One-time pad

XOR (exclusive or)

$\oplus$	0	0	1	1
0	0	1	0	1
=	0	1	1	0

bits are added mod 2

EG $1011 \oplus 1111 = 0100$

note $a \oplus b \oplus b = a$

$25 \equiv 0 \pmod 2$

one-time pad

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

$$m = D_k(c) = c \oplus k$$

E_k, D_k the same!

key k must
- be of same length as m
- only be used once

EG
$k = 1100, 0011$
$m = 1010, 1010$
$c = 0110, 1001$

comments

- perfect confidentiality achieved
  if k perfectly random + only used once
- even if k used twice, can be exploited

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$
$$c_1 \oplus c_2 = m_1 \oplus m_2$$

→ Eve has info about plaintexts!
(if English text in ASCII, enough to recover m_1, m_2)

- little protection of integrity
  m_1 = To: Bob...
  known to Eve
  m_2 = To: Boo...
  Eve can construct c_2 from c_1 without knowing k
- extra challenges:
  - key distribution + management
  - generating perfectly random keys