KSA

Input: K

/* Initialisation: */

for $i = 0$ **to** $N - 1$ **do**

$S[i] = i$

end for

$j = 0$

/* Scrambling: */

for $i = 0$ **to** $N - 1$ **do**

$j = j + S[i] + K[i \mod \ell]$

$Swap(S[i], S[j])$

end for

Output: S