Applied Cryptography

Applied Cryptography

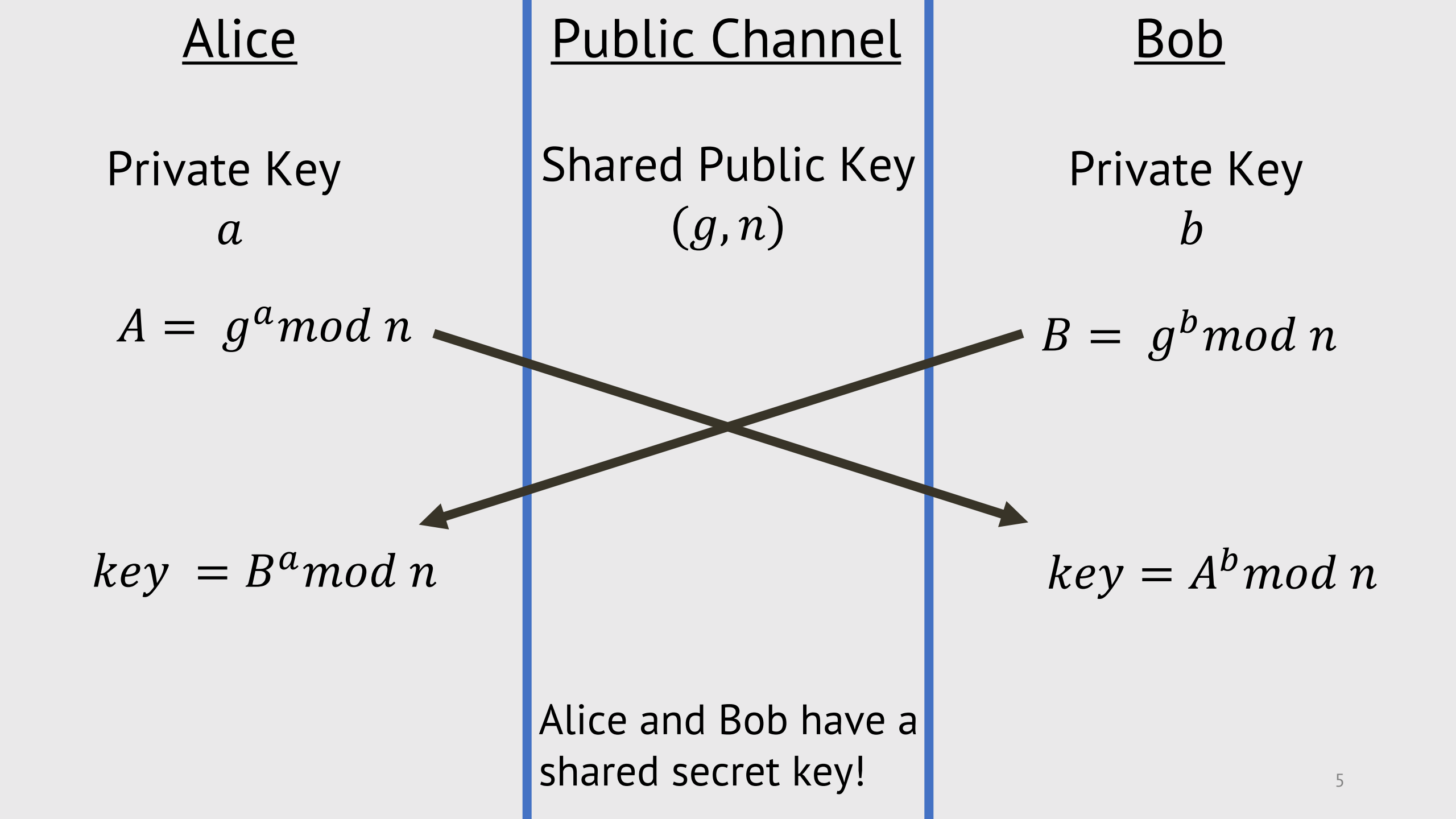
1. Diffie-Hellman Key Exchange
2. Digital Signatures
3. Passkeys
4. Encryption Terminology

