Получены уравнения регрессии, адекватно описывающие зависимость показателей качества хлебобулочных изделий (кислотности, пористости, влажности, балльной оценки) от количества вносимых в рецептуру нетрадиционных видов сырья (порошка плодов рябины, порошка листьев малины, порошка зверобоя). Это дает возможность в конечном итоге варьировать компонентными составляющими рецептур для получения изделий высокого качества.

Установлена возможность сокращения времени брожения теста на основе разработанного пищевого концентрата в 1,5–2 раза, что говорит о целесообразности использования ускоренных технологией производства.

Исследовалось влияние нетрадиционных сырьевых компонентов на сохранение санитарно-микробиологической безопасности хлебобулочных изделий. Установлено, что применение травы зверобоя, листьев малины, плодов рябины при производстве ржано-пшеничных хлебобулочных изделий лечебно-профилактического назначения позволило увеличить их сроки годности на 25 %. Изделия не были подвержены плесневению (при визуальном осмотре плесень не обнаружена) в течение 5–6 суток.

МЕТОД УНИКАЛЬНОЙ АЛФАВИТНОЙ СТРОКИ ДЛЯ ШИФРОВАНИЯ ДАННЫХ НА БАЗЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

П. Р. СИНИЦА

НАУЧНЫЙ РУКОВОДИТЕЛЬ – Д. Ф. ПАСТУХОВ, КАНДИДАТ ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК, ДОЦЕНТ

Для шифрования текстовых данных использовался метод эллиптической криптографии. Впервые предложен метод уникальной алфавитной строки-ключа, в которой произвольный символ алфавита отображается в некоторую точку эллиптической кривой, а его позиция равна разности x и y координат этой точки. При этом не все позиции строки-ключа могут применяться для алфавита, а символы алфавита можно перемешивать в случайном порядке. Огромная размерность пространства алфавитных строк из 80 символов исключает возможность взлома шифра методом простого перебора даже за время 10 в степени 40 лет.

Ключевые слова: эллиптическая криптография, формулы сложения и удвоения точек.

В ядерной части программы на языке C++ применялся эллиптический шифр с алгебраической кривой $y^2 = x^3 + ax + b$ (a,b-ключи) по формуле $shifr = (kG, kP_b + P_m)$,где G -порождающая точка абелевой группы эллиптических точек,k-случайный ключ абонента A, символ с позицией m в алфавитной строке отображается в точку $m \mid P_m(x_m, y_m), m = x_m - y_m$, n_B - открытый ключ абонента B. $P_b = n_b G$. Абонент A шифрует символ с позицией m в строке для абонента B.

Таким образом, шифр 1 символа – это две точки эллиптической кривой kG и $kP_b + P_m$ с 4 целыми числами из группы остатков по простому модулю p: Z_p (правое окно интерфейса рис. 1). Формула дешифрования выглядит так: $P_m = kP_b + P_m - n_b * kG = kn_b G + P_m - n_b * kG = P_m$. То есть, нужно из второй точки шифра вычесть первую точку шифра, умноженную на открытый ключ n_B . В алгоритме использовались формулы удвоения $P_2(x_2, y_2) = P_1(x_1, y_1) + P_1(x_1, y_1)$.

$$\begin{cases} x_2 = \left(k_1{}^2 - 2x_1\right) \bmod p, k_1 = \left(3x_1{}^2 + a\right) \bmod p * \left(2y_1\right)^{-1} \bmod p \\ y_2 = \left(-y_1 + k_1\left(3x_1 - k_1{}^2\right)\right) \bmod p \end{cases} \quad (1)$$

И формулы сложения 2 разных точек эллиптической кривой $P_3(x_3, y_3) = P_1(x_1, y_1) + P_2(x_2, y_2)$.

$$\begin{cases} x_3 = \left(k_2{}^2 - x_1 - x_2\right) \bmod p, k_2 = \left(y_2 - y_1\right) \bmod p * \left(x_2 - x_1\right)^{-1} \bmod p \\ y_3 = \left(-y_1 + k_2\left(2x_1 + x_2 - k_2{}^2\right)\right) \bmod p \end{cases} \quad (2)$$

Графический интерфейс программы с использованием эллиптической криптографии и метода уникальной алфавитной строки ключа из 50 символов написан в среде Visual Studio и показан на Рис.1. Дешифрование возможно если и только если алфавитные строки при кодировании и декодировании совпадают. Выбирают алфавитную строку A и B совместно.

