Stream ciphers

Attacks on OTP and stream ciphers

Review

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

Making OTP practical using a PRG: $G: K \longrightarrow \{0,1\}^n$

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

Security: PRG must be unpredictable (better def in two segments)

Attack 1: **two time** pad is insecure !!

Never use stream cipher key more than once !!

$$C_1 \leftarrow m_1 \oplus PRG(k)$$
$$C_2 \leftarrow m_2 \oplus PRG(k)$$

Eavesdropper does:

$$C_1 \oplus C_2 \rightarrow$$

Enough redundancy in English and ASCII encoding that:

$$m_1 \oplus m_2 \rightarrow m_1, m_2$$

Real world examples

- Project Venona

- MS-PPTP (windows NT):

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

k

m_1

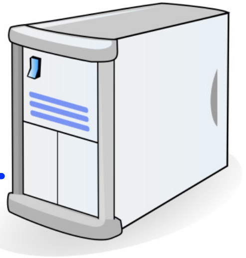
m_2

m_3

s_1

s_2

s_3



k

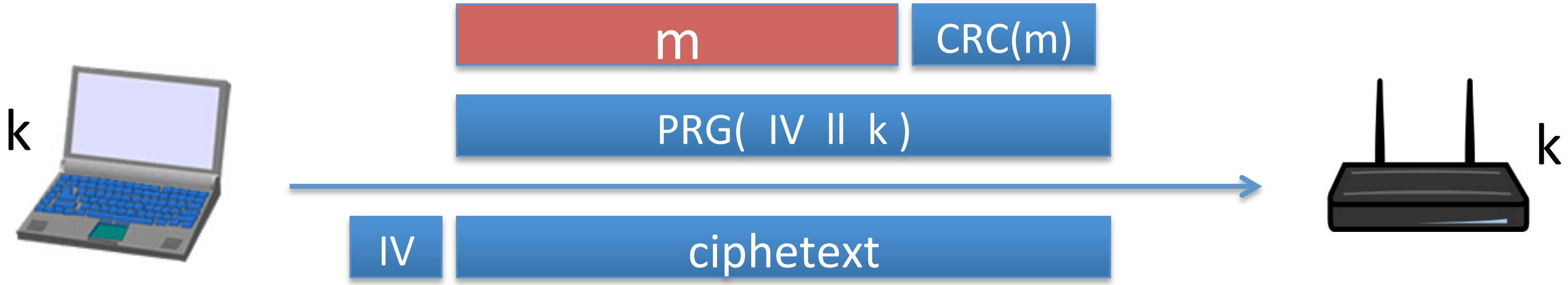
$[m_1 \| m_2 \| m_3] \oplus G(K)$

$[s_1 \| s_2 \| s_3] \oplus G(K)$

Need different keys for $C \longrightarrow S$ and $S \longrightarrow C$

Real world examples

802.11b WEP:

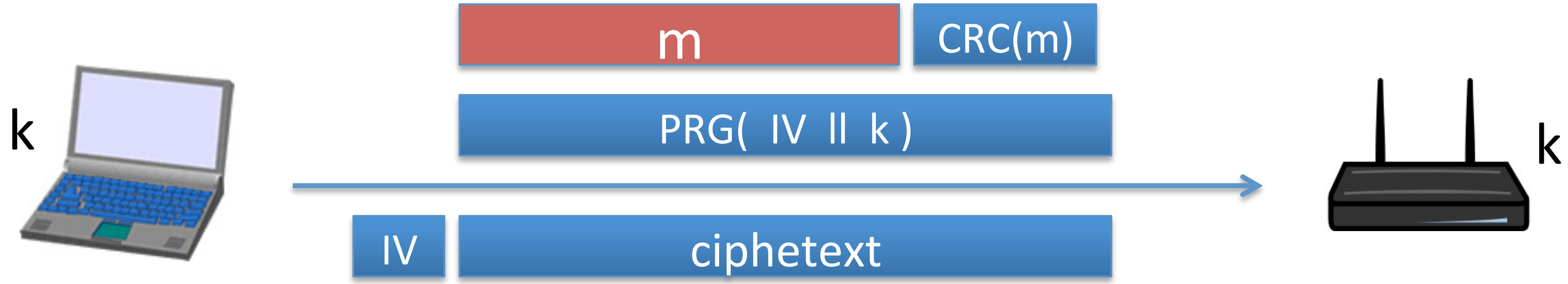


Length of IV: 24 bits

- Repeated IV after $2^{24} \approx$ 16M frames
- On some 802.11 cards: IV resets to 0 after power cycle

Avoid related keys

802.11b WEP:



key for frame #1: (1 ll k)

key for frame #2: (2 ll k)