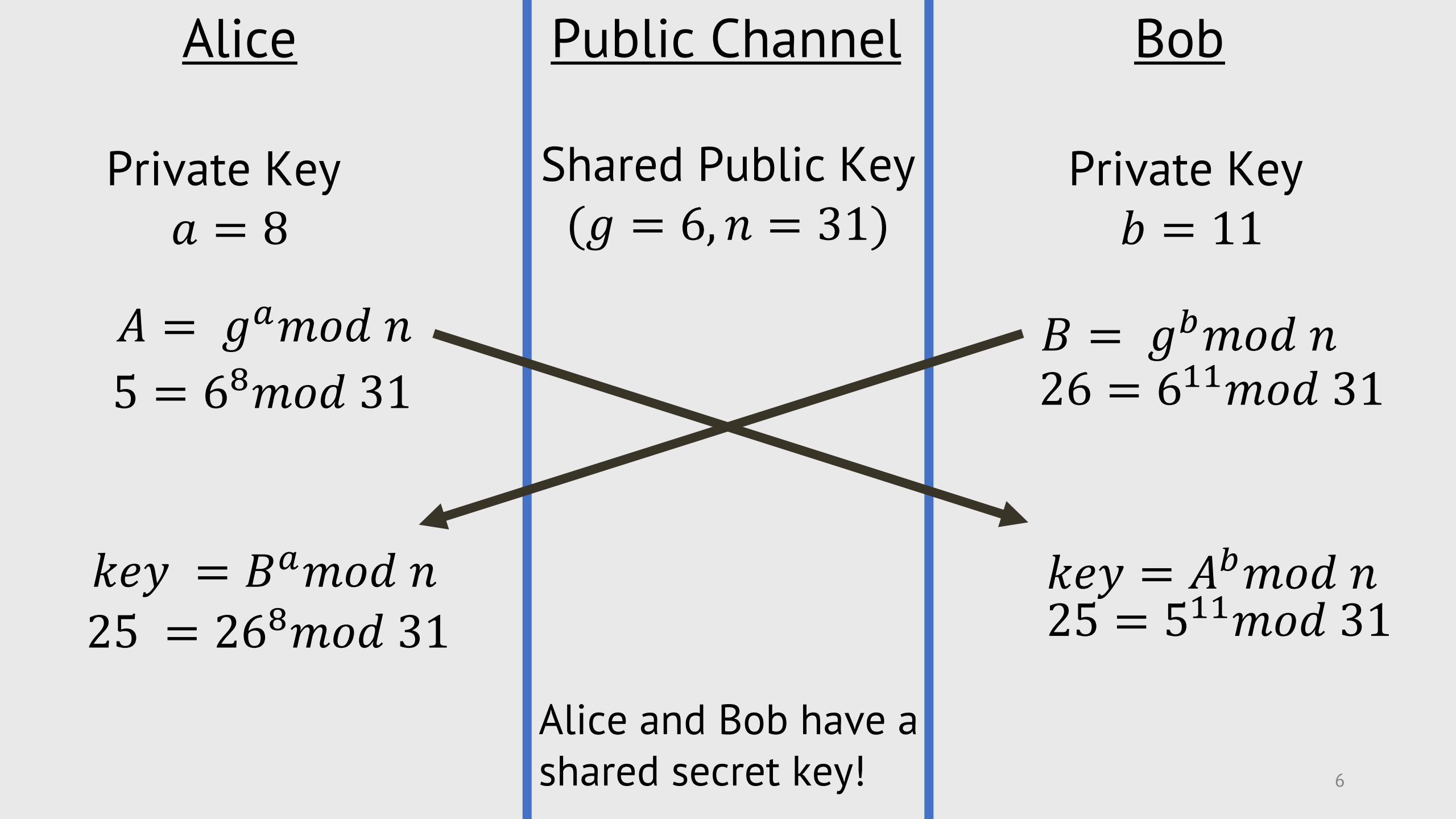
Applied Cryptography

1. Diffie-Hellman Key Exchange
2. Digital Signatures
3. Passkeys
4. Encryption Terminology

Diffie-Hellman key exchange

- With Diffie-Hellman key exchange, two parties arrive at a common secret key, without passing the common secret key in public


Alice
Public Channel
Bob
Private Key
a
Shared Public Key
(g, n)
Private Key
b
$A = g^a mod\ n$
$B = g^b mod\ n$
$key = B^a mod\ n$
$key = A^b mod\ n$
Alice and Bob have a shared secret key!


Alice
Public Channel
Bob
Private Key
$a = 8$
Shared Public Key
$(g = 6, n = 31)$
Private Key
$b = 11$
$A = g^a mod\ n$
$5 = 6^8 mod\ 31$
$B = g^b mod\ n$
$26 = 6^{11} mod\ 31$
$key = B^a mod\ n$
$25 = 26^8 mod\ 31$
$key = A^b mod\ n$
$25 = 5^{11} mod\ 31$
Alice and Bob have a shared secret key!

