# CSCI471/971 Modern Cryptography

Workshop

# Question-1

**Question 1.** Consider the padded RSA Encryption scheme, where the public key is ⟨ N, e ⟩ as usual, an encryption of an l-bit message m is computed by choosing uniform r and outputting c=(m || r)$^e$ mod N, and the decryption of a ciphertext c first computes m'=c$^d$ mod N and outputs the first l bits of m'. Please show that the scheme is not IND-CCA secure.

This scheme is a variant of PKCS #1 v1.5, which was replaced by RSA-OAEP.

# Question-2

**Question 2.** Consider the padded RSA Signature scheme, where the public key is $\langle N, e \rangle$ as usual, a signature on a an l-bit message m is computed by choosing uniform r and outputting $s=(m \,||\, r)^d$ mod N, and the verification algorithm checks if the first l bits of $s^e$ mod N is m. Please show that the scheme is not secure.

END