LAB 7

RSA

5 Hand-in 1

Explain the limitation of protocol attack.

It can be prevented with optimal asymmetric encryption padding.

7 Hand-in 2

Explain the purpose of Optimal Asymetric Encryption Padding (OAEP) to encrypt and decrypt using RSA. Explain how it works.

OAEP will prevent RSA from being vulnerable to protocol attack.

OAEP uses a Feistel network with XORs and two hash functions to transform the message before the signature. A nonce is used to give a non-deterministic result as well. This will then be secure when the hash functions are secure.

Explain the purpose of Probabilistic Signature Scheme (PSS) to sign and verify using RSA. Explain how it works.

PSS allows modern methods of security analysis to prove that its security directly relates to the RSA program. It has an appendix which requires the message itself to verify the signature though the message is not recoverable from the signature.

Encryption:

1. Hash the message to be signed.
2. Transform hash into encoded message. This uses padding which is much more random.
3. A signature primitive is applied to the encoded message by using the private key to produce the signature.

Verification:

1. Hash message to be signed with the hash function used during encryption.
2. A verification primitive is then applied to the signature by using the public key of the key pair to recover the message.

3. Verify that the encoded message is a valid transformation of the hash value.