WORKFLOW

Client A	Client B
known:	known:
$K_A(AES)$	$k_{B-public}(RSA)$
	$k_{B-private}(RSA)$
Digital S	ignature
k _{B-public} can be rep	lace by any info
$k_{_{ extbf{B} ext{-}public}}$	$\mathcal{L}<<<<<$ $\mathcal{L}_{\mathcal{B} ext{-}public}$
$SHA\Big(k_{B extit{-}public}\Big)$	$SHA\Big(oldsymbol{k}_{\mathcal{B} ext{-}public}\Big)$
$\mathcal{D}_{k_{B ext{-}private}}\!\left(ext{SHA}\!\left(k_{B ext{-}public} ight)\! ight)\!<\!<\!<\!<\!<\!<$	$\mathcal{L}<<<<<\mathcal{D}_{\hat{k}_{B ext{-}private}}\left(\mathit{SHA}\left(\hat{k}_{B ext{-}public} ight) ight)$
$ ext{Check}: \mathcal{E}_{ec{k}_{ ext{B-public}}} \Big(\mathcal{D}_{ec{k}_{ ext{B-private}}} \Big(ext{SHA} \Big(ec{k}_{ ext{B-public}} \Big) \Big)$	$=SHA(k_{B-public})??$
Info Comn	nunication
IV(Initialization Vector)>>>>>>>>>>	>>>>>> IV
$\mathcal{F}_{k_{B ext{-}public}}(K_{A})$ >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	>>>>>> $\mathcal{E}_{k_{B\cdot public}}\left(K_{\scriptscriptstyle A}\right)$
	$\mathscr{D}_{k_{\mathcal{B} ext{-}private}}\!\left(\mathscr{E}_{k_{\mathcal{B} ext{-}public}}\left(K_{A} ight)\! ight)\! ightarrow\!K_{A}$
$E_{K_A,IV}(Info)>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>$	$E_{K_A,IV}$ (Info)
	$D_{K_A,IV}\left(E_{K_A,IV}\left(Info ight) ight) ightarrow Info$