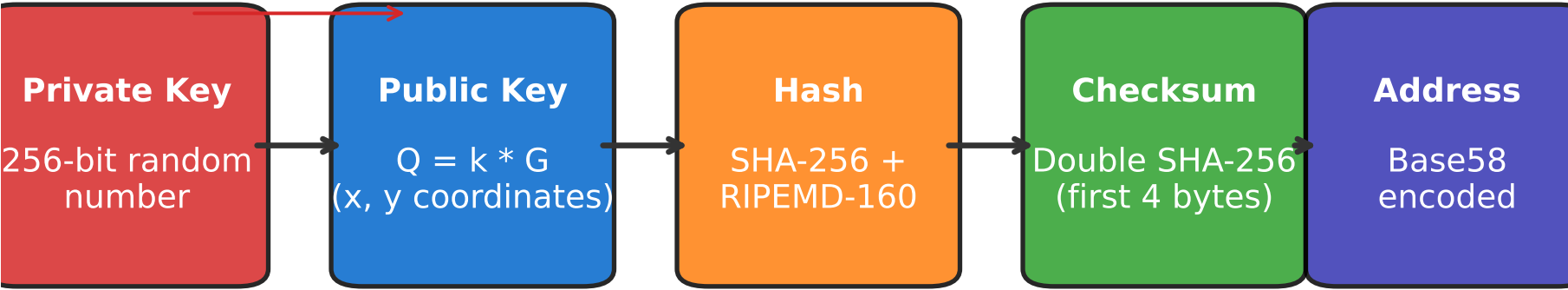


# Bitcoin Address Derivation: From Private Key to Address

**Cannot reverse: Address -> Private Key**

One-way function



*256 bits  
(secret!)*

*33 or 65 bytes  
(public)*

*20 bytes  
(160 bits)*

*4 bytes*

*25-34 chars  
1A1zP1...*