$K_i = H(K_{i-1})$

P_i

in

key **E**

out

C_i