Контрольная работа

Методические указания и задание на выполнение контрольной работы

Требуется выполнить контрольную работу, соответствующую шестой главе лекционного курса. Прежде чем приступать к выполнению контрольной работы, необходимо изучить соответствующую главу и получить оценку «зачтено» по всем лабораторным работам. Задание на контрольную работу представляет собой одну задачу с различными параметрами, заданными по вариантам.

> Вариант задания на контрольную работу выбирается в соответствии последней цифрой пароля.

Требования к оформлению отчета

Для проверки контрольной работы необходимо представить:

1. Файл с текстом программы (программ);
2. Файл с результатами.
3. Файл (отчет) с текстовым описанием работы программы, который должен содержать описание алгоритма работы программы по шагам с указанием выбранных значений параметров.

Если программа написана в соответствии с заданием, в ней нет ошибок, и получен правильный результат ее работы, включая полный и содержательный отчет, то обучающийся получает оценку «отлично» по курсовой работе.

Тема: Доказательства с нулевым знанием

Задание:

Выполнить компьютерную реализацию протокола «Задачи о нахождении гамильтонова цикла в графе», используя пример 6.2 (стр. 124 лекций). Номер варианта Z равен последней цифре номера пароля.

Параметры, выбираемые по варианту Z:

1) Случайную нумерацию вершин, используемую в алгоритме (изначально в примере она равна 7 4 5 3 1 2 8 6), необходимо изменить по формуле ((a+Z)mod 9), где a – это цифра исходной последовательности случайных номеров вершин.

2) Необходимые в алгоритме параметры схемы RSA вычислить, используя значения P и Q по вариантам:

1. Для Z=0: P=11 Q=53;
2. Для Z=1: P=13 Q=47;
3. Для Z=2: P=17 Q=43;
4. Для Z=3: P=19 Q=41;
5. Для Z=4: P=23 Q=37;
6. Для Z=5: P=31 Q=11;
7. Для Z=6: P=43 Q=13;
8. Для Z=7: P=53 Q=17;
9. Для Z=8: P=11 Q=23;
0. Для Z=9: P=13 Q=37;

Программу необходимо реализовать с помощью любой среды визуального программирования под Windows. Обязательным требованием также является вывод всех промежуточных результатов, таких как матрица смежности, гамильтонов цикл, изоморфный граф, закодированная матрица, зашифрованная матрица, посылаемые вопросы и ответы Алисы и Боба.