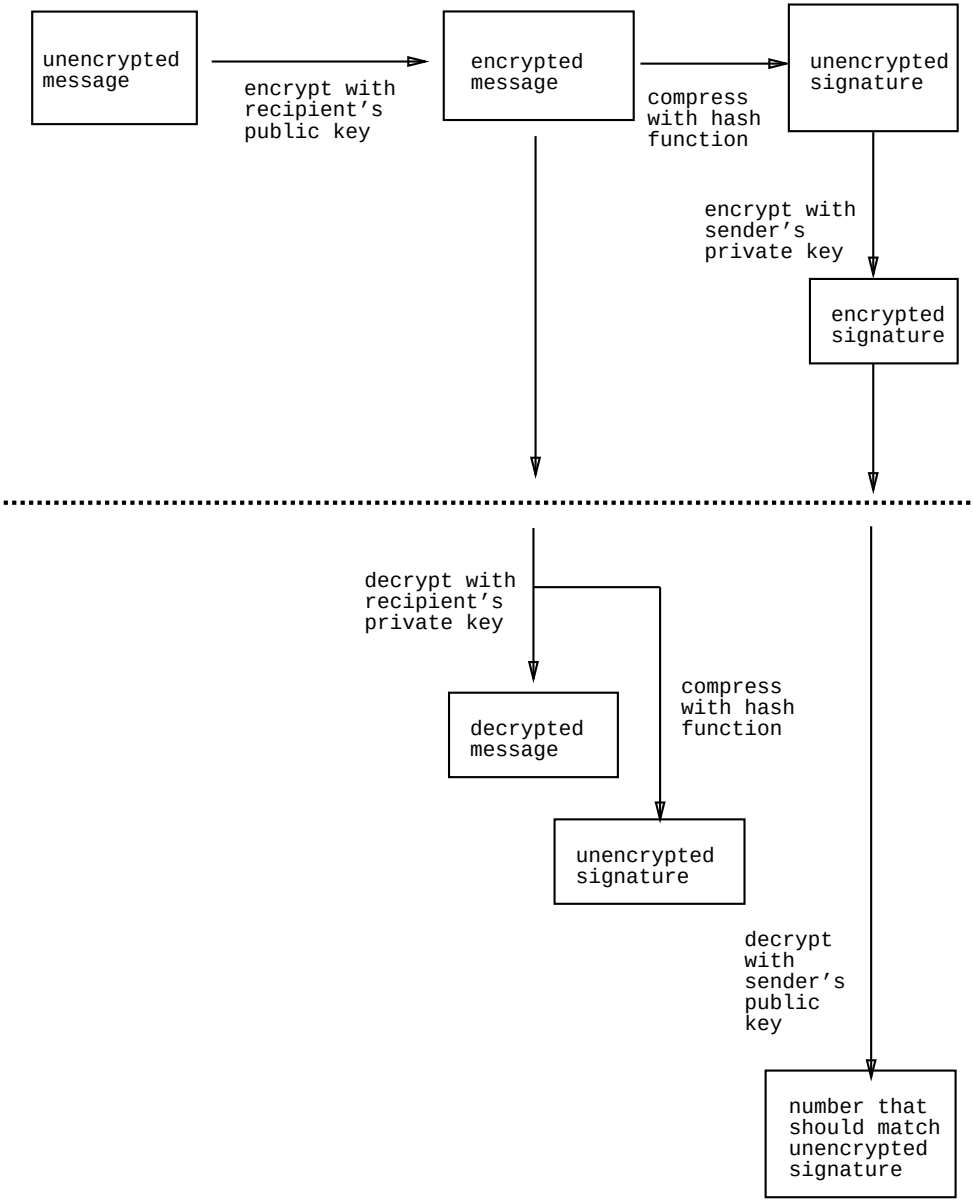
unencrypted message
encrypt with recipient's public key
encrypted message
compress with hash function
unencrypted signature
encrypt with sender's private key
encrypted signature
decrypt with recipient's private key
decrypted message
compress with hash function
unencrypted signature
decrypt with sender's public key
number that should match unencrypted signature