

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