WORKFLOW

Client A	**Client B**
known :	**known :**
$K_A(AES)$	$k_{B-public}(RSA)$
	$k_{B-private}(RSA)$

– – – – – – – – – – – – – – – – – – **Digital Signature** –

– – – – – – – – – – – – – **$k_{B\text{-}public}$ can be replace by any info** – – – – – – – – – – – – – – – – – – –

$k_{B-public}$ <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< $k_{B-public}$

$SHA\left(k_{B-public}\right)$ $SHA\left(k_{B-public}\right)$

$\mathcal{D}_{k_{B-private}}\left(SHA\left(k_{B-public}\right)\right)$ <<<<<<<<<<<<<<<<<<<<<<<< $\mathcal{D}_{k_{B-private}}\left(SHA\left(k_{B-public}\right)\right)$

Check : $\mathcal{E}_{k_{B-public}}\left(\mathcal{D}_{k_{B-private}}\left(SHA\left(k_{B-public}\right)\right)\right) == SHA\left(k_{B-public}\right)$??

– – – – – – – – – – – – – – – – – **Info Communication** –

$IV(Initialization\ Vector)$ >>>>>>>>>>>>>>>>>>>>>>>> IV

$\mathcal{E}_{k_{B-public}}\left(K_A\right)$ >> $\mathcal{E}_{k_{B-public}}\left(K_A\right)$

$\mathcal{D}_{k_{B-private}}\left(\mathcal{E}_{k_{B-public}}\left(K_A\right)\right) \rightarrow K_A$

$E_{K_A,IV}\left(Info\right)$ >> $E_{K_A,IV}\left(Info\right)$

$D_{K_A,IV}\left(E_{K_A,IV}\left(Info\right)\right) \rightarrow Info$