⋮

24 bits

104 bits

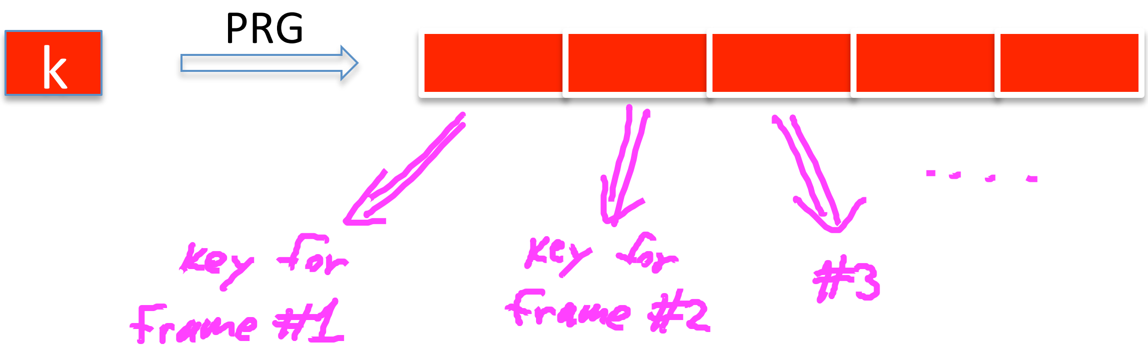
For the RC4 PRG:

FMS2001 $\Longrightarrow$ can recover k after 10^6 frames

Recent attacks $\approx$ 40,000 frames

A better construction

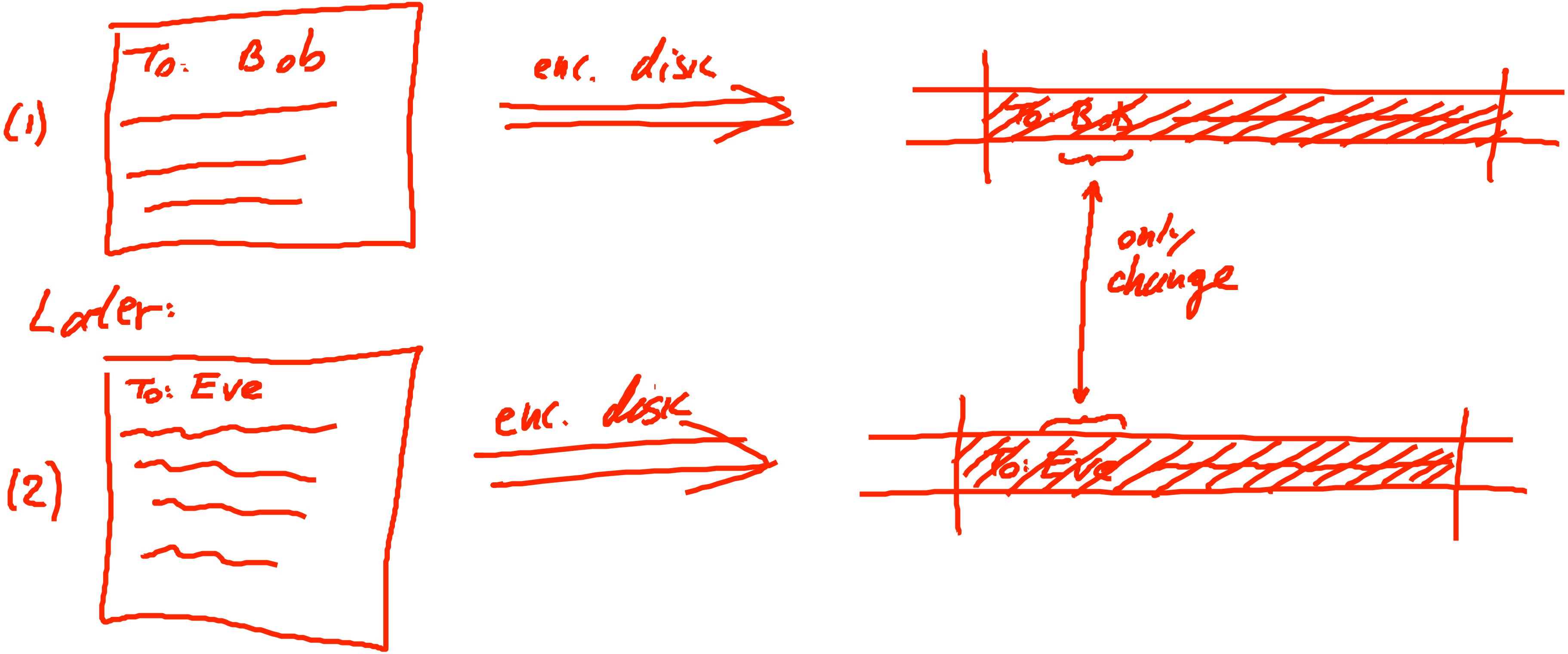
k



$\Rightarrow$ now each frame has a pseudorandom key

better solution: use stronger encryption method (as in WPA2)

