Разуки Юссеф
ХГУПТ

КРИПТОГРАФИЯ В АРАБСКИХ СТРАНАХ

История человечества знает много случаев, когда возникала необходимость в сокрытии передаваемой информации. Это сокрытие могло быть на уровне отдельных людей (например, при ведении бизнеса), на уровне отдельных групп (например, при передаче религиозной информации), на уровне государств (например, при сообщении об объявлении войны).

Принято считать, что первому образцу криптографического письма около 4000 лет. Самые древние криптограммы были найдены на территории Древнего Египта. Но, как нам представляется, криптография намного древнее, и использование шифрованного письма применялось и до египтян.

Криптографические записи обнаружены также в иудейских священных книгах. Самым распространенным методом шифрования в них является так называемый «атбаш». Этот сравнительно простой метод состоит в том, что первую букву алфавита заменяли последней, вторую букву – предпоследней и т.д.

Одним из самых известных древних шифров является так называемая «скитала»; изобретателями этого метода были древние греки. Этот шифр мог быть достигнут таким образом: на длинный стержень наматывалась пергаментная лента, на которую наносился текст вдоль всей оси стержня. Естественно, после разматывания текст невозможно было прочитать. Для расшифровки сообщения получатель должен был обладать таким же стержнем. Собственно этот стержень и назывался скиталой. Широко известен также знаменитый диск Энея, на котором были выбиты отверстия, соответствующие буквам алфавита. Шифровальщик протягивал нить через эти отверстия и, таким образом проявлялись нужные буквы. В случае перехвата диска и угрозы прочтения сообщения можно было быстро вытянуть нить, сделав послание недосягаемым. Но мы хотим рассказать, прежде всего, об использовании

криптографии в арабском мире. Своего расцвета на арабских территориях это искусство достигло в YIII веке н.э. Арабский филолог Халиль аль-Фарахиди первым обратидл внимание на возможность использования стандартных фраз для дешифрования. Книга, в которой он описал свой метод, называется «Китаб аль-Муамма»(«Книга тайного языка»). Арабский ученый ас-Сули написал книгу практической направленности, которая носила название Адаб аль-Куттаб» («Руководство для секретарей»). По сути дела, это один из первых опытов создания именно учебного пособия по шифрованию записей финансово-хозяйственного назначения. Довольно известным в IX веке был труд арабского ученого Абу Бакр Ахмеда ибн Али Ибн Вахшия ан-Набати, в которой дано описание нескольких малоизвестных шифров с применением разных алфавитов. Венчает эти исследования энциклопедия Ибн ал-Хаима, состоящая из 14 томов и носящая название Субх ал-Ааша. Один из солидных разделов этого многотомного труда содержит описание семи шифров замены и перестановки, включает таблицы частотности употребления букв в арабском алфавите.

Следует добавить, что именно арабская культура внесла в словарь криптологии такие понятия как «шифр» и «алгоритм». В настоящее время криптография активно используется в разных сферах нашей жизни. Например, в транспорте для защиты билетов от подделок, в банковских операциях, а также для защиты электронной почты от спама. Поэтому принципы криптографического письма представляют определенный интерес для современной науки.

Рибалко Марія
НТУ «ХПІ»

КУЛЬТУРНИЙ ДІЯЧ ВАСИЛЬ КАРАЗІН

Серед видатних українців гідне місце посідає Василь Назарович Каразін – вітчизняний вчений, винахідник, громадський діяч. Засновник першого у