

1 Punktacja

Osoby które były skrybami dostaną po 40 punktów (niektórzy dopiero po poprawieniu przygotowanych przez siebie notatek).

Na egzaminie jest do zdobycia 100 punktów. Zalicza (60). Na ocenę bardzo dobrą prawdopodobnie będzie potrzeba 90 punktów.

Pracy domowej cały czas nie sprawdziłem (przepraszam, wiem, że tak nie powinno być). Jest za nią maksymalnie 5 punktów.

Osoby które nie były skrybami mają szansę zdobyć (maksymalnie) 30 punktów wykonując pracę wyznaczoną przez wykładowcę. W celu jej przydzielenia proszę zgłaszać się osobiście. Rozmiar (i rodzaj) pracy może zależeć od aktywności na wykładzie i ćwiczeniach.

2 Egzamin

Egzamin odbędzie się 27.01 w godzinach 12.15 – 13:45 w sali 3120.

Egzamin obejmuje materiał z wykładów 1 – 11 (tj. bez wykładów styczniowych).

Na egzaminie nie wolno korzystać z notatek.

Idea jest taka, że jeśli ktoś chodził na wykład i ćwiczenia i w miarę rozumiał co się dzieje, to nie powinien mieć kłopotów z zaliczeniem na dobrą ocenę”

Egzamin będzie się składał z poleceń typu:

1. W paru zdaniach wyjaśnij różnicę między przeciwnikiem aktywnym i pasywnym w MPC (wyjaśnienia zilustruj przykładami).
2. W paru zdaniach wyjaśnij pojęcie *niepokwitowalności* w protokołach głosowania elektronicznego.
3. Nieformalnie wyjaśnij w jaki sposób definiuje się bezpieczeństwo protokołów MPC.
4. Zdefiniuj pojęcie *reenkrypcji* szyfrogramu i pokaż w jaki sposób można jej dokonać w szyfrach homomorficznych.

Za wykonanie poleceń można dostać maksymalnie 100 punktów.

Dodatkowo może pojawić się „zadanie z gwiazdką” (podobne do tych zadań które robiliśmy czasami na ćwiczeniach). Będzie za nie można otrzymać dodatkowe punkty.