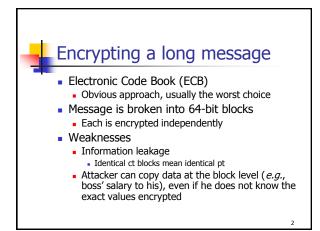
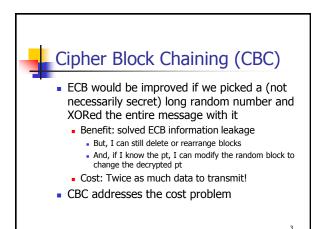
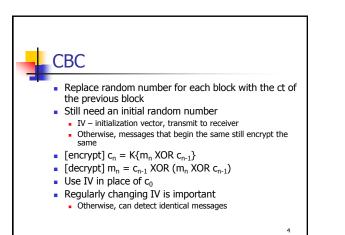
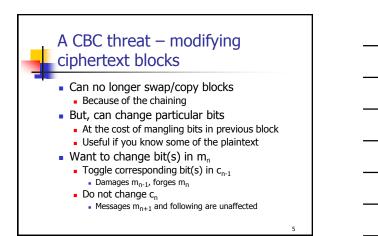
CS-4920: Lecture 8 Modes of operation Reading Chapter 4 Today's Outcomes Explain various methods for applying secret key (block) encryption to a message stream Using secret key techniques to generate MACs (message authentication codes)





© Eric A. Durant, PhD

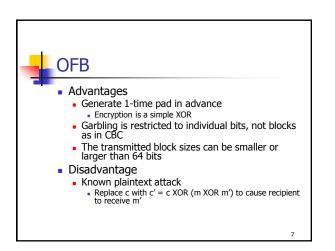


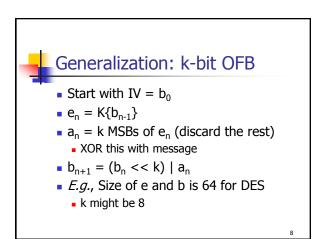


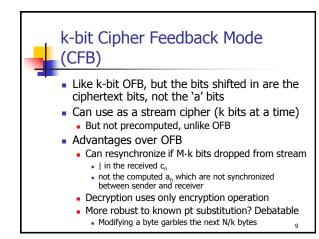


- Converts a block cipher (*e.g.*, DES) into a stream cipher
 - By generating a 1-time pad
- Start with IV = b₀
- $b_{n+1} = K\{b_n\}$
- XOR message with bits as needed before transmission to get ciphertext

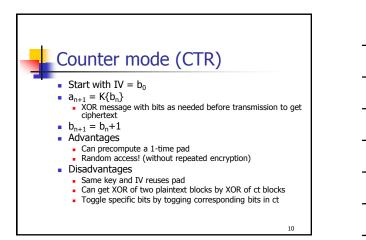
6

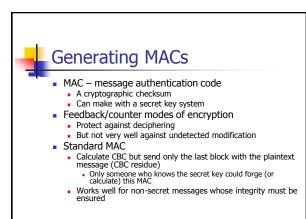






© Eric A. Durant, PhD





11

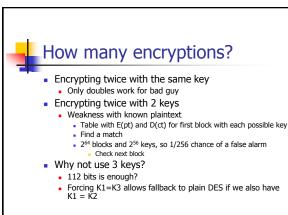
What about confidentiality and integrity together?

- The residue is just the final CBC output, so does this mean we already have C and I? No, if you have the whole CBC stream, integrity is lost – bits may be modified
- There are variations (checksum at end encrypted, ...), but they all have practical or at least theoretical
- weaknesses
- Solutions
 - Separate keys for the CBC stream and residue
 - Related keys are believed secure as well (*e.g.*, XOR with 0xF0F0F0...)
 - Encrypt a cryptographic hash (different than CRC hard to find messages that give the same hash)

12

Multiple encryption DES DES, at 56-bits, may be too weak

- So, do multiple DES passes
- Accepted method is
 - EDE (encrypt-decrypt-encrypt)
 - Also called 3DES
- Only two keys: K₁ and K₂
- Encrypting: Es with K₁, D with K₂



14

13