Задача 5. Пусть $u = \frac{z+4}{z-2i}$, $v = \frac{z}{iz+4}$, где $z \in R$. Изобразите множество всех комплексных чисел z, для которых:

a) число u будет действительным; b) число u будет мнимым; c) число v будет действительным; d) число v будет мнимым.

Список использованной литературы

1. Терещенко, О. И. Комплексные числа : практ. пособие / О. И. Терещенко, М. И. Ефремова. – Мозырь : МГПУ им. И. П. Шамякина, 2006. – 41 с.

КРИПТОГРАФИЯ В УЧРЕЖДЕНИЯХ ОБЩЕГО СРЕДНЕГО ОБРАЗОВАНИЯ

Макаренко Сергей (УО МГПУ им. И. П. Шамякина, Беларусь)
Научный руководитель – М. И. Ефремова, канд. физ.-мат. наук, доцент

Криптография – это наука о защите информации, и ее применение в школе может быть полезным для обучения учеников логическому мышлению, математическому моделированию, анализу данных и программированию. Вот несколько способов, как можно использовать криптографию в школе.

1. Учащиеся могут использовать шифрование для обмена сообщениями друг с другом в классе, используя простые шифры, такие как шифр Цезаря или шифр Плейфера.

2. Школьники получают возможность изучить различные типы шифрования и создать свой собственный шифр для шифрования сообщений. Они могут также проверить стойкость своего шифра, попросив других учеников попытаться его расшифровать.

3. Существует множество головоломок, которые основаны на криптографии. Ученики с легкостью могут решить такие головоломки, используя знания о криптографии.

4. Учащиеся получают знания истории криптографии, включая использование шифров в различных исторических событиях, таких как Вторая мировая война. Они могут также изучить работу знаменитых криптографов, таких как Алан Тьюринг.

5. Учащиеся могут освоить криптографические протоколы, которые используются для защиты информации в сетях. Это может помочь им понять, как работают Интернет и сети.

Эти задачи помогут ученикам развивать свои навыки криптографии и понимание принципов ее работы.

Целью данной работы является разработка методических рекомендаций для проведения факультативных занятий по криптографии для учащихся 10–11 классов учреждений общего среднего образования.

RSA-криптосистема – это одна из самых популярных криптографических систем с открытым ключом, которая была разработана в 1977 году

Роном Ривестом, Ади Шамиром и Леонардом Адлеманом [1]. RSA использует два ключа: открытый и закрытый. Открытый ключ не является секретным и может использоваться для шифрования сообщений. Закрытый ключ является секретным и используется для расшифровки сообщений, которые были зашифрованы с использованием открытого ключа.

Процесс шифрования сообщения в RSA-криптосистеме состоит из нескольких шагов:

1. Генерация ключей: генерируется пара ключей, состоящая из открытого и закрытого ключей.

2. Шифрование сообщения: сообщение шифруется с использованием открытого ключа. Пусть (e, n) и будет открытым ключом. При этом каждому символу сообщения присваивается числовое значение *c*, после чего это число возведется в степень открытого ключа, по модулю некоторого числа *n* ($M = c^e (mod\, n)$).

3. Расшифрование сообщения: зашифрованное сообщение расшифровывается с использованием закрытого ключа. Адресат получает сообщение (M, e, n). Он, как и все, знает n и e. Он также должен знать секретный ключ – такое натуральное $d < n$, что $e \cdot d \equiv 1 \left(mod\left(\varphi(n)\right)\right)$, где $\varphi(n) -$ функция Эйлера. Зашифрованное число возведется в степень закрытого ключа по модулю n $(M^d = c(mod\, n))$, после чего каждому числу будет сопоставлен символ.

Преимуществом RSA-криптосистемы является ее безопасность. Для того чтобы расшифровать сообщение, злоумышленнику необходимо вычислить закрытый ключ, что является вычислительно сложной задачей. Кроме того, RSA-криптосистема используется для создания электронных подписей, которые обеспечивают аутентификацию и защиту целостности данных.

Приведем примеры, предлагаемые учащимся на факультативных занятиях [2].

Пример 1. Пусть пользователь A хочет передать пользователю B сообщение M, которое в некоторой кодировке соответствует числу 9 и зашифровано с помощью алгоритма *RSA*. Пользователь B имеет следующие ключевые параметры: $p = 7, q = 11, d = 53$. Описать процесс шифрования сообщения пользователем A.

Пример 2. Пользователю системы *RSA* с ключевыми параметрами $n = 77, d = 53$ передано зашифрованное сообщение C, состоящее из блока цифр: 42. Расшифровать это сообщение.

Пример 3. Зашифруйте свою фамилию в системе *RSA*.

Пример 4. Найдите наибольший общий делитель чисел $(11,26)$, при помощи расширенного алгоритма Евклида.

Пример 5. Решите линейное сравнение с одним неизвестным:

$14x \equiv 12 (mod\ 18)$.

Пример 6. Зашифруйте сообщение «Сад» в системе *RSA* при $n = 3337, e = 79$.

Использование криптографии в школе может помочь ученикам развивать навыки логического мышления, математического моделирования, анализа данных и программирования и помочь им лучше понимать важность защиты информации в современном мире.

Список использованной литературы

1. Коутинхо, С. Введение в теорию чисел. Алгоритм *RSA* / С. Коутинков. – М., 2001. – 328 с.

2. Крупенкова, Т. Г. Криптографические средства защиты информации : учеб.-метод. пособие / Т. Г. Крупенкова. – Минск : БНТУ, 2012. – Ч. 1. – 83 с.

РАЗРАБОТКА И ВНЕДРЕНИЕ В ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС ЭЛЕКТРОННОГО УЧЕБНИКА ПО ТЕМЕ «КВАДРАТНЫЕ УРАВНЕНИЯ»

Мелихова Мария (УО МГПУ им. И. П. Шамякина, Беларусь)
Научный руководитель – В. С. Савенко, д-р техн. наук, профессор

Понятие уравнения является одним из фундаментальных понятий, изучаемых в курсе алгебры и начал анализа общеобразовательной школы. В связи с возросшей ролью математики в современной науке и технике будущие биологи, экономисты, социологи нуждаются в серьезной математической подготовке, которая давала бы возможность математическими методами исследовать широкий круг новых проблем, применять современную вычислительную технику, использовать теоретические достижения на практике. Именно поэтому в педагогической науке и практике методика обучения теме «Квадратные уравнения» занимает особое место.

Совершенствование образовательного процесса с учетом компетентностного подхода предполагает применение учащимися полученных знаний и умений в конкретных учебных и жизненных ситуациях. Для реализации компетентностного подхода при изучении данной темы нами было разработано электронное средство обучения «Квадратные уравнения». Оно разработано с помощью программы Turbosite и может быть использовано в формате .pdf.

В электронном средстве обучения «Квадратные уравнения» рассматриваются следующие вопросы: формулы корней квадратного уравнения; виды квадратных уравнений; теорема Виета и ей обратная; решение целых рациональных уравнений, сводящихся к квадратным; решение задач при помощи квадратных уравнений в заданиях централизованного тестирования по математике. Большое внимание уделено наглядности при объяснении учебного материала и решении практических задач.

Можно выделить следующие универсальные учебные действия, которые усваивают учащиеся при обучении с помощью электронного