MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Security of encrypt-and-sign). *Consider a following message transmission protocol. A sender* $\mathcal{P}_1$ *knows the public encryption key* pk_2 *of a receiver* $\mathcal{P}_2$ *and the receiver* $\mathcal{P}_2$ *knows the public signing key* pk_1 *of the sender* $\mathcal{P}_1$*. To encrypt a message* m *the sender* sk *computes* $c \leftarrow \mathsf{Enc}_{\mathsf{pk}_2}(m)$, $s \leftarrow \mathsf{Sign}_{\mathsf{sk}_1}(c)$ *and sends* (c, s) *over unreliable channel to* $\mathcal{P}_2$*. The receiver* $\mathcal{P}_2$ *first checks the authenticity by computing* $\mathsf{Ver}_{\mathsf{pk}_1}(c, s)$ *and then decrypts the message* $m \leftarrow \mathsf{Dec}_{\mathsf{sk}_2}(c)$*. Prove that the protocol remains secure even if the adversary gets oracle access to the receiver, i.e., it can send any tuples* c, s *and obtain the corresponding decryption.*

Solution. Let us first formalise two games that are analog of IND-CCA2 security games... Next let us prove that the decryption queries will yield $m \neq \perp$ with small enough probability Based on this let us define trivial decryption oracle and reduce the security to IND-CPA games...