Московский физико-технический институт(национальный исследовательский университет)		
Кафедра радиотехники и систем управления		
Контрольная работа: Защита информации	10 октября 2020 года	Билет № 1
Ф.И.О.	Гр.№	Сем.

0. Укажите в заголовке билета свои данные (фамилию, имя, отчество, группу, фамилию семинариста). Отсутствие указанных данных равносильно отсутствию работы. Работа должна быть выполнена чистым и аккуратным подчерком. В конце решения каждой задачи должны быть отдельно выписаны ответы.

1. Рассмотрите множество паролей, состоящих из 9 строчных и заглавных латинских букв, а также цифр.

   - каков размер этого множества?
   - сколько времени потребуется на взлом шифротекста, зашифрованного данным паролем, если предположить, что во взломе участвуют все компьютеры мира (7 млрд.), а средний компьютер перебирает 10^5 паролей в секунду?
   - каковы затраты электроэнергии в денежном эквиваленте, если средний компьютер потребляет мощность 400 Вт, а стоимость 1 кВт/час составляет 5 рублей?

2. Источник открытого текста характеризуется случайной величиной X, принимающей два значения x_1 и x_2 с вероятностями $p(x = x_1) = 1/6$ и $p(x = x_2) = 5/6$ соответственно. Источник ключей характеризуется случайной величиной Z, независимой от величины X, принимающей два значения z_1 и z_2 с вероятностями $p(z = z_1) = 1/5$ и $p(z = z_2) = 4/5$ соответственно. Функция шифрования $E_z(x)$ задаётся следующими правилами: $(x_1, z_1) \longrightarrow y_1, (x_1, z_2) \longrightarrow y_2, (x_2, z_1) \longrightarrow y_2, (x_2, z_2) \longrightarrow y_1$.

   a) Найдите собственную информацию каждого из сообщений открытого текста в битах
   b) Найдите энтропию источника сообщений, источника ключей и шифротекста в битах
   c) Найдите взаимную информацию открытого текста и ключа в битах
   d) Найдите взаимную информацию открытого текста и шифротекста в битах
   e) Найдите взаимную информацию ключа и шифротекста в битах
   f) Найдите апостериорное распределение вероятностей открытого текста для обоих вариантов перехваченных злоумышленником шифротекстов y_1 и y_2.

   Используя вычисленные значения, определите, является ли данная шифросистема абсолютно надёжной. Если нет, то что в данной криптосистеме необходимо поменять? Покажите, что апостериорные вероятности после доработки будут удовлетворять необходимым требованиям абсолютно надёжной криптосистемы.

3. Вычислить в поле Галуа GF (256), $m(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$, следующее значение: $222 \cdot 125 + 241^2$. Многочлены заданы как десятичное представление двоичных коэффициентов, свободный член многочлена соответствует самой младшей цифре двоичного представления. В ответе привести в десятичном представлении результаты умножения, возведения в степень и сложения.

4. Вычислить в поле Галуа $GF(25)$,$m(x) = x^2 + 3$, следующее значение: $22 \cdot 9 + 7^2$. Многочлены заданы как десятичное представление пятиричных коэффициентов, свободный член многочлена соответствует самой младшей цифре пятиричного представления. В ответе привести в десятичном представлении результаты умножения, возведения в степень и сложения.

5. Используя алгоритм быстрого возведения в степень (с помощью разложения показателя степени по степеням двойки) вычислить $224^{275}\ mod\ 257$. Указать выполненные промежуточные операции и их результат. Просто ответ в виде числа не засчитывается за правильный.

6. Привести следующие два элемента последовательности, сформированной линейным конгруэнтным методом, если предыдущие 3 элемента последовательности такие: $271, 127, 179$, а все вычисления выполняются в поле F_{499}.

7. Приведите предыдущие 5 бит выхода генератора псевдослучайной последовательности, основанного на регистре сдвига с линейной обратной связью, если известно, что характеристический полином регистра — $m(x) = x^5 + x^3 + x^2 + x + 1$, а дальнейшая последовательность такова: $1, 0, 0, 0, 1, 0$. Генератор приведен на рисунке.

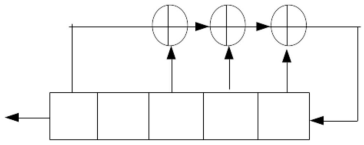

Рис. 1: Регистр сдвига с линейной обратной связью

8. Приведите выходную последовательность шифра, если открытый текст равен $M = 01010110$, ключ $K = 11001011$ сам шифр выглядит как $C = S((M \boxplus K\ mod 2^8) << 3)$, где $\boxplus mod 2^8$ – двоичное суммирование с переносом (старший бит теряется). $<< 3$ – битовый циклический сдвиг влево на 3 бита, S – блоки подстановок, каждый из которых заменяет 4 бита значением, находящимся в соответствующей ячейке.

   $S_1 = 1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12$ – применяется к старшим 4 битам.
   $S_2 = 14, 11, 4, 12, 13, 6, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9$ – применяется к младшим 4 битам.