Adam Geipel and Walter Verburg

CS455, 9:25 Session

11/10/2015

CS455 Programming Assignment

Part 1:

Content: E(Session key, KBPublic)

Length: 256 bytes

Method: RSA 2048

Part 2:

Content: E(E(MD(nonce + data), K­APrivate), KBPublic)

Length: 32 bytes

Method: SHA 256

Part 3:

Content: E(Nonce + Data, KSession)

Length: Variable

Method: AES 128