

Website
Domain, D

Choose password
using rules, P_M

Leaked
hash, L

Salt, S_1

→ $P_D = H_1(P_M \mid S_1 \mid D)$

Salt, S_2

→ $H = H_2(S_2 \mid P_D)$

Compare $H =?= L$