CRYPTO 01 – WED 1

$(|m_0| = |m_1|)$

$\forall m_0, m_1 \in \mathcal{M}$ $[\text{len}(m_0) = \text{len}(m_1)]$ and $\forall c \in \mathcal{C}$

$Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$

k IS UNIFORM IN $\mathcal{K}$ $(k \xleftarrow{R} \mathcal{K})$

PLAINTEXT CAN'T BE KNOWN FROM CIPHER TEXT (CT ATTACK)

$\forall m, c: \quad Pr[E(k, m) = c] = \frac{\#\text{KEYS } k \in \mathcal{K} \text{ WHEN } E(k, m) = c}{|\mathcal{K}|}$

SO!

$\forall m, c: \quad \#\{k \in \mathcal{K} : E(k, m) = c\} = \text{CONST.}$ (PERFECT SECRECY)

OTP IF $E(k, m) = c$ $\Rightarrow$ $k \oplus m = c$, $k = m \oplus c$ $\Rightarrow$ $\#\{k \in \mathcal{K} : E(k, m) = c\} = 1$ $\forall m, c$

ONLY IF:
- NO CT ONLY ATTACK
- KEY LENGTH AT LEAST AS LONG AS MSG

$|\mathcal{K}| \geq |\mathcal{M}|$

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$

$E(k, m) = k \oplus m, \quad D(k, c) = k \oplus c$

(PERFECT SECRECY)

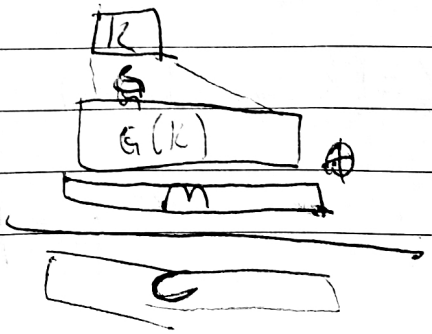
SYMMETRIC ENCRYPTION – STREAM CIPHERS

$\forall m \in \mathcal{M}, k \in \mathcal{K}: \quad D(k, E(k, m)) = m$

SC: REPLACES "RANDOM" KEY BY "PSEUDORANDOM" KEY IN ORDER TO MAKE OTP PRACTICAL.

$c = E(k, m) := m \oplus G(k)$

$D(k, c) := c \oplus G(k)$



PRG MUST BE UNPREDICTABLE

$G: K \longrightarrow \{0,1\}^n$ IS PREDICTABLE IF:

$\exists$ "EFFICIENT" alg A and $\exists\ 1 \le i \le n-1$

$$Pr\left[A(G,K)\big|_{1,\dots,i} = G\left(K\big|_{i+1}\right)\right] \geq \frac{1}{2} + \epsilon$$

WEAK PRGs DO NOT USE FOR CRYPTO.

LO GLIBC RANDOM()

NEVER USE

OTP ATTACK (FOR OTP USED 2 TIMES OR 2 TIME PAD ATTACK)

$PRG(K) \oplus M_1 \longrightarrow C_1$

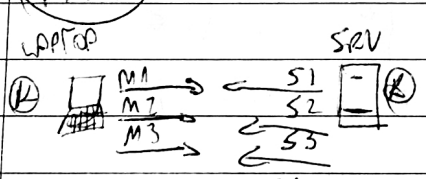
$PRG(K) \oplus M_2 \longrightarrow C_2$

$C_1 \oplus C_2 \longrightarrow M_1 \oplus M_2$

$M_1 \oplus M_2 \longrightarrow M_1, M_2$ (ASCII)

EXAMPLES

PPTP



$[M_1 || M_2 || M_3 || \dots] \oplus PRG(K)$

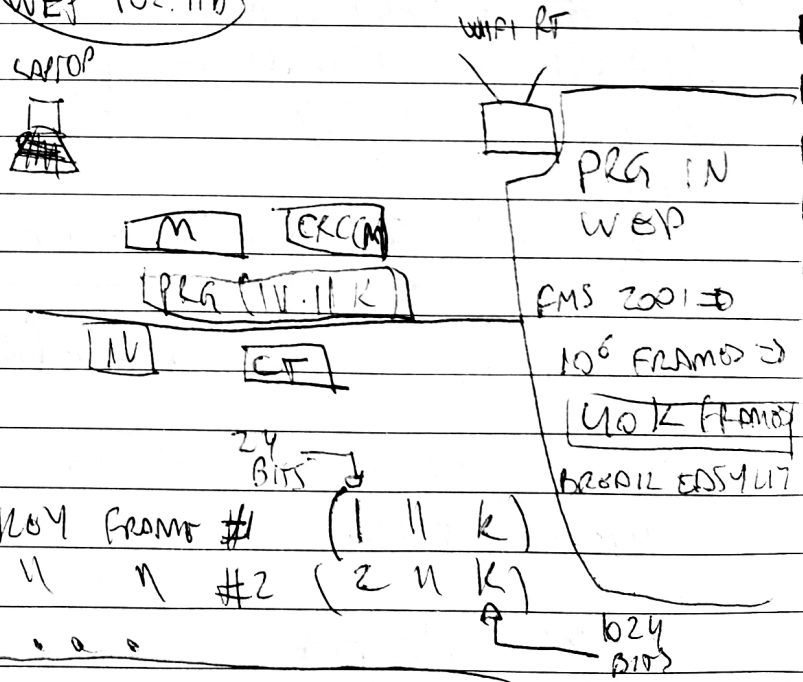
$[S_1 || S_2 || S_3 || \dots] \oplus PRG(K)$ } SAME KEY

