

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

#### Литература:

- 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

- Наличие описания выбранной интерпретации заданного протокола, лучше сделать в pdf-формате.
- Большинство протоколов требуют предварительные вычисления ОБЩИХ данных и ИНДИВИДУАЛЬНЫХ данных участников протокола. Поэтому эти процедуры должны быть учтены до начала исполнения основного тела протокола.
- 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.
- 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.