Digitale Empfangsbestätigung
Wenn eine Nachricht von Alice an Bob gesendet wird, schickt Alice diese unterschrieben und verschlüsselt an Bob.
Bob entschlüsselt und überprüft die Unterschrift. Dann unterschreibt B die Nachricht, verschlüsselt sie mit seinem Public Key und schickt sie an Alice zurück.
Alice entschlüsselt und überprüft die Unterschrift. Stimmen die Nachrichten überein, so hat Bob die Nachricht korrekt bekommen.

Vorsicht ist geboten, wenn die Nachricht mit dem selben Schlüsselpaar. (V,S) = (E,D), also dass der öffentliche Verifikationsschlüssel der Verschlüsselungsschlüssel ist und der private Signaturschlüssel der Entschlüsselungsschlüssel ist. (für alle Beteiligten)
Mallory bringt somit Bob dazu die Verschlüsselung zu entfernen.

Angriffvorgang		**$E_x = V_x$** **$D_x = S_x$**
A unterschreibt, verschlüsselt und schickt an **B**	$E_B (S_A (m))$	$E_B (D_A (m))$
M fängt die Nachricht ab. Und leitet sie an **B** weiter (dadurch denkt **B M** verschlüsselt und signiert)		
B entschlüsselt und überprüft Signatur	$V_A (D_B (E_B (S_A (m)))) = m$	$E_M (D_B (E_B (D_A (m)))) = E_M (D_A (m))$
B unterschreibt, verschlüsselt und schickt an **A / M**	$E_A (S_B (m))$	$E_M (D_B (E_M (D_A (m))))$
Somit hat **M** den Nachrichtentext. Eigener D_M, dann E_B, dann D_M, und zum Schluss E_A E_B und E_A ist ein Public Key		$D_B (E_M (D_A (m)))$ $E_M (D_A (m))$ $D_A (m)$

Tanja Kohler, 01120637