Атака на криптосистему Мак-Элиса, построенную на кодах Рида—Маллера

Требования к программе

Режим 1. На вход подаются параметры

1. r - цело число, степень кода $RM(r, m)$,
2. m - целое число число переменных кода $RM(r, m)$.

Программа записывает в файлы открытый и секретный ключи кода Рида—Маллера.

Режим 2. На вход подаётся файл открытого ключа криптосистемы.

Программа должна, используя атаку Миндера—Шокроллахи, вычислить секретный ключ криптосистемы.

Режим 3. На вход подаётся файл открытого ключа и файл секретного ключа криптосистемы.

Программа должна проверить соответствует ли секретный ключ открытому и выдать на экран true, если файл секретного ключа соответствует открытому ключу, и false — иначе.

Предпочтительный язык программирования — python или golang. В случае использования другого языка нужно создать простую сборочную систему на основе make-файлов для трёх операционных системы: Windows 10, MacOS 10.15+, Linux.

Требования к выполнению задания и принцип его оценивания.

1. Предполагается, что к программе будет приложен файл пояснительной записки с форматов файлов секретных и открытых ключей. Влад в оценку — 10 %.
2. Оценивается правильность работы программы (вклад в оценку — 85 %) и её эргономика (вклад в оценку — 5 %).
3. Плагиат кода — обнуляет выполнение задачи. И она не засчитывается. Плагиатом не является любое заимствование с указанием его авторства. Заимствованный участок кода не включается в оценивание. Например, Вы не смогли реализовать функцию и заимствовали её у друга, указав это в программе.

Реализация этой функции исключается из вклада в оценку правильности работы программы на основе «важности» (принципиальности) этой функции в программе. Важность вещь разумно-субъективная, определяемая лектором курса. Так, если Вы заимствовали функцию построения кода Рида—Маллера, то, ясно, что это важная функция, т. к. она проверяет знания по теме курса. И её вклад может быть до 30 % вклада кода программы в оценку. В этом случае, этот вклад вычитается из общего вклада в 85 % и получается 55 % вклада программы. Если же была заимствована функция реализации интерфейса командной строки, то она не относится к тем функциям, которые призваны проверить знания по курсу, поэтому её принципиальность может быть оценена не более, чем в 5 %.

4. Для получения оценки «отлично» нужно выполнить задание более, чем на 79 %, оценка «хорошо» ставится за выполнение на 65 % — 79 %, за 50 % — 65 % — «тройка», и при выполнении задания менее, чем на 50 % ставится — «неудовлетворительно». Зачёт по курсу ставится за не менее, чем 70% выполнение задания.