S/MIME Updates

Jim Schaad

August Cellars

Seoul, Korea

Issues Left

- List AES-192 explicitly (No)
- Text on deterministic ECDSA?
  - Keep or kill?
- ECDSA P-384 w/ SHA-384 (SHOULD?) – signature and digest
  - (Same fate as AES-192?)
- SHA-3
  - No EdDSA448 right now, so no SHA-3 currently required.

Work Left

- Add security considerations on padding
- Regenerate examples so they are valid messages