$x_i = (x_{i-1})^2 \bmod n$