



$$\begin{aligned}
 S^h &\equiv (a^z \bmod q)^h \equiv (a^{xh^{-1} \bmod q-1} \bmod q)^h \equiv a^{x \bmod q-1} \bmod q \equiv \\
 &\equiv Y \bmod q
 \end{aligned}$$

$S^h = Y \bmod q$

2. ב. נרצה לראות כי  $(1)$  איננה תמיד נכונה.   
 ב.3. נראה כי  $M$  ו- $S$  נכונים, ונראה כי  $S' = Y \bmod q$  נכונה.   
 נראה כי  $S' = Y \bmod q$  נכונה,  $S' = Y \bmod q$  נכונה.   
 נראה כי  $S' = Y \bmod q$  נכונה,  $S' = Y \bmod q$  נכונה.

$$S' = (S^{(h(M'))^{-1}})^{h(M)} \Rightarrow S' = (S^{(h(M'))^{-1}})^{h(M)} h(M)$$

$$\Rightarrow S' = (S^{h(M')(h(M'))^{-1}})^{h(M)} \Rightarrow S' = S = Y \bmod q$$

נראה כי  $S' = Y \bmod q$  נכונה,  $S' = Y \bmod q$  נכונה.

$$\text{ver}(M', S') = \text{ver}(M, S) = \text{true}$$