WE NEED $\neq$ KEYS

$C \longrightarrow S \;//\; S \longrightarrow C$

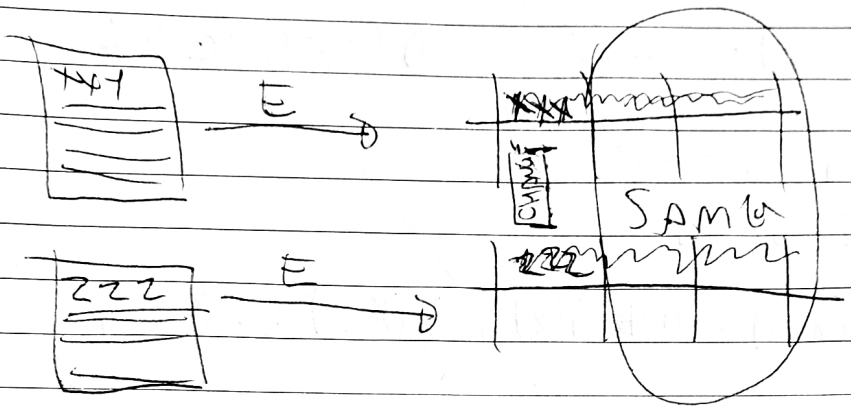
$K = (K_{S \to C}, K_{C \to S})$

WEP 802.11b



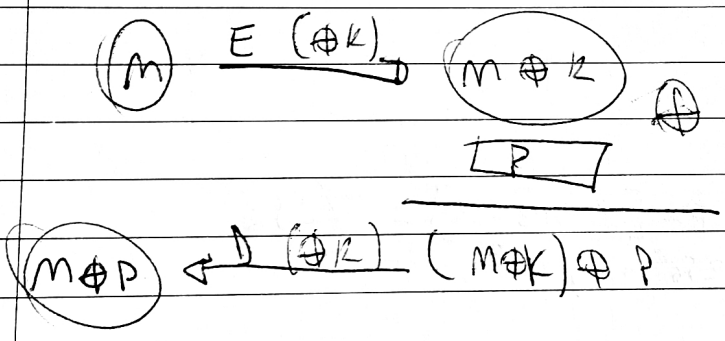
SHOULD AVOID RELATED KEYS

ONE-TIME OTP ATTACK: DISK ENCRYPTION



NEVER USE SC (STREAM CIPHER) MORE THAN ONCE
- NETWORK TRAFFIC → NEGOTIATE NEW KEY FOR EVERY SESSION (TLS)
- DISK ENCRYPTION → DOES NOT USE (SC)

ATTACK 2 (MALLEABILITY)



ATTACK 2 (NO INTEGRITY)

FROM BOB $\xrightarrow{E(\oplus K)}$ FROM BOB ⊕ 000

FROM EVE $\xrightarrow{D(\oplus K)}$ FROM: EVE

PREDICTABLE

BOB	EVE	BOB ⊕ EVE
426F62	457665	071907

→ REAL WORLD SC

OTP: $E(k,m) = m \oplus k$, $D(k,c) = c \oplus k$

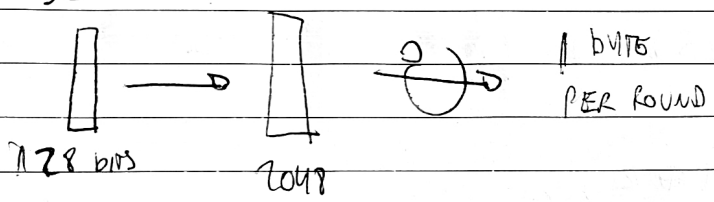
PRG: $G: K \rightarrow \{0,1\}^N$

SEED

SC $E(k,m) = m \oplus G(k)$, $D(k,c) = c \oplus G(k)$

SC RC4

SEED

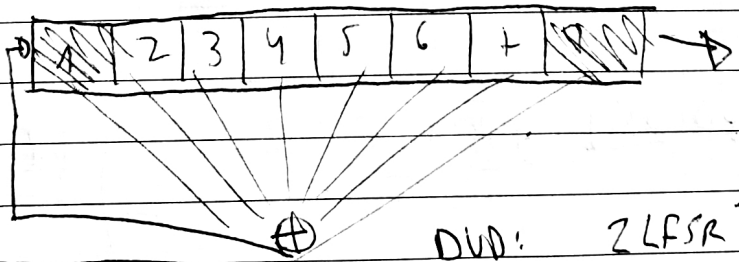


→ USED IN HTTPS AND WEP

- BIAS: INITIAL OUTPUT $Pr[2^{nd} \text{ byte} = 0] = 2/256$
- PROB. $(0,0)$ IS $1/256^2 + 1/256^2$
- RELATED KEY ATTACKS

SC CSS (BADLY BROKEN)

- HARDWARE SC - LFSR (LINEAR FEEDBACK SHIFT REGISTER)



SEED IS THE INIT STATE OF LFSR

SEED = 5 BYTES = 40 BITS

DVD: 2 LFSR
GSM: 3 4
BLUETOOTH: 4 4
} ALL BROKEN.

MODERN SC | ESTREAM (2008)

$PRG: \{0,1\}^S \times R \rightarrow \{0,1\}^N \quad N >> S$

SEED — NONCE — NON REPEATING VALUE FOR A GIVEN KEY

$E(k, m; r) = m \oplus PRG(k; r)$

NEVER USE MORE THAN ONCE (UNIQUE)

ESTREAM SALSA20

$SALSA20(k; r) := H(k, (r, 0)) \,||\, H(k, (r, 1)) \,||\, \ldots$