PU A
Public key
Private key
PR A
H()
E()
Hash
Encryption
Decryption
Message
M
Join
||
Signed Message
M||E(PR A,H(M))
Hash
Compare
D()
Plaintext

C=E(PR

A