	Группа 531 КНиИТ (Криптографические протоколы)	
	531 группа	Задание 3 (до 24.10.2022)
1	Антипин Алексей (2)	Мысленный покер с тремя игроками.
2	Афанасенко Кирилл (1)	Аутентификация по программе SKEY (на основе однонаправленных функций)
3	Гаврилова Виктория (2)	Доказательство с нулевым разглашением изоморфизма графов
4	Коннова Анна (2)	Доказательство с нулевым разглашением гамильтоновости графа
5	Конюшенко Александра (2)	Схема аутентификации Фейге – Фиата – Шамира
6	Краснобаев Александр (1)	Схема аутентификации Гиллу – Кискате
7	Латанов Кирилл (1)	Протокол аутентификации Шнорра
8	Маскаев Владимир (2)	Схема подписи Фиата – Шамира.
9	Минуситов Амиль (1)	Схема подписи Гиллу – Кискате.
10	Мязин Александр (1)	Схема подписи Шнорра.
11	Пронин Никита (1)	Схема подписи Эль – Гамаля.
12	Сажина Елизавета (2)	Схема подписи DSA.
13	Старичков Павел (1)	Неоспаримая цифровая подпись (Дэвид Чаум).
14	Ступин Артём (1)	Подпись с доверенным лицом.
15	Таран Александр (2)	Протокол Диффи – Хельмана.
16	Тихонова Мария (2)	Векторная схема Джорджа Блэкли (George Blakley), деление по гиперплоскостям.
17	Цуканов Илья (2)	(m, n)-пороговая схема Асмута – Блума на основе Греко – Китайской теоремы об остатках.
18	Швецова Елизавета (2)	Бросание монет с помощью квадратичных корней.
19	Юрченко Елена (2)	Бросание монет с помощью модулярного возведения в степень.

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.