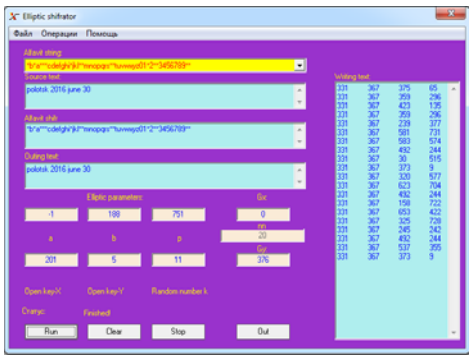

Рис. 1. Графический интерфейс программы

Библиографические ссылки

1. *Пастухов Д. Ф., Пастухов Ю. Ф, Синица П. Р.* Шифрование на базе эллиптических кривых : учеб.-метод. пособие [Электронный ресурс]. Новополоцк : ПГУ, 2016. URL: http://elib.psu.by:8080/handle/123456789/16814 (дата обращения: 31.05.2020).

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОРОЖНОГО ДВИЖЕНИЯ НА АВТОМОБИЛЬНЫХ ДОРОГАХ РЕСПУБЛИКИ БЕЛАРУСЬ

Е. Ю. СКВОРЦОВ

НАУЧНЫЙ РУКОВОДИТЕЛЬ – Д. Ю. МАКАЦАРИЯ, КАНДИДАТ ТЕХНИЧЕСКИХ НАУК, ДОЦЕНТ

В статье рассматриваются основные направления и тенденции обеспечения безопасности движения с учетом выбора скоростного режима, проезда перекрестков, проведения ремонтных работ.

Ключевые слова: автомобиль, безопасность, дорожное движение, скорость.

Автомобилизация населения влияет на многие процессы, происходящие в различных сферах жизнедеятельности. В условиях увеличения интенсивности дорожного движения изменяются многие факторы. Одним из них является безопасность дорожного движения. Рост количества транспортных средств на автомобильных дорогах, изменение их скоростных режимов движения приводит к увеличению вероятности возникновения дорожной аварийности, а также к преждевременному износу асфальтобетонного дорожного покрытия. Данные факторы снижают уровень безопасности дорожного движения [1].

Требования к перевозке пассажиров и грузов автомобильным транспортом диктуют необходимость перехода на новый уровень обеспечения безопасности дорожного движения. Они реализуются комплексно на различных этапах. Краткосрочные мероприятия позволяют обеспечивать безопасность дорожного движения за счет использования новейших методик и применения современных средств организации дорожного движения. Долгосрочные мероприятия подразумевают существенные изменения в дорожном движении за счет проведения ремонта асфальтобетонного покрытия и реконструкции автомобильных дорог. Расширение проезжей части дороги, устройство островков безопасности и другие инженерные решения позволяют эффективно разделять между собой транспортные и пассажирские потоки.

Режимы движения транспортных средств постоянно изменяются. Развитие дорожной инфраструктуры направлено на ускорение процесса оказания услуг в сфере перевозок. Технические возможности автомобилей теоретически позволяют реализовать скоростной потенциал транспортных средств. Однако при отсутствии соответствующей дорожной инфраструктуры и подготовки водителей транспортных средств сделать это безопасно не представляется возможным.

Рассматривая потенциальную аварийную опасность участков автомобильных дорог необходимо выделить места пересечения транспортных потоков в пространстве и во времени. В основном они представляют собой перекрестки автомобильных дорог. Одним из способов разделения транспортных потоков во времени является использование средств светофорного регулирования. Сложнее реализовать способы разделения транспортных потоков в пространстве. Возведение эстакад, путепроводов и других инженерных сооружений являются более эффективными, но требуют существенных капитальных затрат.

Реализация комплексной государственной политики, включает одним из направлений улучшение движения по улицам и дорогам. Совершенствование профессиональной деятельности сотрудников