Password Heathen ticution
Server has to Store Some information
about your pass word.
What if the server Stores it exactly? Could easily Steal all the passwords
Could easily steal all the pass words
16- Sac 100 15 can 100 all 1
if ser we is compromised. (Some passwords might be used in multiple places x - x)
(Same passwords might be ased in
malphie places x - x)
Anyone know about hach fanctions?
11.7000 (0.000) 50.0000
hash functions are hard to invert:
if h: X -> Y, then for
procedure (computer program) to find
brocours (Computer brogram) 10 mil
$any \times \epsilon \times s.t. h(x) = y. \leftarrow$
So, we could store nipressional instead
So, we could store hipassword) instead of the pass and itself.
04 400 1000 (4.26/4.
Prine tost as a Gold:
rive rasi as a solo
\times , $\sqrt{82} \pm 0$
\times_{2} \wedge_{0} \times_{3} $+$ \circ \wedge
\times , \times 2 ± 0 \times AND.
n = n = 0
Just ned to Bld over &&