расписания, просматривать и редактировать его. Ключевыми особенностями являются возможности просмотра статистических данных о затраченном времени преподавателя и выставления степени важности и срочности задачи.

Список использованных источников:

1. [Электронный ресурс]. – Электронные данные. – Режим доступа: https://kinderklub.ru/professiya-uchitel/upravlenie-vremenem-kak-instrument-prepodavatelya/.
2. Википедия [Электронный ресурс]. – Электронные данные. – Режим доступа: https://ru.wikipedia.org/wiki/Управление_временем.

ПРОГРАММНОЕ СРЕДСТВО «KASISKI-BABBAGE FREQUENCY ANALYSIS»

Биткин Н.С., Болтак С.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Болтак С.В. – ассистент

Современные криптосистемы отличаются своим многообразием, уровнем криптостойкости и сложностью понимания. Поэтому начинающему криптографу необходим более простой и понятный пример для ознакомления с огромным миром шифров и методов взлома. Разработанный программный продукт позволяет провести криптоанализ шифротекста, зашифрованного шифром Виженера с прогрессивным способом генерации ключевой последовательности.

Шифр Виженера может использовать так называемый прогрессивный ключ (дублирование ключевого слова осуществляется с одновременным сдвигом букв ключа на одну позицию при каждом новом повторении) [1]. В этом случае задача взлома становится не совсем тривиальной.

В алгоритм взлома необходимо внести следующие изменения: повторяющиеся последовательности необходимо учитывать только в позициях, чьи номера кратны длине алфавита исходного текста (это очевидно, так как минимально необходимое количество сдвигов ключа для получения исходного равняется мощности алфавита).

Данная работа представляет собой анализ возможностей метода Касиски-Бэббиджа при атаке шифротекста, полученного с использованием шифра Виженера с прогрессивным ключом. Средняя скорость обработки – порядка миллиона символов в минуту. Исходя из полученных результатов можно сделать следующие выводы:

1) метод абсолютно неэффективен на шифротексте, длина которого не превышает произведение мощности алфавита на длину ключа;
2) при достижении определённых размеров шифротекста метод взлома позволяет получить результат с вероятностью более 90% для ключа любой длины;
3) при повторном шифровании ранее зашифрованного текста вероятность успеха стремится к нулю, тоже самое касается шифрования текста, не имеющего смысла;
4) научно-популярная литература более устойчива к рассматриваемой атаке. Из-за насыщенности таких текстов терминами, которые в большинстве своём являются словами с большим количеством букв, вероятность совпадения последовательностей меньше;

Разработанное программное средство позволяет наглядно продемонстрировать работу метода Касиски-Бэббиджа на шифротексте, полученном шифром Виженера с прогрессивным ключом. Как видно из рисунка 1, успешность взлома зависит от длины шифротекста.

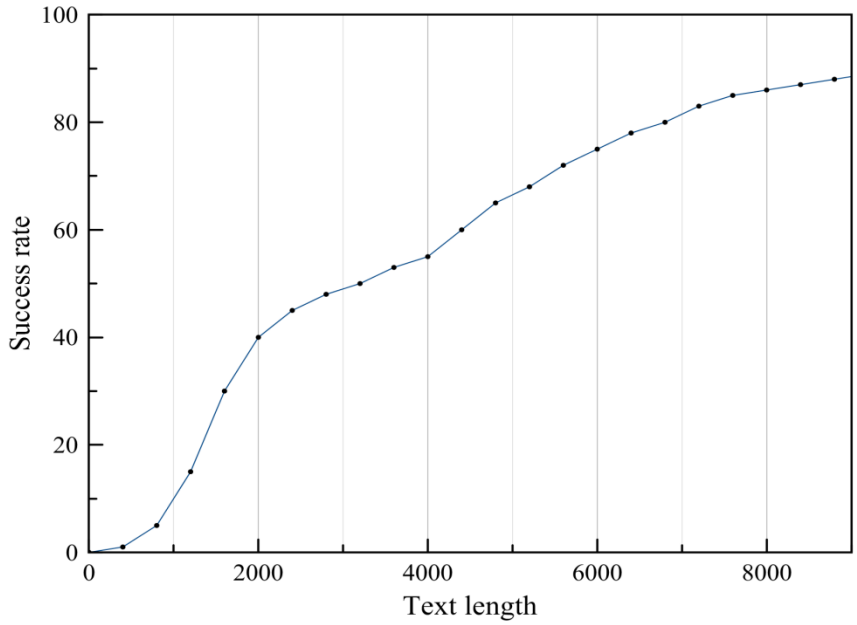

Рисунок 1 – Процент успешности атаки при фиксированной длине ключа

Список использованных источников:
1. Tilborg H.C.A. Fundamentals of Cryptography. A Professional Reference and Interactive Tutorial. Kluwer, 1999. с. 9-16.

ПРОГРАММНОЕ СРЕДСТВО МОНИТОРИНГА РАБОТЫ СЕРВИСОВ В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ

Бобков А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Смолякова О.Г. – к.т.н.,доцент

Информационные технологии полностью изменили жизнь современного человека. Мгновенный и беспрепятственный доступ к любой информации упростил и ускорил большинство процессов, связанных с различными сферами деятельности. С ростом серверных приложений появляется проблема, связанная с тем, что приложения не помещаются на одном сервере. Данная проблема решается созданием распределенных систем. В докладе сформулированы цели и особенности реализации программного средства, осуществляющего контроль работоспособности серверов в данной системе.

С методологической точки зрения мониторинг программ можно рассматривать как процедуру по оценке, целью которой является выявление и (или) измерение эффектов продолжающихся действий без выяснения причин. Мониторинг выступает в качестве внутренней процедуры, основанной на индикаторах и результатах, а также как инструмент сбора информации и отчетности.

Важно различать понятия «мониторинг» и «оценка программ». Сущность этих терминов одинакова — отслеживание результатов работы программ и выдача данных лицам, принимающим решение. Однако между ними есть и различия, заключающиеся в вопросах, на которые должно ответить проведение оценки или мониторинга. Мониторинг программ подразумевает ответ на вопрос: как идут дела? Он основывается на отслеживании текущей ситуации и сравнении текущего положения дел с ранее разработанным планом.

Программное средство мониторинга работы сервиса в распределенной системе является веб-инструментом отслеживания, который в режиме реального времени отображает активность различных сервисов в распределенной системе [1].

Основные возможности, предоставляемые программным средством:

- возможность просмотра всех сервисов, а также их статусов;
- возможность добавления и редактирования сервисов;
- возможность автоматического подъема сервиса;