Selected Comments and Issues

on the July, 2001 draft
“Recommendation for Block Cipher Modes of Operation.”
Many thanks for...

- detailed, helpful comments received so far:
  - Don Johnson, Certicom
  - Miles Smid, Entrust-CygnaCom
  - Phillip Rogaway, University of California at Davis and Chiang Mai University
  - Francois Rousseau, Communications Security Establishment

- Comments accepted until August 31.
General Considerations

• The usual tension:
  – for security, interoperability: restrict options
  – to accommodate current practices: provide flexibility

• Are there issues for which 3DES should be handled differently than AES?

• The goal is to issue the recommendation around the time the AES FIPS is approved.
How to apply CBC-MAC to any Number of Blocks

• Problem with vanilla CBC: Forgeries can be constructed by extending a message with known MAC.

• Draft restricts each key to messages that consist of a fixed number of blocks.

• This restriction is too severe for most applications.
Some Possible Solutions

• XCBC (MAC)
• RMAC
• Double/Triple Encrypt the final block
• Prepend the message with number of blocks
• Truncate the MAC
• Warning to user
• Other solutions?
Messages of Arbitrary Bit Length

- Ciphertext Stealing for CBC?
- XCBC methods for CBC-MAC?
- Padding schemes
  - Out of scope?
  - How many and which should be specified?
  - Recommended or mandatory?
  - Warnings about potential protocol attacks?
Guidance

• Should the document give more systematic guidance in the selection and use of modes?

• NIST is considering whether to develop a separate guidance document
  – might allow for more detailed guidance than is feasible in Phase 1
  – would allow more time for appropriate review
What guidance, specifically?

• Deprecate ECB?
• Discuss advantages and disadvantages of modes? A la Annex A of ISO/IEC 10116?
• Discuss specific applications/environments, e.g., constrained environments?
• Discuss interaction of encryption and authentication? Other protocol issues?
Requirements on IVs

- In CBC and CFB, an adversary that can predict the IVs of messages may obtain information that allows the ciphertexts of certain messages to be distinguished.

- Should IVs for CBC and CFB be required to be unpredictable by an adversary?

- Proposal to set $C_0 = \text{CIPH}_K(\text{IV})$

- What should be the required of IVs in OFB?
Segment Length in CFB Mode

• Draft allows any segment length, $s$, up to the block size

• Should $s$ be limited to a small set of values to limit option proliferation?
  – $\{1, 8, 128\}$ suggested

• Should example vectors be provided for more values of $s$?
Other Comments

- What truncation values of the MAC should be permitted or required?
- Should interleaved modes be described?
- Other comments?