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