Домашнее задание

1. Известны открытые ключи Алисы $(107, 187)$ и Боба $(7, 253)$. Алиса хочет послать сообщение 17 Бобу и подписать его своей подписью. Вычислите зашифрованное сообщение Алисы и его цифровую подпись.

2. Вы хотите, чтоб некто М подписал своей электронной подписью сообщение х. Однако, очевидно, вы не добьётесь результата, послав М сообщение х, поскольку оно выглядит подозрительно. Однако, пусть (e, n) открытый ключ М, а (d, n) — его секретный ключ (d вам неизвестно).

Возьмём случайное число r по модулю n и составим сообщение $y = r^e x \pmod n$. Предположим, что y выглядит достаточно невинно, для того, чтобы М согласился подписать y своей электронной подписью и переслать вам подписанную версию: s_y. Если M подпишет сообщение, то как по подписанному сообщению s_y и известным вам данным получить правильную подпись для сообщения x?

3. Алиса и три её друга используют криптосистему RSA. При этом её друзья используют открытые ключи $(N_i, 3)$ с возведением в степень 3, и $N_i = p_i q_i$ для случайно выбранных n-битовых простых чисел p_i и q_i. Покажите, что если Алиса пошлёт одно и то же n-битовое сообщение M всем троим, то перехватившая все три закодированных сообщения Ева (и знающая открытые ключи) сможет быстро (полиномиально) восстановить M.
Указания. Пусть модули попарно взаимнопросты. Как, зная зашифрованные сообщения, получить значение $M^3 \pmod{N_1 N_2 N_3}$?

4. Ева решила подобрать секретный ключ Алисы (d, N) с помощью вероятности: она выбирает случайное число от 2 до $N - 1$ и проверяет, подходит ли оно на роль d за полиномиальное время. Оцените ассимптотически математическое ожидание числа попыток Евы. Является ли её алгоритм более эффективным (в среднем), чем полный перебор?

5. Докажите, что алгоритм, заданный псевдокодом строит случайное m-элементное подмножество множества $\{1, \dots, n\}$. То есть, что `RandomSample(`*m, n*`)` равновероятно возвращает каждое m-элементное подмножество, в предположении, что `Random(`*1,n*`)` случайная величина, возвращающая с равной вероятностью числа от 1 до n.

```
Function RandomSample(m, n) :
    if m == 0 then
        return ∅
    else
        S = RandomSample(m − 1, n − 1);
        i = Random(1, n);
        if i ∈ S then
            return S ∪ {n}
        else
            return S ∪ {i}
        end
    end
end
```

6. Рандомизированный алгоритм поиска k-й порядковой статистики на каждом шаге делает partition по случайному элементу отрезка массива (если в нём более одного элемента) и рекурсивно вызывается либо для левого, либо для правого отрезка получившегося разбиения. Докажите, что математическое ожидание времени работы алгоритма есть $O(n)$, используя анализ индикаторных случайных величин $X_{i,j,k}$, возвращающих 1, если i-я порядковая статистика массива сравнивалась с j-й (при поиске k-й порядковой статистики).

Указания.

1. Получите явную формулу для $\mathrm{E}[X_{i,j,k}]$.

2. Пусть X_k — случайная величина, возвращающая число всех сравнений при поиске k-й порядковой статистики. Покажите, что

$$\mathrm{E}\left[X_k\right] \leqslant 2\left(\sum_{i=1}^{k}\sum_{j=k}^{n}\frac{1}{j-i+1} + \sum_{j=k+1}^{n}\frac{j-k-1}{j-k+1} + \sum_{i=1}^{k-2}\frac{k-i-1}{k-i+1}\right)$$

3. Докажите $\mathrm{E}[X_{i,j,k}] \leqslant 4n$.