Problem 9): The **DDH** Assumption allows two parties communicating over an encrypted channel to derive a shared value k (*usually for use as a key*) so that, to an eavesdropper, k is indistinguishable from a uniform element of some group $\mathbb{G}$.