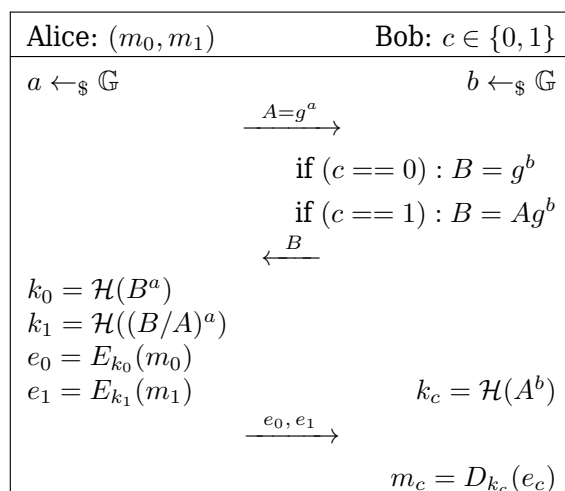


Projekt nr 1

Niech (\mathbb{G}, \cdot) będzie grupą cykliczną rzędu q , a g jej generatorem. Niech $\mathcal{H} : \mathbb{G} \rightarrow \mathbb{G}$ będzie funkcją KDF (key derivation function). Niech (G, E, D) będzie symetrycznym schematem szyfrowania.

1. Zaimplementuj protokół poniższy \mathbf{OT}_1^2



2. Sporządź dokumentację wykorzystanych komponentów protokołu
 - (a) Grupa (\mathbb{G}, \cdot) . Podaj parametry bezpieczeństwa grupy oraz jej zalety i wady ze względu na efektywność obliczeń i bezpieczeństwo.
 - (b) Funkcja KDF. Jakie są jej rekomendacje? Podaj jej zalety i wady ze względu na efektywność obliczeń i bezpieczeństwo.
 - (c) Schemat (G, E, D) . Podaj parametry bezpieczeństwa schematu oraz jego zalety i wady ze względu na efektywność obliczeń i bezpieczeństwo.