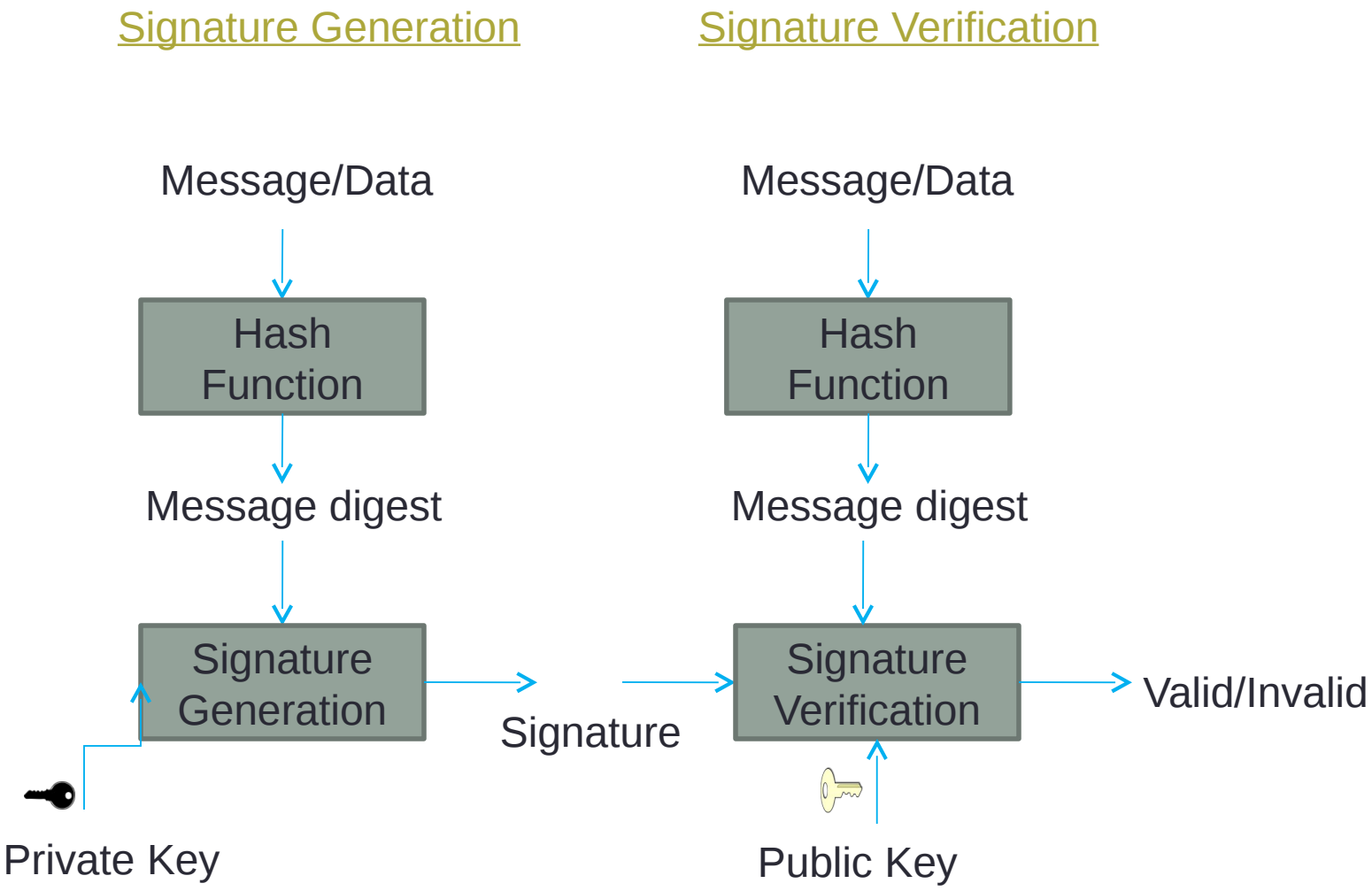
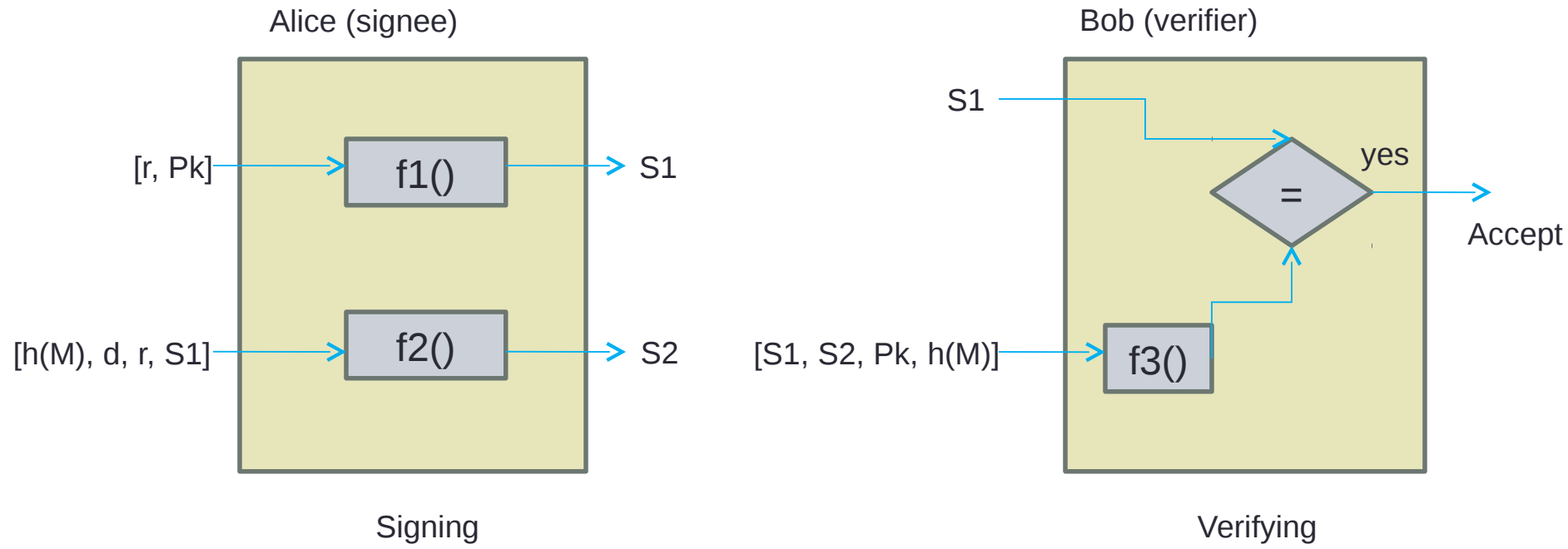
Digital Signatures

