

Stream cipher

Can we use k as a seed?

$$E_k(m) = m \oplus \text{RNG}(k)$$

➡ Be careful of key reused attack !

Break