Applied Cryptography

1. Diffie-Hellman Key Exchange
2. Digital Signatures
3. Passkeys
4. Encryption Terminology

Digital Signatures

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents
- A valid digital signature on a message gives a recipient confidence that the message came from a sender known to the recipient

PK Encryption:

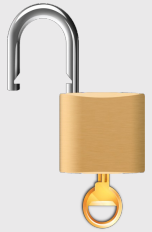
$$m^e \bmod n \equiv c$$

$$c^d \bmod n \equiv m$$

Using **public** key exponent e to encrypt and **private** key exponent d to decrypt

Digital Signature:

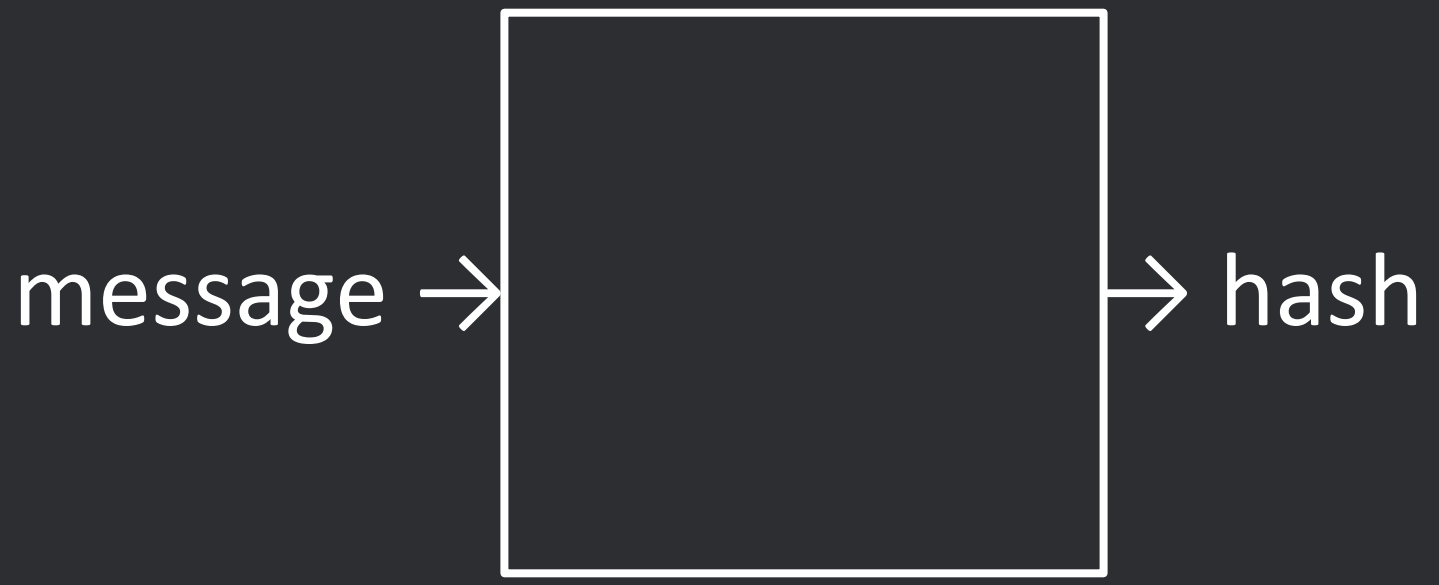
$$m^d \bmod n \equiv c$$



$$c^e \bmod n \equiv m$$

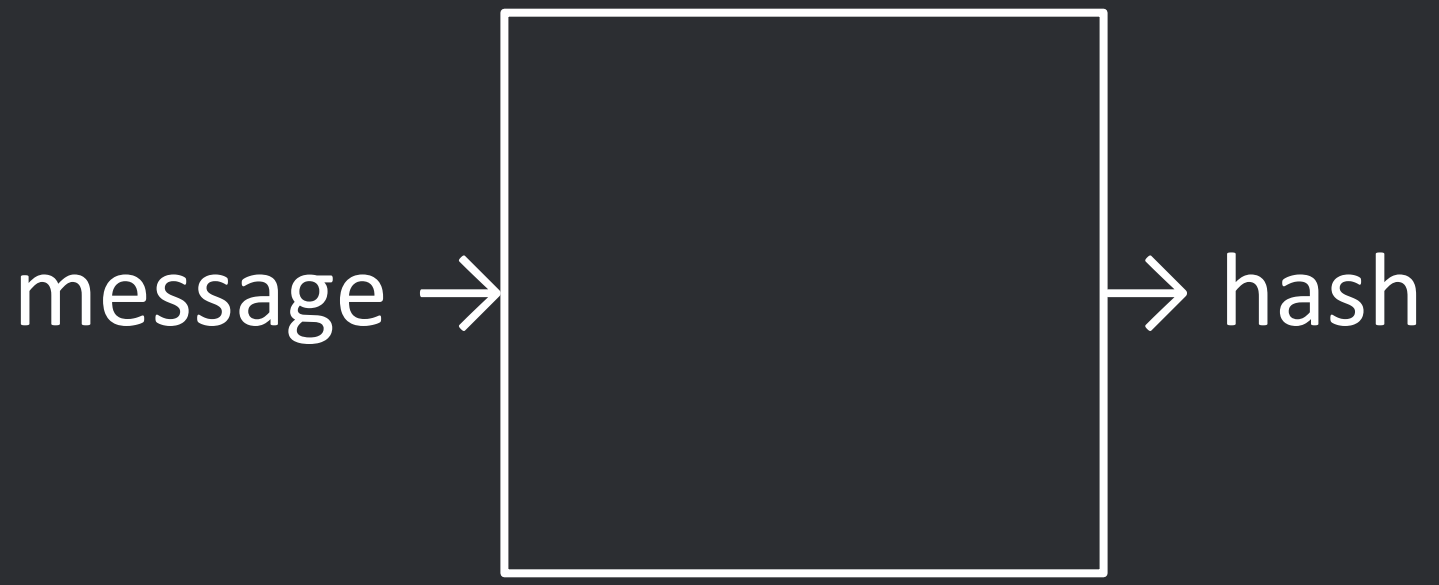
Using **private** key exponent d to encrypt and **public** key exponent e to decrypt

