Kryptografia dla informatyków I, 2017/18 10.1.2018

# Kolokwium

*Stefan Dziembowski* MIM UW

**Zadanie 1:**

Podaj definicję symetrucznego schematu szyfrowania bezpiecznego w sensie CPA.

**Zadanie 2:**

Narysuj i krótko objaśnij jak działa 3-rundowa sieć Feistela.

**Zadanie 3:**

Podaj protokół uzgadniania klucza Diffiego-Hellmana.