Preliminary Outline of Topics
Second Modes of Operation Workshop
August 24, 2001

The following outline is preliminary and subject to change.

I. Presentation and discussion of modes proposals
   A. authenticated encryption: IAPM, IACBC, OCB, XCBC-XOR, XECB-XOR
   B. authentication: PMAC, RMAC, XCBC, XECB-MAC
   C. confidentiality: 2DEM, ABC, KFB, PCFB

II. Modes for the Internet and other technical comments on modes

III. Comments on the draft NIST Recommendation for modes
   A. adjusting CBC-MAC to handle variable numbers of blocks
   B. padding/other handling of partial blocks
   C. the requirements on IVs for CBC
   D. the level of guidance in the choice and the use of modes

IV. Where do we go from here?
   A. What are the issues?
   B. Other modes
   C. Next steps in the process