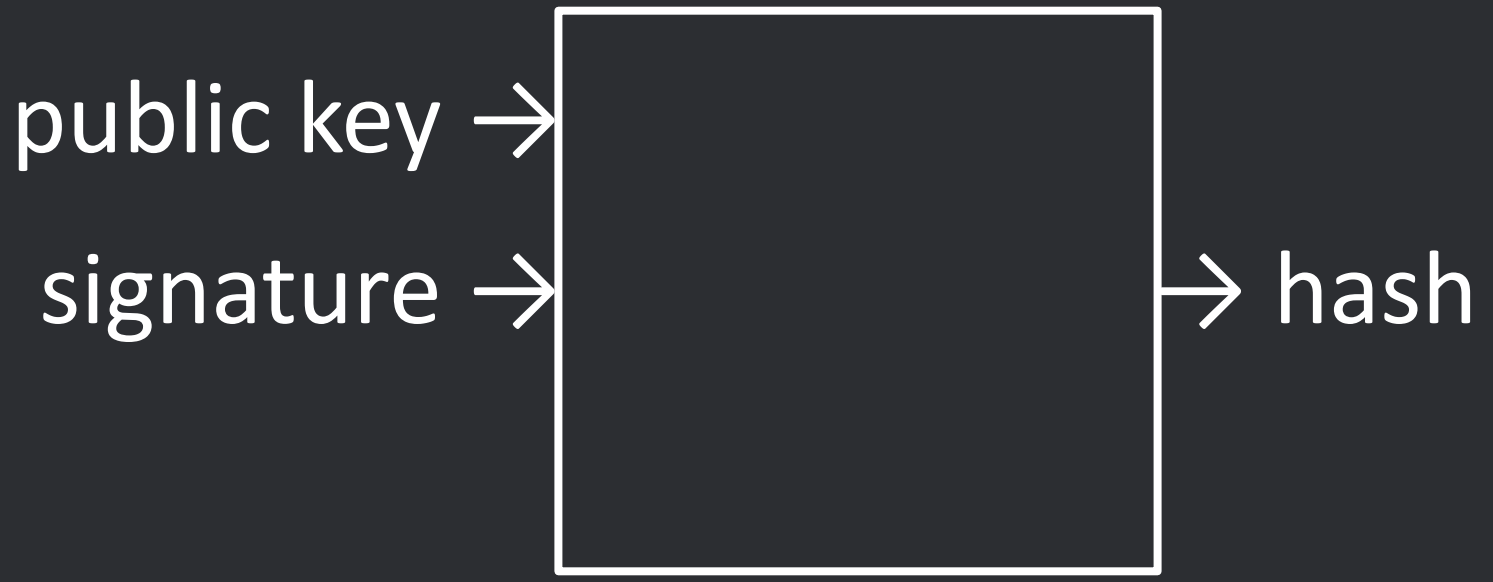
Sign


message
hash


private key
hash
signature

Verify


message
hash


public key
signature
hash

Applied Cryptography

1. Diffie-Hellman Key Exchange
2. Digital Signatures
3. Passkeys
4. Encryption Terminology

Passkeys

Applied Cryptography

1. Diffie-Hellman Key Exchange
2. Digital Signatures
3. Passkeys
4. Encryption Terminology

Encryption at Rest

Encryption in Transit

End-to-End Encryption

Full-Disk Encryption

Ransomware