Abstract: Alice has an important message to send to Bob. She can accomplish this by employing Bob’s public key to encrypt the message into a ciphertext, followed by emailing Bob the ciphertext. After sending the encrypted message to Bob, Alice’s email system dutifully keeps an identical copy of the ciphertext in her “Sent” folder in the cloud storage. Sometime later Alice finds herself in a position where she needs to recover the message from the ciphertext, without access to Bob’s decryption key. In this talk I will explain how the problem above can be solved by the use of public key encryption that allows backward recovery by the sender. I will also discuss how to convert a traditional public key encryption technique into one that admits backward recovery by the sender, in such a way that the security of the resultant mechanism can be formally proven.