Kryptografia dla informatyków I, 2017/18 8.2.2018

Egzamin - teoria

Stefan Dziembowski MIM UW

Zadanie 1:

Podaj definicje *zobowiązania bitowego* (ang. *bit commitment scheme*) w różnych wariantach ograniczenia na moc obliczeniową przeciwnika.

Zadanie 2:

Podaj definicję *Transferu Utajnionego Rabina* (ang. *Rabin Oblivious Transfer*) w pasywnym wariancie bezpieczeństwa.