Projekt nr 1

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

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

Alice: (m_0, m_1)		Bob: $c \in \{0, 1\}$
$a \leftarrow_\$ \mathbb{G}$		$b \leftarrow_\$ \mathbb{G}$
	$\xrightarrow{A=g^a}$	
		if $(c == 0) : B = g^b$
		if $(c == 1) : B = Ag^b$
	$\xleftarrow{B}$	
$k_0 = \mathcal{H}(B^a)$		
$k_1 = \mathcal{H}((B/A)^a)$		
$e_0 = E_{k_0}(m_0)$		
$e_1 = E_{k_1}(m_1)$		$k_c = \mathcal{H}(A^b)$
	$\xrightarrow{e_0, e_1}$	
		$m_c = D_{k_c}(e_c)$

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.