**50.042 FCS Lab 7 Write-up**

**Q: Explain the limitation of protocol attack.**

For RSA encryption protocol attack, this attack is weak against encryptions with introduced randomness, such as the Optimum Asymmetric Encryption Padding (OAEP). OAEP is a stronger padding scheme that uses a Feistel network to transform the message before the signing. It makes use of 2 hash functions the XOR operation, and a nonce in the process. This breaks the deterministic nature of the encryption and thus the attacker cannot just change the message deterministically (without knowing the message) to his intended message, and the integrity of the message is protected.

For the RSA digital signature protocol attack, this does not work on scenarios where the hash of the message is signed instead of the message itself. In such a scenario, let’s say the attacker attempts to carry out the attack the same way. He generates a random signature s’, and computes its corresponding encryption, m’. This m’ is supposedly the hash of the message itself. However, due to the one-wayness property of hash functions, it is difficult (or impossible) to find a pre-image that, when hashed, will produce this (fake) hash m’. Thus this attack is not feasible if the signature is the hash of the message instead of the message itself.

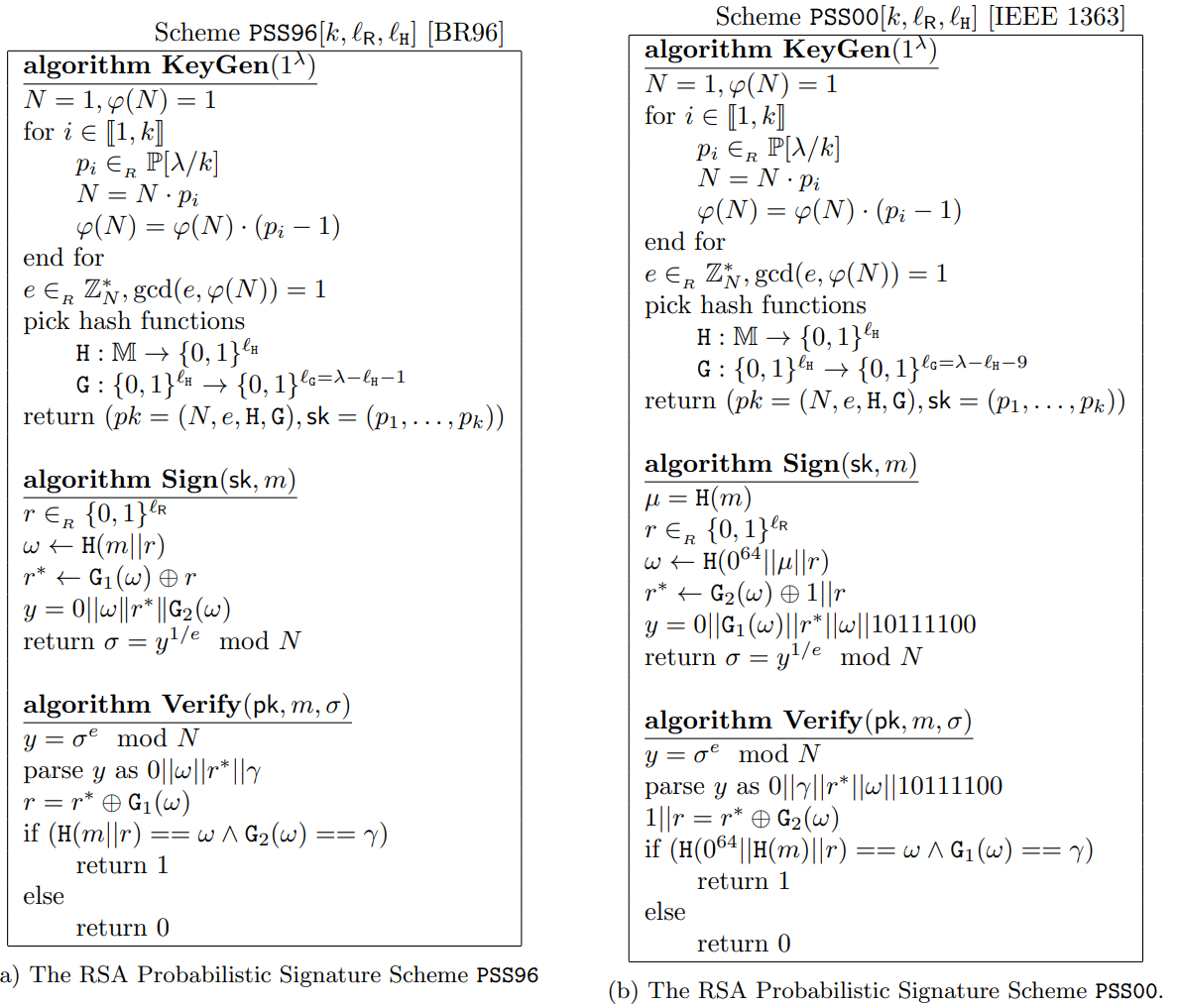
**Q: Explain the purpose of Optimal Asymmetric Encryption Padding (OAEP) to encrypt and decrypt using RSA. Explain how it works.**

OAEP is a stronger padding scheme that uses a Feistel network to transform the message before the signing. It makes use of 2 hash functions and the XOR operation in the process. Then nonce helps to give a non-deterministic result. This breaks the deterministic nature of the encryption so that it prevents encryption protocol attacks. It is proven to be secure under the RSA assumption that G and H are secure.

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

PSS is a signature scheme based on the RSA cryptography system and provides enhanced security. In this scheme, the transform operation uses padding that is much more random. This breaks the deterministic nature of the encryption.

The PSS makes use of a random salt and 2 hash functions, H and G. The signature scheme can be seen in the figure below.



Source: <https://eprint.iacr.org/2019/1268.pdf>