	Группа 531 КНиИТ (Криптографические протоколы)	
	531 группа	Задание 5
1	Антипин Алексей (2)	Схема аутентификации Фейге – Фиата – Шамира
2	Афанасенко Кирилл (1)	Схема аутентификации Гиллу – Кискате
3	Гаврилова Виктория (2)	Протокол аутентификации Шнорра
4	Коннова Анна (2)	Схема подписи Фиата – Шамира.
5	Конюшенко Александра (2)	Схема подписи Гиллу – Кискате.
6	Краснобаев Александр (1)	Схема подписи Шнорра.
7	Латанов Кирилл (1)	Схема подписи Эль – Гамаля.
8	Маскаев Владимир (2)	Схема подписи DSA.
9	Минуситов Амиль (1)	Неоспаримая цифровая подпись (Дэвид Чаум).
10	Мязин Александр (1)	Подпись с доверенным лицом.
11	Пронин Никита (1)	Протокол Диффи – Хельмана.
12	Сажина Елизавета (2)	Векторная схема Джорджа Блэкли (George Blakley), деление по гиперплоскостям.
13	Старичков Павел (1)	(m, n)-пороговая схема Асмута – Блума на основе Греко – Китайской теоремы об остатках.
14	Ступин Артём (1)	Бросание монет с помощью квадратичных корней.
15	Таран Александр (2)	Бросание монет с помощью модулярного возведения в степень.
16	Тихонова Мария (2)	Мысленный покер с тремя игроками.
17	Цуканов Илья (2)	Аутентификация по программе SKEY (на основе однонаправленных функций)
18	Швецова Елизавета (2)	Раскрытие секретов «всё или ничего»
19	Юрченко Елена (2)	Однонаправленный сумматор.

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

5. Наличие описания выбранной интерпретации заданного протокола, лучше сделать в pdf-формате.
6. Большинство протоколов требуют предварительные вычисления ОБЩИХ данных и ИНДИВИДУАЛЬНЫХ данных участников протокола. Поэтому эти процедуры должны быть учтены до начала исполнения основного тела протокола.
7. 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.
8. 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.