Attacks Against One Time Pad

MSc in Information Security & Digital Forensics.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Review

- Cipher over (K,M,C): a pair of "efficient" algs (***E***, ***D***) s.t.

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

- Weak ciphers: subs. cipher, Vigener, …

- A good cipher: **OTP** $M=C=K=\{0,1\}^n$

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

- Lemma: OTP has perfect secrecy (i.e. no CT only attacks)

- Bad news: perfect-secrecy ⇒ key-len ≥ msg-len

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Steam Ciphers : *Making OTP Practical*

Idea: replace “random” key by “pseudorandom” key

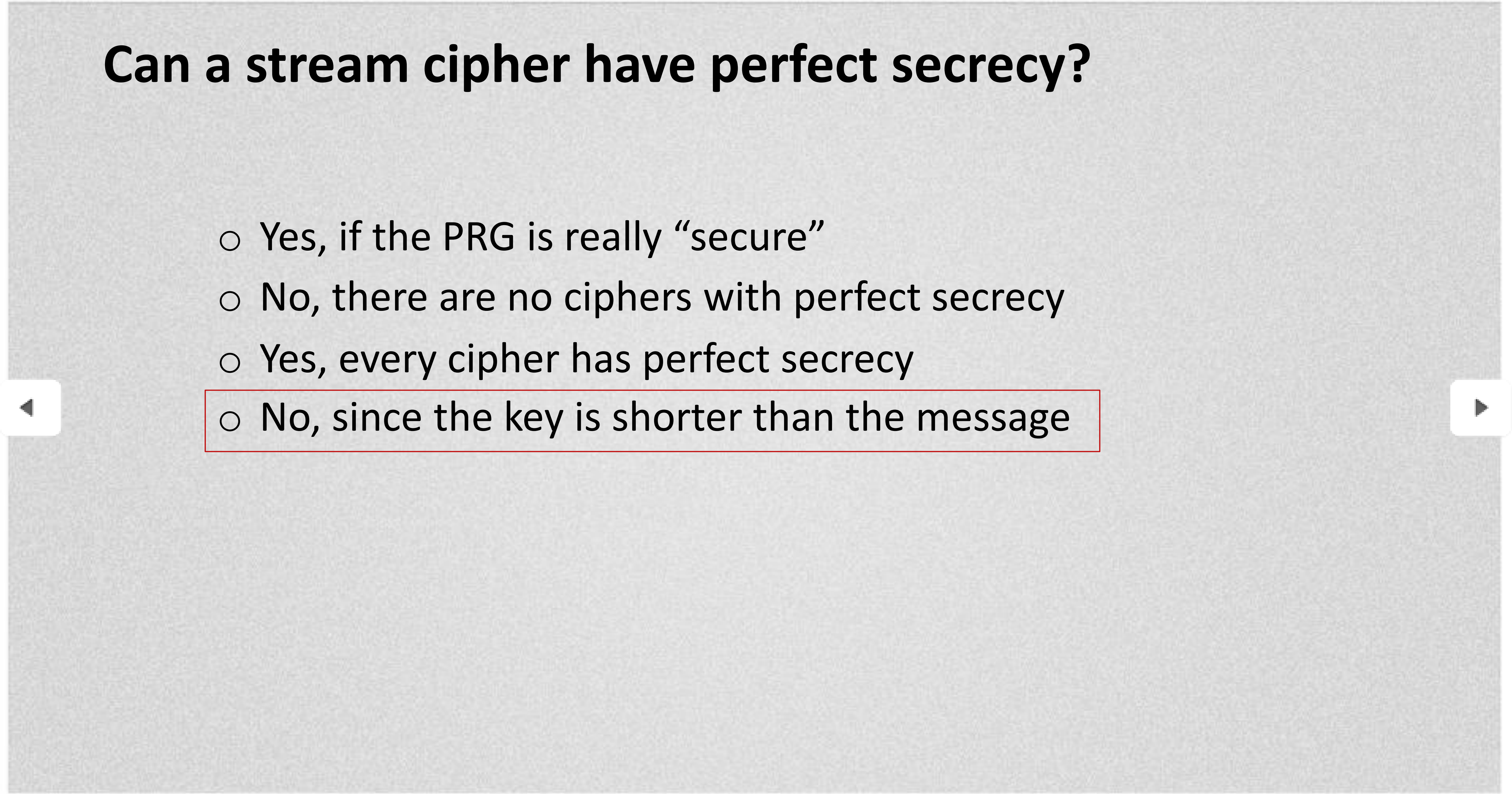
A Pseudo random generator (PRG) take an input (**seed**) and generators a random steam of output.

It is computed by a **deterministic** algorithm.

We basically use the output from our PRG as if it were our key to a OTP.

Real key would have been out input to the PRG, our **seed** and would be much shorter than any key needed for a OTP

Steam Ciphers : Making OTP Practical



Can a stream cipher have perfect secrecy?

○ Yes, if the PRG is really “secure”

○ No, there are no ciphers with perfect secrecy

○ Yes, every cipher has perfect secrecy

[✓ ○ No, since the key is shorter than the message]

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Weak PRGs

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

Security: PRG must be unpredictable

We should never use weak PRGs, as these make the entire stream cipher insecure.

