ШИФРОВАНИЕ И КРИПТОГРАФИЯ КАК ПРИЕМЫ, ПОМОГАЮЩИЕ ПОВЫСИТЬ МОТИВАЦИЮ ПРИ ОБУЧЕНИИ ЯЗЫКУ С УЧЕТОМ МЕДИАСРЕДЫ

Меденцева Наталья Петровна

Аннотация: *Статья посвящена истории рстанвления шифровки и криптографии как педагогических приемов.*

Ключевые слова: *Шифр, шифровка, криптография, приемы мотивации учащихся.*

В настоящее время, в век бурного развития информационных технологий, уже невозможно представить себе мир без применения паролей, кодов доступа, шифрования и дешифровки информации, нумерологии, «игры с числами». Методы шифрования встречались и в древности, но сейчас приобретают большие масштабы. Их создание привлекает как простых людей, так и специалистов: программистов, математиков, других специалистов ИТ-индустрии, которые придумывают всё новые формы.

Криптография способствует формированию умений и навыков, носящих общенаучный и обще интеллектуальный характер, содействует участию студентов в творческой деятельности. Поэтому применение приемов шифрования и криптографии способны вызвать большой интерес у студентов на занятиях по изучению языка.

Криптография – это наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта).

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

Согласно источникам, первые способы шифрования текста появились вместе с зарождением письменности. Способы тайного письма применялись древними цивилизациями Индии, Месопотамии и Египта. В письменах

Древней Индии упоминаются способы изменения текста, которые использовали не только правители, но и ремесленники, желающие скрыть секрет мастерства. Истоком криптографии считается использование специальных иероглифов в древнеегипетской письменности около четырех тысячелетий назад.

Первым шифром, зародившимся в древних цивилизациях и актуальным, в некотором роде, и по сей день, можно считать шифр замены. Чуть позже был придуман шифр сдвига, который применялся Юлием Цезарем, почему и был назван в его честь .

Помимо шифров, нельзя не упомянуть о приборах для шифрования, которые разрабатывали древние математики. Например, скитала – первый шифратор, разработанный в Спарте. Представлял собой палку, на которую по всей длине наматывалась лента пергамента. Текст наносился вдоль оси палки, после чего пергамент снимался, и получалось шифрованное сообщение. Ключом служил диаметр палки. Однако такой способ шифрования был абсолютно нестойким – автором взлома стал Аристотель. Он наматывал ленту пергамента на конусообразную палку до тех пор, пока не появлялись отрывки читаемого текста.

Также ярким примером из мира древних шифраторов может стать диск Энея – диск с отверстиями по количеству букв в алфавите. Нитка протягивалась последовательно в те отверстия, которые соответствовали буквам сообщения. Получатель вытаскивал нитку,

записывал последовательность букв и читал секретное послание. Однако этот шифратор обладал существенным недостатком – достать нитку и разгадать послание мог кто угодно.

Шифры существуют для того, чтобы скрыть ценную информацию и сохранить секрет. И если удается разгадать написанное, то можно узнать тайну какой-то личности, координаты клада или даже историю целой цивилизации. Но существуют послания, которые столетиями остаются неразгаданными.

Необходимость засекречивать важные послания возникла еще в древности. Со временем люди находили новые, все более сложные способы делать послания недоступными чужим глазам. Вопреки распространенному мнению, код и шифр – это не одно и то же. В коде каждое слово заменяется на какое-то иное кодовое слово, в то время как в шифре заменяются сами символы сообщения. Когда люди говорят «код», они, как правило, имеют в виду «шифр». Древние рукописи и языки были поняты с помощью техник декодирования и дешифрования. Самый известный пример – Розеттский камень Древнего Египта. Фактически коды и шифры определяли исход многих войн и политических интриг на протяжении всей истории человечества. Существуют тысячи типов шифрования сообщений, но в этой статье мы рассмотрим лишь самые известные и значимые из них.

Стеганография – это искусство скрытого письма. Этой технике даже больше лет, чем кодам и шифрованию. Например, сообщение может быть написано на бумаге, покрыто ваксой и проглочено с той целью, чтобы незаметно доставить его получателю. Другой способ – нанести сообщение на бритую голову курьера, подождать, пока волосы вырастут заново и скроют послание. Лучше всего для стеганографии использовать повседневные объекты. Когда-то в Англии использовался такой метод: под некоторыми буквами на первой странице газеты стояли крохотные точки, почти невидимые невооруженным глазом. Если читать только помеченные буквы, то получится секретное сообщение! Некоторые писали сообщение первыми буквами составляющих его слов или использовали невидимые чернила. Была распространена практика уменьшения целых страниц текста до размера буквально одного пикселя, так что их было легко пропустить при чтении чего-то относительно безобидного. Стеганографию лучше всего использовать в сочетании с другими методами шифрования, так как всегда есть шанс, что ваше скрытое послание обнаружат и прочитают.

ROT1-этот шифр известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, A заменяется на B, B на C, и т.д. «ROT1» значит «ROTate 1 letter forward through the alphabet» (англ. «сдвиньте алфавит на одну букву вперед»). Сообщение «I know what you did last summer» станет «J lopx xibu zpv eje mbtu tvnnfs». Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд, но дети с радостью «играют» с его помощью .

В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из «all the better to see you with» получается «lla eht retteb ot ees joy htiw». Другой пример – менять местами каждые две буквы. Таким образом, предыдущее сообщение станет «la tl eh eb tt re ot es ye uo iw ht». Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения. Сложные ключи могут сделать такой шифр довольно сложным на первый взгляд, но многие сообщения, закодированные подобным образом, могут быть расшифрованы простым перебором ключей на компьютере.

СПИСОК ЛИТЕРАТУРЫ:

1. Фёдорова Л. И. Как грамотно организовать занятие по языку, используя технологии коллективного обучения и графические органайзеры //Иностранные языки в Узбекистане. – 2020. – №. 6. – С. 104-113.

1. Меденцева Н. П. Практико-методические функции применения ИКТ и технических средств обучения в вузах Узбекистана //Педагогика высшей школы. – 2015. – №. 1. – С. 41-42.

2. Медведева В. Г. Шифры и шифровки. https://urok.1sept.ru/articles/661670

3. Меденцева Н. П. Влияние современных медиа на выбор методики обучения письменной речи //Проблемы и перспективы развития образования. – 2019. – С. 1-3.

4. https://cryptoworld.su/lesons-of-cryptography-1/

5. https://gitjournal.tech/kriptografija-chto-jeto-takoe-i-zony-primenenija/