Томмазо Спинелли и его шифры

(из истории криптографии раннего нового времени)[1]

Домнина Екатерина Геннадьевна

аспирантка

Московский государственный университет им. М.В. Ломоносова, Москва, Россия

E-mail: ekaterina.domnina(at)gmail.com

Доклад посвящен методике дешифрования шифров замены, наиболее распространенной форме кодирования информации в английской дипломатической переписке XV – первой половины XVI века. Основным материалом для исследования послужили письма Томмазо Спинелли (1472-1522), представлявшего интересы английского короля при императоре, его брату Леонардо (1473-1531), канонику кафедрального собора Флоренции и спальничему Юлия II. Переписка Томмазо охватывает период с 1490-х по 1522 год и насчитывает более ста документов, примерно треть из них содержит зашифрованные фрагменты. Данная переписка принадлежит к неизданной части семейного архива флорентийских купцов Спинелли, внесших заметный вклад в расширение экономического, политического и культурного взаимодействия между европейскими государствами в период позднего средневековья – раннего нового времени (Beinecke Rare Book and Manuscript Library, Yale University, Spinelli Archive, Gen Mss 109).

Изучение подобного рода документов представляет большой интерес не только с точки зрения получения дополнительной информации для углубления наших знаний по истории данного периода, но и, в некоторых случаях, позволяет скорректировать существовавшие ранее представления о ключевых событиях эпохи. Примером такой перспективы использования сведений, полученных в результате дешифровки, может служить недавнее исследование М. Симонетта. Работая с архивом урбинских герцогов да Монтефельтро, Симонетта обнаружил зашифрованное письмо, по прочтении которого он установил, что организатором знаменитого заговора Пацци (26 апреля 1478 года), составленного с целью убийства Джулиано и Лоренцо Медичи, был сам герцог Федерико, а не папа Сикст IV, как считалось ранее (Simonetta, 2003, p. 261-284).

Шифр, которым пользовался Федерико да Монтефельтро, относится к так называемым «простым» шифрам, или шифрам замены. Благодаря своей простоте и, одновременно кажущейся сложности при первом взгляде на них, шифры замены активно использовались не только в ренессансной дипломатии, но и в детективной литературе такими классиками жанра как Э. А. По («Золотой жук») и А. Конан Дойл («Приключения пляшущих человечков») (Dooley, 2005, p. 291, 294). Такие шифры составлялись по принципу присвоения каждой букве исходного алфавита некого символа, после чего с помощью этой искусственной азбуки производилась запись текста. Как правило, пользователи этих шифров не прибегали к дополнительным методам защиты своей информации, то есть сохраняли естественный порядок букв в словах, пробелы между словами в предложениях, знаки препинания и, наконец, короткие слова – личные местоимения, артикли, предлоги и т.д.

Главным условием подбора ключа к таким шифрам является установление того языка, на котором написан исходный текст, что обычно можно сделать на основании данных о происхождении документа. После определения языка документа необходимы количественный анализ символов текста с целью выявления среди них наиболее

[1] Исследование является частью проекта по изучению истории английской дипломатической службы, который был поддержан Фондом Дж. Фокса при Йельском университете (США) в 2005-2006 гг.

употребительных и последующее определение их соответствия самым часто встречающимся буквам алфавита данного языка. Далее начинается завершающий, и самым трудоёмкий этап работы – процесс установления остальных буквенно-символьных соответствий путем их простого подбора при чтении текста.

Интересующий нас шифр Томмазо Спинелли представляет собой усложненный вариант шифра замены и построен по принципу присвоения некоторым буквам сразу нескольких символов с последующим их чередованием. Следует отметить, что Спинелли регулярно производил смену ключа используемых им шифров, но тот факт, что базовый набор использовавшихся им символов на протяжении более тридцати лет оставался неизменным, свидетельствует о надежности его шифра. Данная тенденция прослеживается и в корреспонденции других английских дипломатов этого периода (Джованни Джильи, Джон Кларк), чьи зашифрованные письма были взяты нами для сравнения (British Library, Cotton MSS, Vitellius B III, IV). Другой отличительной чертой этих документов является сочетание простого и закодированного текста в одном и том же письме. Это также может служить подтверждением того, что авторы этих писем считали свои шифры верным средством защиты информации, даже в случаях перехвата корреспонденции.

Набор знаков, которые Спинелли применял для замены букв итальянского алфавита, представляет собой смесь букв греческого алфавита, астрономических и математических символов, а также пиктограмм, происхождение которых нам не удалось установить. В целом, «азбука» Спинелли сродни «тироновым нотам», виду скорописи, известной со времен античности (Pratt, 1942, p. 143). Однако в отличие от «нот», основанных на использовании ограниченного числа слов, каждое из которых обозначалось определенным символом, Спинелли заменял каждую букву одним или несколькими символами. Приверженность простым формам шифра замены составляет характерную особенность английской криптографии данного периода, в то время как в дипломатической практике других стран – Испания, Милан, Венеция, Папское государство – применялись как различные разновидности «тироновых нот», так и новые шифровальные системы, такие как полиалфавитные шифры Леона Баттиста Альберти (Meister, 2006, p. 24-118).

Источники и литература:

1. Behrens B. (1933) The office of the English resident ambassador: its evolution as illustrated by the career of Sir Thomas Spinelli, 1509-1522 // Transactions of the Royal Historical Society. Fourth ser. Vol. XVI. P. 161-195.
2. Beinecke Rare Book and Manuscript Library, Yale University, Spinelli Archive, Gen Mss 109, box 123, folders 2459-2466; box 126, folders 2566-2587.
3. Black C.J., Challis C.E. (1968) Henry VIII to his ambassadors at the Diet of Ratisbon, 17 June 1541. York.
4. British Library, Cotton MSS, Vitellius B III, fols. 51-64; Vitellius, B IV, fols. 172-176.
Dooley J.F. (2005) Codes and ciphers in fiction: an overview // Cryptologia. Vol. XIX. № 4. P. 290-328.
5. Jacks P., Caferro W. (2001) The Spinelli of Florence: fortunes of a Renaissance merchant family. University Park, Pa. P. 243ff.
6. Meister A. (1906) Die Geheimschrift im Dienste der paepstlichen Kurie. Paderborn. P. 24-118.
7. Pratt F. (1942) Secret and urgent: the story of codes and ciphers. New York. P. 143.
8. Simonetta M. (2003) Federico da Montefeltro contro Firenze. Retroscena inediti della congiura dei Pazzi // Archivio storico italiano. Vol. CLXI. № 596. P. 261-284.
9. Speziali P. (1955) Aspects de la cryptographie au XVIe siècle // Bibliothéque d'Humanisme et Renaissance. Travaux et documents. T. XVIII. P. 188-206.