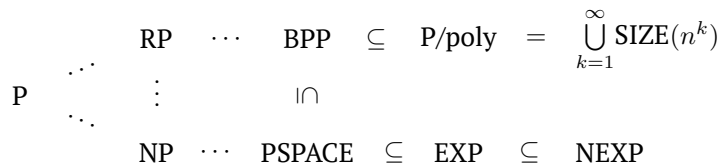


Контрольная работа по теоретической криптографии

Последний срок сдачи письменных ответов — 3 ноября 2021 года.

Указанные баллы «начисляются» при безукоризненном выполнении задания. Существенные недочёты снижают оценку. Итоговый балл, превышающий 10, понижается до 10 в силу особенностей десятибалльной системы оценок.

1. Вставьте в диаграмму вместо многоточий знаки \subseteq , \subsetneq , \supseteq , \supsetneq или $=$, указывающие на соотношения классов сложности:



Выбор знаков обязательно **обоснуйте**.

[1 балл]

2. Пусть f — слабо односторонняя функция, сохраняющая длину ($\forall x \in \mathbb{B}^* |f(x)| = |x|$), а функция g определена так:

$$g(x0) = x0, \quad g(x1) = f(x)1 \quad (x \in \mathbb{B}^*),$$

то есть если строка-аргумент заканчивается на 0, то она не меняется, а если на 1, то она преобразуется в конкатенацию значения функции f от префикса x аргумента и бита 1.

Докажите, что

- g не является сильно односторонней функцией,
- g — слабо односторонняя функция.

[1 балл]

[3 балла]

3. Докажите, что если существует односторонняя функция, то $\text{P} \neq \text{NP}$.

[4 балла]

(Подсказка. Для этого достаточно для односторонней функции f задать язык $L_f \in \text{NP}$, который не принадлежит P . Последнее можно доказать от противного для случая, когда язык L_f состоит, например, из слов, содержащих, кроме значения функции, некоторую информацию о его прообразе. Обратите внимание, что задача обращения односторонней функции — задача поиска и она трудна в среднем, а P и NP определяются для задач распознавания.)

4. Докажите, что если $f : \mathbb{B}^* \rightarrow \mathbb{B}^*$ — односторонняя функция, то для любого полинома $p(\cdot)$ при всех достаточно больших $n \in \mathbb{N}$ мощность образа $f(\mathbb{B}^n)$ больше $p(n)$, то есть

[4 балла]

$$\forall p \exists n_0 \forall n \geq n_0 \quad |\{f(x) : x \in \mathbb{B}^n\}| > p(n).$$

(Подсказка. Можно доказывать от противного, используя тот факт, что из равенства $\sum_{i=1}^n \alpha_i = 1$, где $\alpha_i \in \mathbb{R}$ (α_i — вероятности некоторых событий), следует неравенство $\sum_{i=1}^n \alpha_i^2 \geq \frac{1}{n}$.)