Practice05

Friday, March 31, 2023 1:46 PM

Stream ciphers (XOR ciphers)

$X = \{0, \dots, 255\}$, OTP

$m \in X^n$ $E_k(m) = C = m \oplus k$

$k \in_R X^n$ $D_k(C) = C \oplus k = E_k(C)$

$\oplus$ XOR	0	1
0	0	1
1	1	0

$a \oplus b = a + b \bmod 2$

$(a \otimes b = a \cdot b \bmod 2)$

$C \oplus k = (m \oplus k) \oplus k \overset{4}{=}$

$= m \oplus (k \oplus k) \overset{1}{=}$

$= m \oplus 0 \overset{2}{=} m$

1° $a \otimes a = 0$

2° $a \otimes 0 = a$

3° $a \oplus b = b \oplus a$

4° $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

Issue 1°: key reuse

m_1, m_2, $C_1 = m_1 \oplus k$, $C_2 = m_2 \oplus k$

$C_1 \oplus C_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) =$

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

0

$m_1 \oplus m_2$

$m_1 \oplus (C_1 \oplus C_2) = (m_1 \oplus m_1) \oplus m_2 = m_2$

0

Key retrival:

$C = m \oplus k$

$m \oplus C = (m \oplus m) \oplus k$

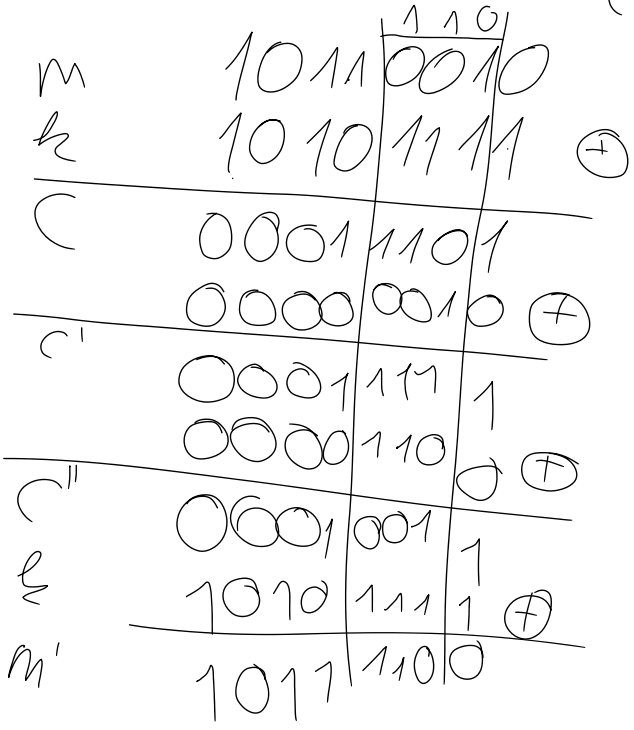
$m \oplus c = (m \oplus m) \oplus k$

Bitflip attack

Attack in the middle

$m \oplus k = c \longrightarrow m', (m, c) \longrightarrow c'$

$c' = c \otimes m \otimes m'$



XOR ciphers are inspired by OTP but use psrg with seed as key

Solution for key reuse

IV: Initialization vector (public)

K: private key for encrypt

For Ec $k = f(IV, K)$

$c = E_k(m)$

(c, IV)