1. При шифровании 11-битовой строки сначала выполняется кодирование циклическим кодом с порождающим многочленом $1+x+x^4$, а затем производится шифрование полученной 15-битовой строки с помощью шифра Виженера с длиной ключа $p \in \{2, 3, 4, ..., 15\}$ (все ключи данной длины равновероятны). При каких p вероятность успеха атаки имитации против такой криптосистемы максимальная. (Выдать список значений через запятую)

   Ответ: 3,5.

   Решение. Отождествим векторы длины 15 с многочленами над двухэлементным полем степени не выше 14.

   При $p = 3$ шифрование шифром Виженера это добавление линейной комбинации многочленов $1 + x^3 + x^6 + x^9 + x^{12}$, $x + x^4 + x^7 + x^{10} + x^{13}$ и $x^2 + x^5 + x^8 + x^{11} + x^{14}$. Но все три этих многочлена кратны $1 + x + x^4$, а значит, являются кодовыми словами. Следовательно, множество криптограмм совпадает с множеством открытых текстов и вероятность успеха атаки имитации равна 1.

   При $p = 5$, аналогично, поскольку $1 + x^5 + x^{10}$ кратен $1 + x + x^4$.

   При $p \notin \{3, 5\}$ соответствующие многочлены не являются кодовыми словами, следовательно, выбор ключа задает выбор смежного класса по коду, а значит вероятность успеха атаки имитации строго меньше 1.

2. При шифровании 5-битовой строки (все такие строки равновероятны) сначала добавляется 000, 001, 011 или 111 так, чтобы количество единичек в полученной 8-битовой строке стало кратно 4, а затем к полученной 8-битовой строке применяется одноразовый щит (все ключи равновероятны). Найдите вероятность успешной подмены для такого шифра.

   Ответ: 5/8.

   Решение. Каждая криптограмма может быть получена из каждого из 32 допустимых (т.е. построенных как описано в уловии) веторов длины 8. Следовательно, каждая криптограмма может быть расшифрована на 32 ключах.

   Поменяем в полученной криптограмме 5 первых битов и 7-й бит, т.е. добавим 11111010. Имеется 20 допустимых векторов, в которых среди первых 5 битов 2 или 3 единицы. Значит с вероятностью 5/8 в открытом тексте среди первых 5 битов 2 или 3 единицы. Если их 2, то окончание в 6-м, 7-м и 8-м битах 011, если из 3, то окончание 001. В обоих случаях добавление 11111010 к допустимому слову дает допустимое слово. Таким образом вероятность успеха подмены не менее 5/8.

   Для доказательства оценки сверху следует заметить, что множество ключей, расшифровывающих пару криптограмм c_1 и c_2 равно по мощности множеству ключей, расшифровывающих пару криптограмм 0 и $c_1 \oplus c_2$. Множество ключей, расшифровывающих пару криптограмм 0 и c совпадает с множеством $U(c)$ допустимых векторов, остающихся допустимыми после добавления c. Теперь перебирая, трехбитовые окончания x вектора c получим, что при $x \neq 010$ множество $U(c)$ содержит не более 16 векторов, то же верно и если $x = 010$, но $s \neq 11111010$.