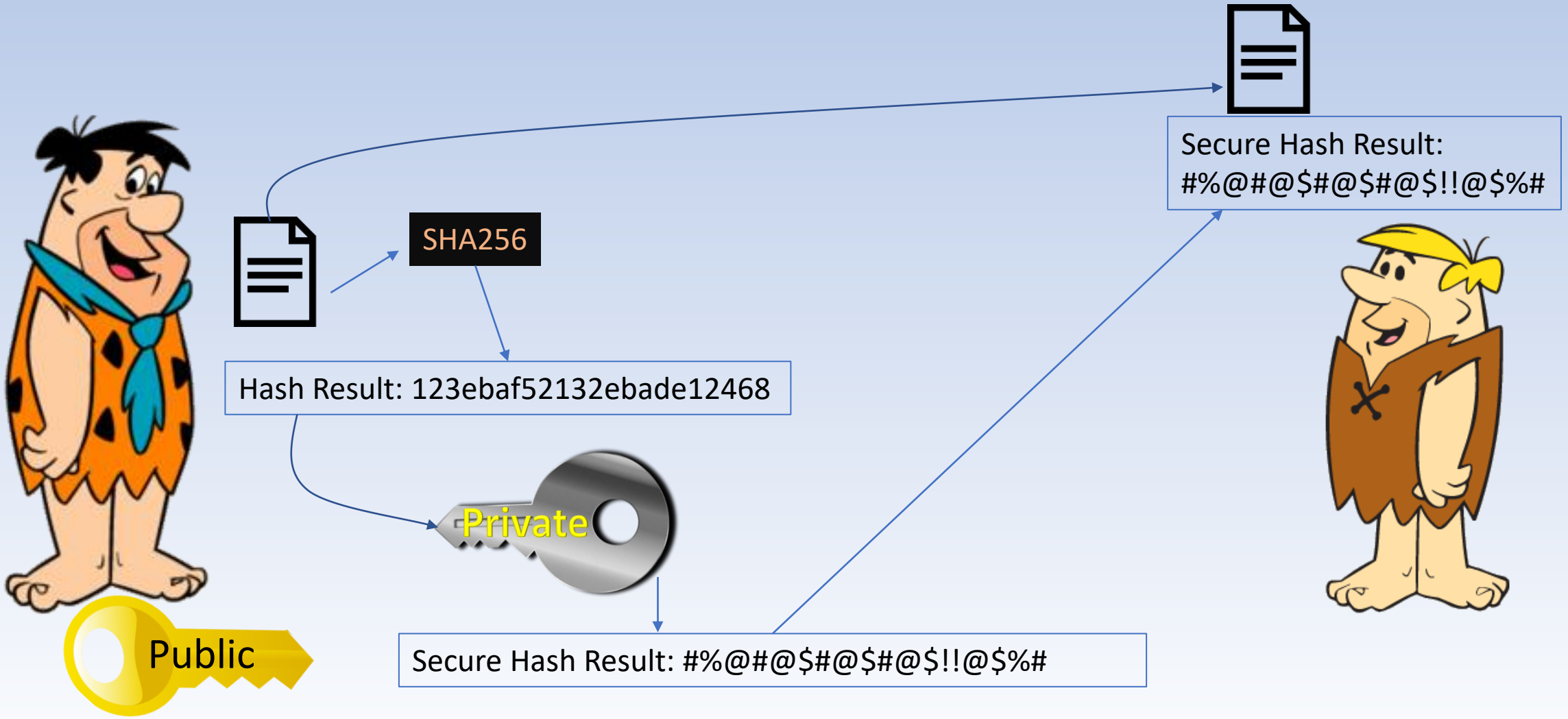
Digital Signature – Usage

- Used for:
  - Data integrity
    - Checks that the data has not been modified from its original state
  - Nonrepudiation
    - Proves which Private Key created the signature
    - When the Private Key is kept safe, it also proves who sent the data

The Signature Creation Process

- Data is processed via a Hash method (SHA256 for example)
- The Hash produces a string of characters as a result
  - This result is unique to this data
  - If the same data is hashed again, it will produce the same result
  - If the data is modified and hashed again, the result will be different
- The Hash Result is then encrypted by the senders Private Key
  - A Digital Signature = Hash result encrypted by the senders Private Key
- The Data and the Digital Signature are sent to the receiving party

The Signature Creation Process (Pic)



The Checking Process

- The receiving party now has the data and the Digital Signature
- The receiving party also needs the sender's Certificate
  - This holds the Public key of the sender
- The receiving party Hashes the received data
- They use the Public Key of the sender to decrypt the Digital Signature
- The decrypted Digital Signature exposes the original Hash Result
- The Original Hash is compared with the Hash done by receiving party
- If both are the same
  - Data has not been modified
  - Because the Public key decrypted the DigSig we can prove who sent the data

The Signature Checking Process (Pic)