

EGZAMIN POPRAWKOWY

Polecenia i pytania (100p)

1. Podaj definicję *dowodu interaktywnego*.
2. (a) Podaj definicje protokołu *zobowiązania bitowego*.
(b) Podaj przykład implementacji takiego protokołu.
(c) Podaj w jaki sposób można wykorzystać taki protokół do stworzenia protokołu *losowania bitu przez telefon*.
3. Co to znaczy, że przeciwnik (w obliczeniach wielopodmiotowych) jest *aktywny*?
4. Co to jest *kanal rozgłaszający (broadcast channel)*?
5. Co to są *niepokwitowalne* protokoły głosowania?
6. Nieformalnie wyjaśnij co to jest *dowód z desygnowanym weryfaktorem*?
7. Podaj protokół PIR z wykładu (przynajmniej ten o złożoności komunikacyjnej około \sqrt{n} — gdzie n jest rozmiarem bazy danych).
8. Co to są protokoły *ślepych podpisów*? Podaj implementację ślepych podpisów RSA.

Powodzenia!