	Группа 531 КНиИТ (Криптографические протоколы)	
	531 группа, 1 подгруппа.	Задание 4
1	Богатова Екатерина Дмитриевна	Схема подписи DSA.
2	Дусалиев Тахир Ахатович	Неоспаримая цифровая подпись (Дэвид Чаум).
3	Змéева Вероника Александровна	Аутентификация по программе SKEY (на основе однонаправленных функций)
4	Иванова Ксения Владиславовна	Доказательство с нулевым разглашением изоморфизма графов
5	Ка́йдышева Дарья Сергеевна	Доказательство с нулевым разглашением гамильтоновости графа
6	Костéнко Владислав Денисович	Схема аутентификации Фейге – Фиата – Шамира
7	Кузнецов Егор Дмитриевич	Схема аутентификации Гиллу – Кискате
8	Мызников Сергей Анатольевич	Протокол аутентификации Шнорра
9	Назаров Кирилл Дмитриевич	Схема подписи Фиата – Шамира.
10	Сенокóсов Владимир Владимирович	Схема подписи Гиллу – Кискате.
11	Сергеев Сергей Евгеньевич	Схема подписи Шнорра.
12	У́хов Александр Андреевич	Схема подписи Эль – Гамаля.

Литература:

1. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. (есть на кафедре, но можно скачать и в электронном виде)

Требования к выполненному заданию

1. Наличие описания выбранной интерпретации заданного протокола, лучше сделать в pdf-формате.
2. Большинство протоколов требуют предварительные вычисления ОБЩИХ данных и ИНДИВИДУАЛЬНЫХ данных участников протокола. Поэтому эти процедуры должны быть учтены до начала исполнения основного тела протокола.
3. Разбиение протокола на МИНИМАЛЬНОЕ число блоков, каждый из которых будет предназначен для выполнения с помощью одной (отдельной) программы, либо подпрограммы, либо процедуры. Причём минимальное число этих блоков должно быть ДОСТАТОЧНЫМ для корректного проведения протокола.
4. Для отчёта заранее заготовьте необходимые файлы входных параметров, чтобы не тратить время на их генерацию, например, какое-то сообщение достаточного размера, которое будем разбивать или подписывать и т.д.