1. В чем заключается основная идея криптографических преобразований

на основе шифров замены?

2. Привести классификационные признаки и дать сравнительную характеристику разновидностям подстановочных шифров.

3. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?

4. Найти ключ шифра, с помощью которого получен шифртекст:

‘byajhvfwbjyyfzgjcktljdfntkmyjcnm’.

5. Расшифровать (с демонстрацией каждого шага алгоритма) текст Сi =

= ‘qrscqcocqclc’, зашифрованный аффинным шифром Цезаря при N =26, а = 3,

b = 5.

6. Зашифровать и расшифровать свою фамилию (на основе кириллицы),

используя аффинный шифр Цезаря.

7. Можно ли использовать в качестве ключевого в шифре Виженера слово,

равное по длине открытому тексту? Обосновать ответ.

8. По какому признаку можно определить, что текст зашифрован шифром

Плейфера?

9. Имеются ли предпочтения в выборе размеров таблицы Трисемуса для

виртуального алфавита мощностью 40: 4х10? 10х4? 5х8? 8х5? 2х20? 20х2?

10. Охарактеризовать основные виды атак на шифры.

11. Сравнить криптостойкость шифра Цезаря и шифра Виженера.

12. Охарактеризовать основные методы взлома подстановочных шифров.