Andrei Oprisan

COMSW4181

HW 1, Problem 1 – Adversarial Thinking

(a) (4)

While a digital signature can only be verified using the public key of the signer, message authentication codes can only be verified through the secret key that was used to generate them. Digital signatures are created with the private key of the owner and thus the underlying message can be verified by anyone using the public key, providing integrity, authentication, and non-repudiation. Message authentication codes do not provide for non-repudiation, meaning the receiver can forge messages, since the keyed hash is included with the message. MACs use symmetric encryption, so the only way to validate message authenticity is to make sure that the private key is secured and used to decrypt the message.