Digital Signature Process



Digital Signature Standard

General idea of DSS



S1,S2 : Signatures
M : Message
h(M) : hash of M
d : Alice's private key
Pk: Alice's public key
r : random secret

Digital Signature Standard

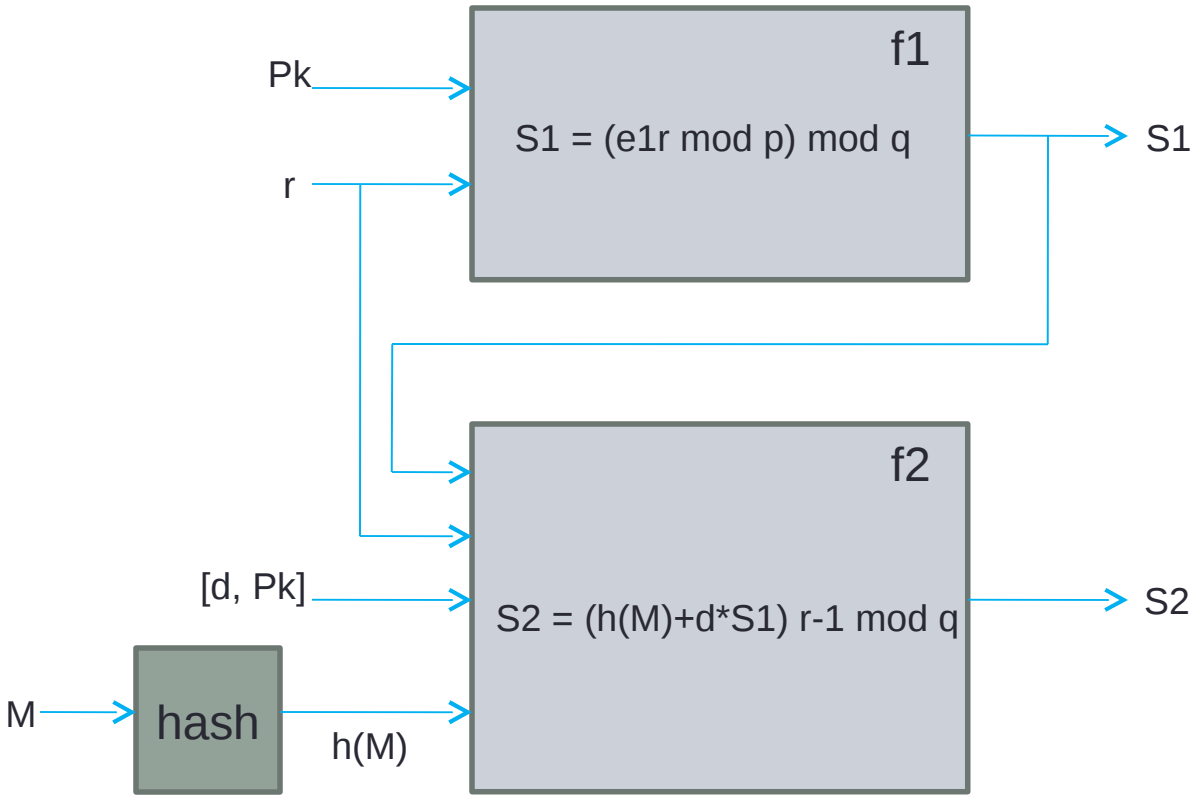
Key Generation

Before signing a message to any entity, Alice(the signee) must generate keys and announce the public keys to the public

Choose a prime p, between 512 and 1024 bits in length. The number of bits in p must be a multiple of 64
Choose a 160-bit prime q in such a way that q divides (p-1)
Choose a primitive root e0 in Zp
Create e1 such that : $e1 = e0^{(p-1)/q} \bmod p$
Chose d as private key and calculate $e2 = e1^{d}$
Alice's public key Pk is (e1, e2, p, q); Private key is d

Digital Signature Standard

Signing



Digital Signature Standard

Verifying