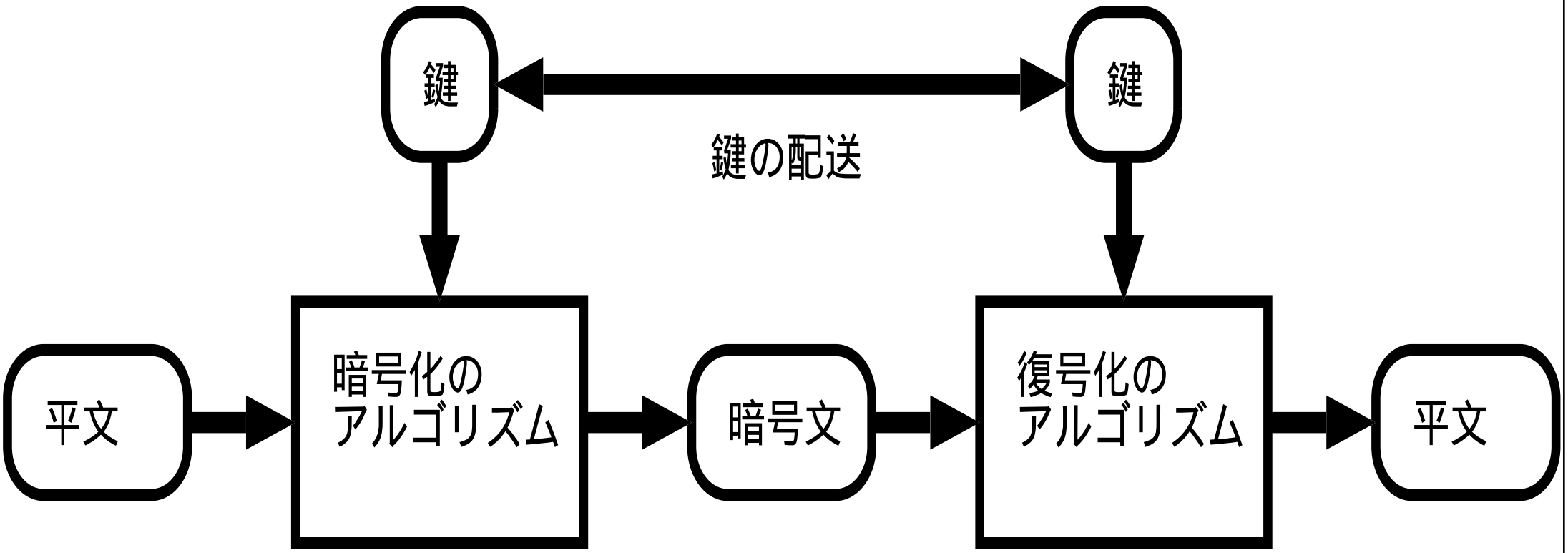
慣用鍵暗号とディジタル署名

鍵を持っているのはふたりだけだから相手から送られてきた後でメッセージを送ったことを否定することを防止はできない

ふたり以外が署名を確認できない