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

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.