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

Exercise (Asymmetric encryption as commitment). *Show that an asymmetric IND-CPA secure cryptosystem* $\mathfrak{C} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with perfect decryption can be converted to perfectly binding and computationally binding commitment by using the following construction:*

$\mathsf{Gen}^\star$

$\lceil (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}$
$\lfloor \textbf{\textit{return}}\ \mathsf{pk}$

$\mathsf{Com}_{\mathsf{pk}}(m)$

$\lceil r \leftarrow \mathcal{R}$
$\lvert c \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m; r)$
$\lfloor \textbf{\textit{return}}\ (c, (m, r))$

$\mathsf{Open}_{\mathsf{pk}}(c, m, r)$

$\lceil \hat{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m; r)$
$\lvert \mathsf{if}\ c = \hat{c}\ \textbf{\textit{return}}\ m$
$\lfloor \mathsf{else}\ \textbf{\textit{return}}\ \perp\ .$

Solution.