Some weak PRGs are commonly used and should be avoided:

Random(), should never be used for crypto (Kerberos V4)
linear congruential generator

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Attacks on OTP and Stream Ciphers

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:

$$C_1 \oplus C_2 \rightarrow m_1 \oplus m_2$$

Enough redundancy in English and ASCII encoding that:

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

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Real World Examples

- Project Venona
- MS-PPTP   (windows NT)
- 802.11b WEP
- Disk Encryption

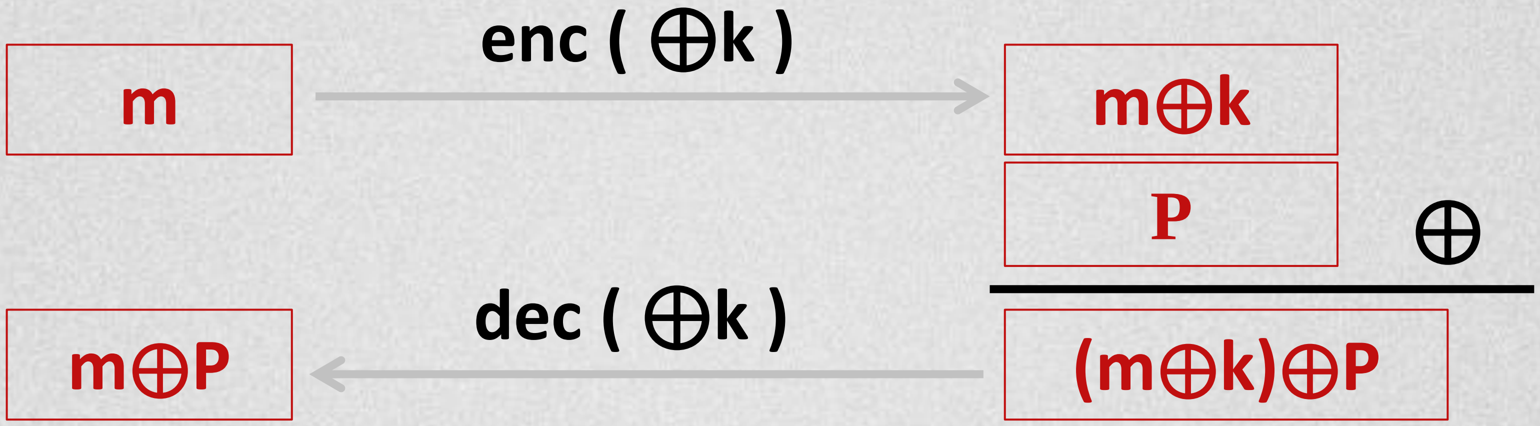
Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

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

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Attack 2: No Integrity (OTP is malleable)

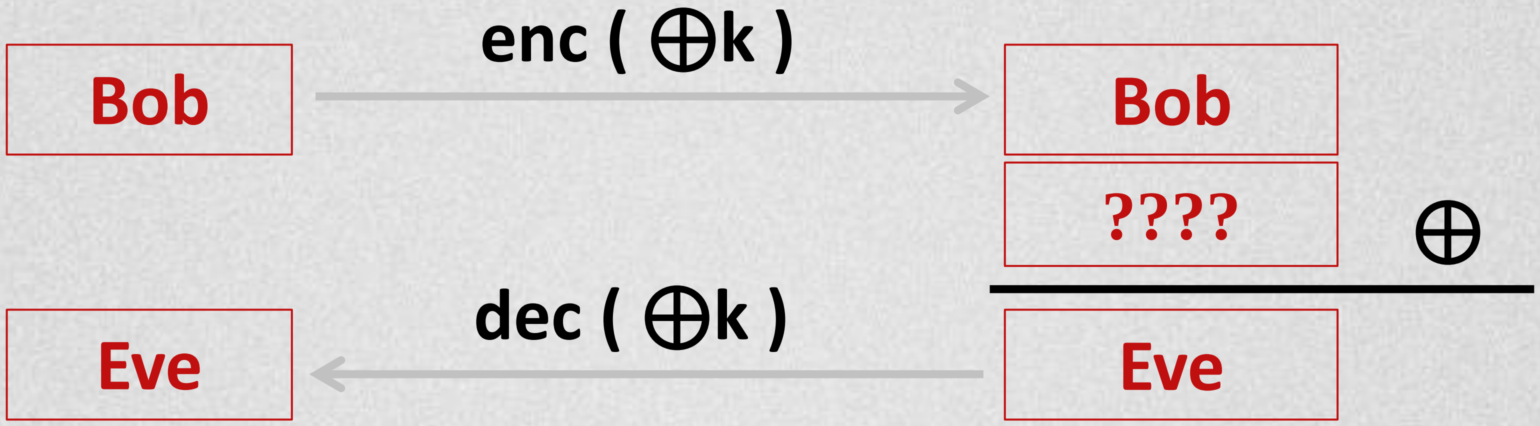


Modifications to ciphertext are undetected and have predictable impact on plaintext

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Attacks on OTP and *Stream Ciphers*

Attack 2: No Integrity (OTP is malleable)



Bob	Eve	Bob ⊕ Eve
42 6f 62	45 76 65	07 19 07

Modifications to ciphertext are undetected and have predictable impact on plaintext

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Thank You !

End of Section

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie