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

Литература:

2. 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.