CS Capstone - RSA-CRT-2048 with SHA-224

George Wood

? April/May 2018

1

- SHA 224 utilized because FIPS 186-4 reccomends using a hashing algorithm of identical security strength to the key length being used. Larger is sometimes acceptable if disclosed, weaker is NEVER acceptable.