Stream cipher

Can we use $\mathbf{k}$ as a seed?

$$E_k(m) = m \oplus RNG(k)$$

➡ Be careful of key reused attack !

RC4 - Rivest Cipher 4

Key Size	40 - 2048 bits
Speed	~ 8 cycles / byte

Very simple implementation

Designed in 1987 ... but broken in 2015