Yet another example: disk encryption



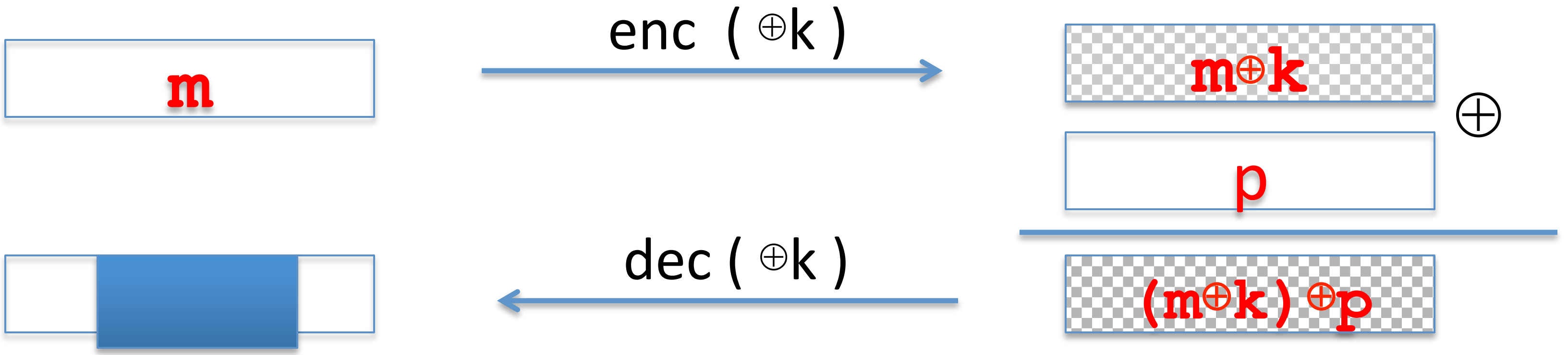
Two time pad: summary

Never use stream cipher key more than once !!

- Network traffic: negotiate new key for every session (e.g. TLS)

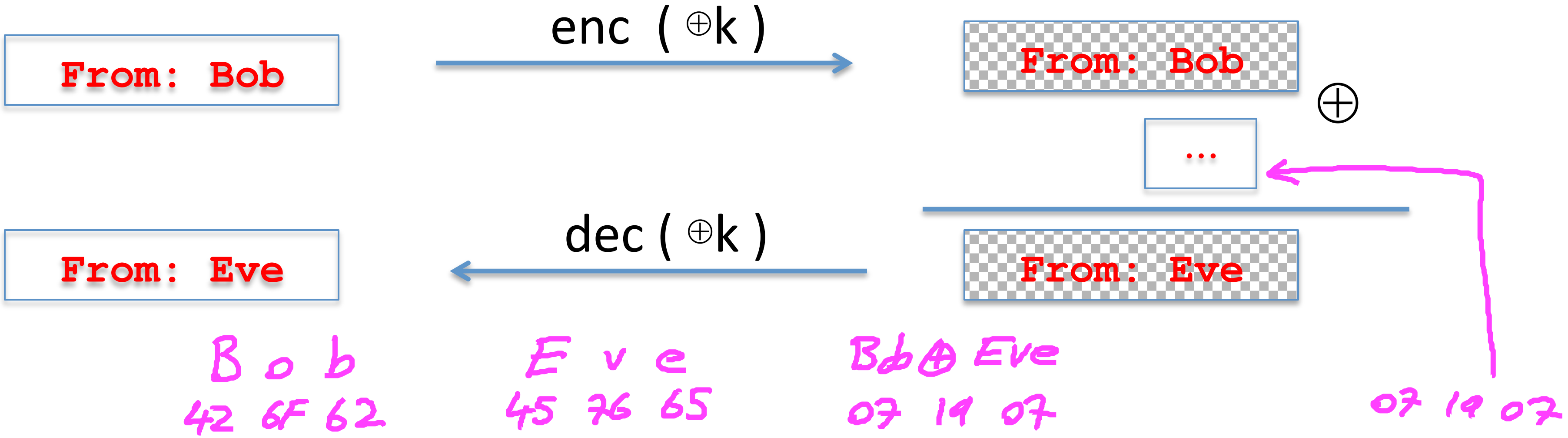
- Disk encryption: typically do not use a stream cipher

Attack 2: no integrity (OTP is malleable)



Modifications to ciphertext are undetected and have **predictable** impact on plaintext

Attack 2: no integrity (OTP is malleable)



Modifications to ciphertext are undetected and have predictable impact on plaintext

End of Segment