Stream ciphers

wanted version of one-time pad with key k of fixed length (EG k 128 bits)

bad idea repeat k as needed

good idea use k to generate longer keystream $PRG(k)$ of pseudo-random numbers using k as a seed

stream cipher

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

comments

- we lost perfect confidentiality
- security relies on choice of PRG
  must be unpredictable
- we must not reuse keystream
- however, we can reuse key k using a nonce

$$E_k(m) = m \oplus PRG(\overbrace{(\text{nonce}, k)}^{\text{seed}})$$

transmit nonce along with c