Information Systems Security Lec 2:

Digital Signatures

Vanessa Teague, vjteague@unimelb.edu.au

August 2017

What’s a digital signature?

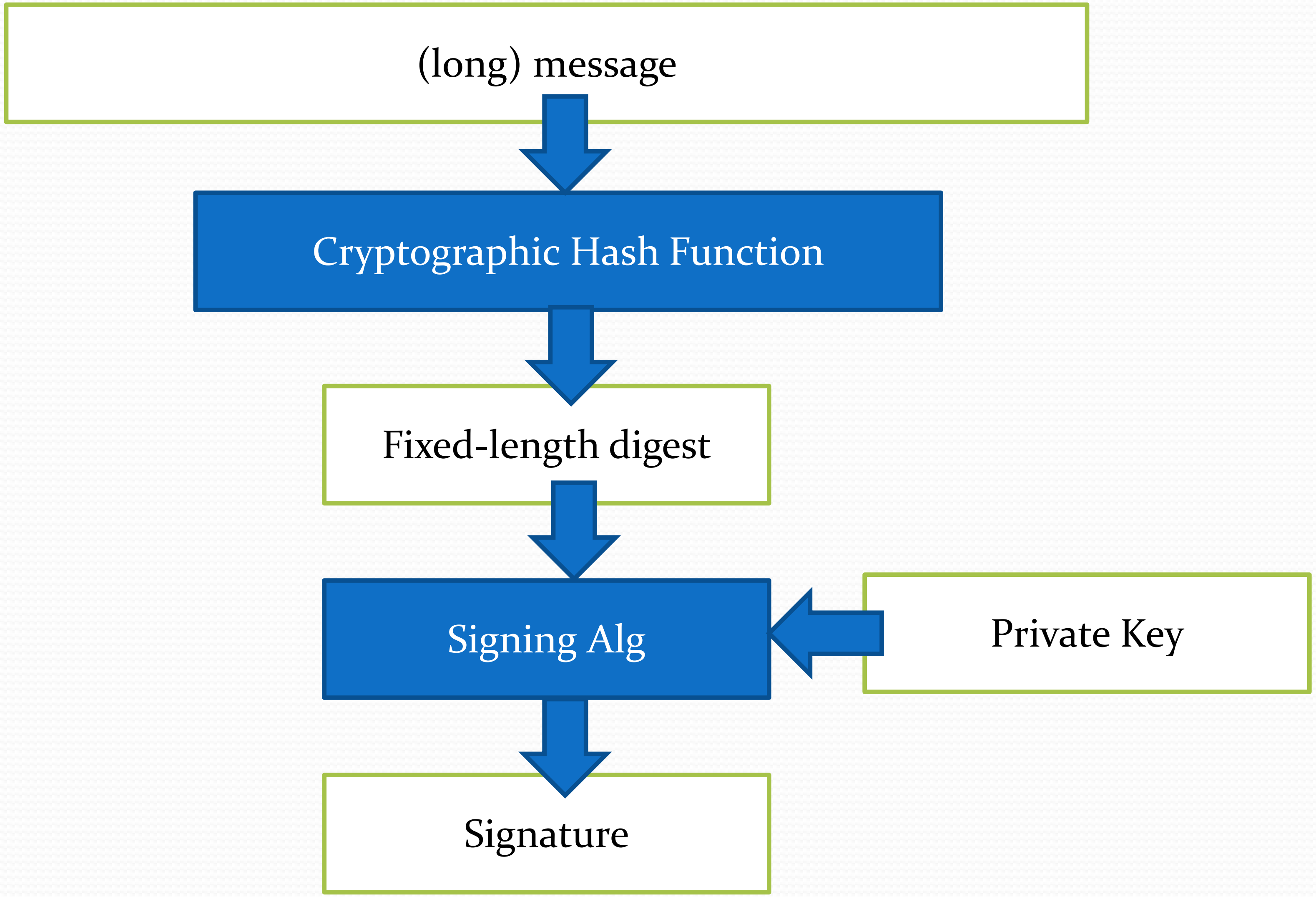
- A mathematical link between a particular message and a particular public key.
  - Signature = Sign(message, private_key)
    - A string of bits that Alice appends to her message
  - Verify(message, signature, public key)
    - Allows Bob to check (using Alice’s public key) that Alice’s private key was used to sign
- Without Alice’s private key, you can’t forge/modify/sign a different message: if you try, verification will fail
- Common examples: RSA, DSA

Digital signatures: more details

- Most digital signature algorithms (e.g. RSA, DSA) hash a message before signing
- A hash algorithm takes a (possibly long) message, and produces a fixed-length digest (at least 160 bits)
- For crypto hashes, it should be infeasible to find two messages that hash to the same digest (this is called a "collision")
- Ex: think about the hashing you studied in algorithms classes, e.g. H(m) = m *a + b mod c. Does that satisfy this def?
- Common examples: MD5 (though this has problems), SHA256, SHA512

A picture of hash & sign

- Ex: If the attacker finds a collision in the hash function, what can they do?



