**Лаб. раб. № 1. Часть I.**

Задание: Разработка библиотеки примитивов, реализующих арифметические операции в одномодульной системе вычетов. Разработать контрольные примеры.

**Лаб. раб. № 1. Часть II.**

Задание: Реализовать примитивы прямого и обратного преобразования простейшей симметричной криптографической системы. Разработать контрольные примеры.

**Лаб. раб. № 1. Часть III.**

Задание: Реализовать атаку на простейшую симметричную криптосистему методом сужения.

1. **Тип криптографического преобразования:**
   1. схема Цезаря;
2. **Разрядность слова сообщения:**
   1. 8 бит;
3. **Тип основного ключа:**
   1. периодический;
4. **Метод криптоанализа:**
   1. метод сужения;
5. **Ограничения на алфавит сообщения:**
   1. ПС, ВК, ЗП, Ц, английские и русские в альтернативной кодировке заглавные буквы;
6. **Ограничения на алфавит основного ключа**
   1. Ц, английские буквы;
7. **Ограничения на линейную конгруэнтную последовательность (на модуль ЛКДПСЧ)**
   1. нет.