Stream cipher

Can we use **k** as a seed?

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

➡ Be careful of key reused attack !

Typical usage : choose a new iv and send it using another encryption scheme **E'**

$$E_k(m) = (E'_k(iv)\ ,\ m \oplus RNG(iv))$$

RC4 - Rivest Cipher 4

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

Very simple implementation

Designed in 1987 ... but broken in 2015