(long) message

Cryptographic Hash Function

Fixed-length digest

Signing Alg

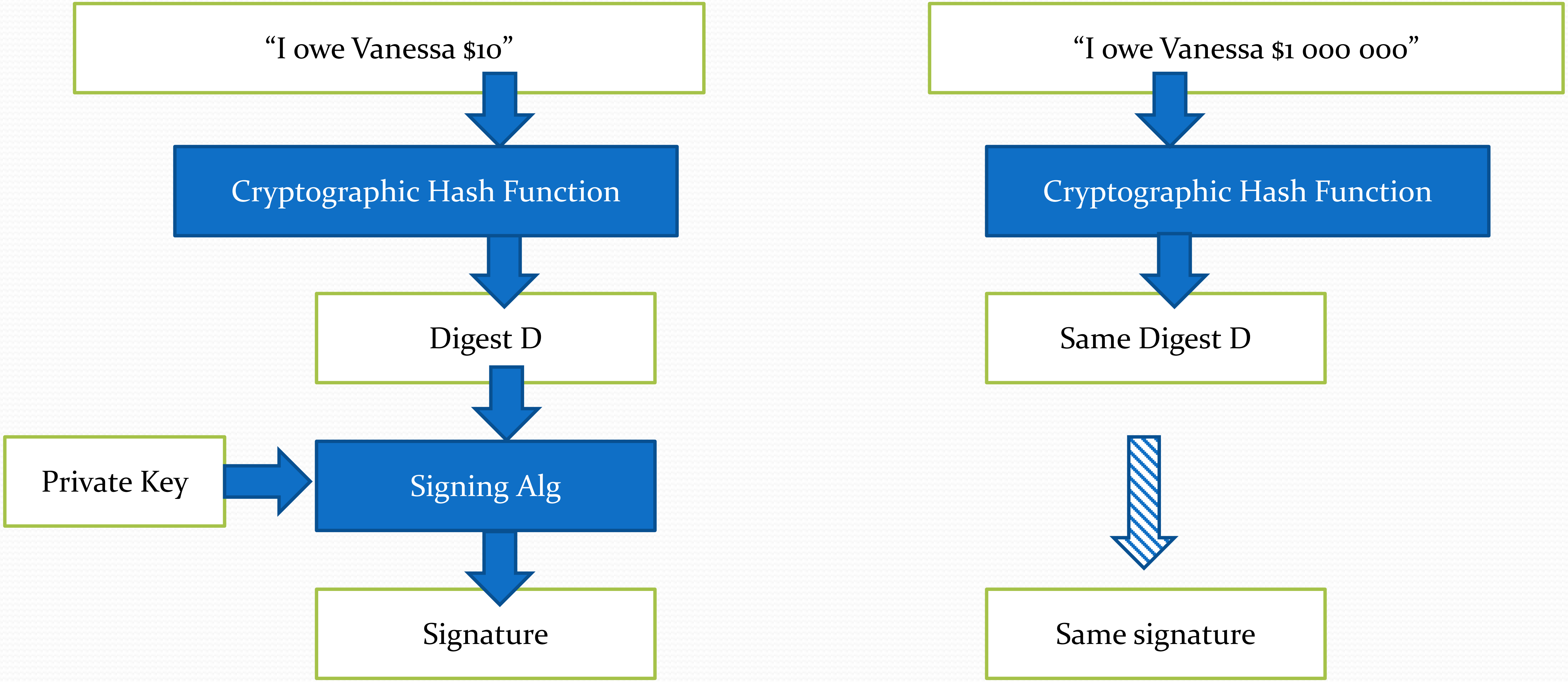
Private Key

Signature

Hash function collisions

- An adversary who finds collisions in the hash function can

If 2 messages hash to the same digest, they have the same signature



“I owe Vanessa $10”

Cryptographic Hash Function

Digest D

Private Key

Signing Alg

Signature

“I owe Vanessa $1 000 000”

Cryptographic Hash Function

Same Digest D

Same signature