Egzamin z PPK - przykładowe pytania

1. Wyjaśnij co to są *rekomendacje* (w standardach PKI)?

   Odpowiedź: Jeśli A rekomenduje B to oznacza, że A zaświadcza, że B wydaje wiarygodne certyfikaty.

   Można też dodać, że istnieją rekomendacje wyższych poziomów i wyjaśnić co to znaczy (ale nie jest to konieczne).

2. Przedstaw protokół uzgadniania klucza Diffiego-Hellmana.

   Odpowiedź (jedna z możliwych):
   Niech p będzie liczbą pierwszą i niech γ będzie generatorem Z_p^*. Uczestnikami protokołu są Alicja i Bob.

Alicja		Bob
losuje $a \in \{0, \ldots, p-1\}$	$\xrightarrow{\alpha=\gamma^a}$	
	$\xleftarrow{\beta=\gamma^b}$	losuje $b \in \{0, \ldots, p-1\}$
$K_A := \beta^a$		$K_B := \alpha^b$

   Powinno wyjść: $K_A = K_B$. To jest uzgodniony klucz.