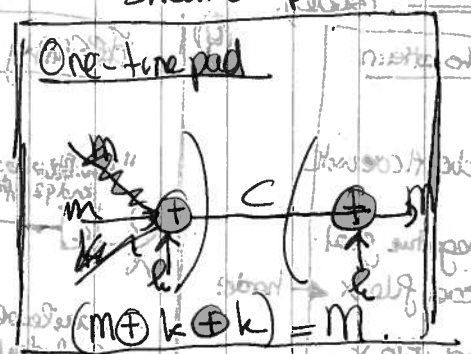
Stream cipher

(10) One-time pad



$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

(10a)

XOR

	0	1
0	0	1
1	1	0

$0 \oplus 1 \oplus 1 = 0$

⇒ cannot reuse key!

(11) Be clever: computationally hard.

- Eg. pseudo-random gen. PRG(seed) ⇒ k (Appendix A4).
- RC4. → slide

Note: no authenticity. (wed)

Window of validity.

Human unfriendly.