АСТАХОВ МАРАТ АНДРЕЕВИЧ

Независимый исследователь, выпускник Московского государственного университета им. М. В. Ломоносова
marat1089@mail.ru
https://moscowstate.academia.edu/MaratAstakhov

Позднесредневековый шифр пропорциональной замены и методика его дешифровки (на примере неизученного испанского документа из архива СПбИИ РАН)

В статье представлен краткий обзор истории криптографии до начала раннего Нового времени. Особое внимание уделено распространенному в позднее Средневековье шифру пропорциональной замены, в котором каждая буква открытого текста в соответствии с частотой ее встречаемости заменялась несколькими символами тайнописи. На примере работы с обнаруженным в архиве Санкт-Петербургского института истории РАН зашифрованным письмом 1460 г. из королевской канцелярии Арагонской Короны выделены общие этапы дешифровки и даны практические рекомендации исследователям, занимающимся подобным материалом. После установления языка, на котором был составлен документ, пособия по криптографии обычно советуют провести анализ частоты встречаемости символов в тексте и сравнить с уже установленными данными распределения букв по тому или иному языку. Тем не менее автор данной статьи исходил из того, что шифр пропорциональной замены был изобретен именно для того, чтобы исказить частотные данные и усложнить взлом тайнописи, поэтому применил собственный, оригинальный метод.

После проведения каталогизации символов, присвоения каждому из них отдельного номера и перенесения этих цифр в электронную таблицу стала видна «перспектива» текста, были определены устойчивые сочетания значков и слова-палиндромы, которые было возможно однозначно дешифровать. В конечном итоге, как бы разгадывая кроссворд без подсказок, автор дешифровал весь текст. Данный опыт может быть полезен всем, кто в своих исследованиях имеет дело со средневековыми криптографическими документами.

Ключевые слова: Арагонская Корона; криптография; методы дешифровки; средневековая дипломатия; средневековые шифры; шифр замены.

ДЛЯ ЦИТИРОВАНИЯ / FOR CITATION

Астахов М. А. Позднесредневековый шифр пропорциональной замены и методика его дешифровки (на примере неизученного испанского документа из архива СПбИИ РАН) // Vox medii aevi. 2018. Vol. 2(3). С. 105–125. URL: *http://voxmediiaevi.com/2018-2-astakhov*

MARAT ASTAKHOV

Independent Scholar, graduate of Lomonosov Moscow State University
marat1089@mail.ru
https://moscowstate.academia.edu/MaratAstakhov

Late Medieval Homophonic Substitution Cipher and its Decipherment (Evidence from Little Known Spanish Document from the Archive of the Saint Petersburg Institute of History of the Russian Academy of Sciences)

The article presents a brief overview of the history of cryptography before the beginning of the Early Modern Period. Particular attention is paid to the homophonic substitution cipher used in the Late Middle Ages where each letter in the plaintext was replaced by several (more than one) characters in the ciphertext in accordance with its frequency. After examination of an encrypted letter of 1460 from the royal chancery of the Crown of Aragon kept in the archive of the Saint Petersburg Institute of History of the Russian Academy of Sciences we summarize some general principles of decipherment and give some practical recommendations to the researchers engaged in such domain. As soon as the language of ciphertext is recognized, cryptography manuals usually advise the further frequency analysis and comparison of results with the already known data for the distribution of letters in a particular language. However, basing on the fact that the homophonic substitution cipher was aimed to distort frequency analysis and complicate the cracking, we developed our own approach.

After cataloguing the symbols, numbering and transferring them into a spreadsheet, the "perspective" of the text became visible, revealing stable combinations of signs and words-palindromes, which could be decrypted unambiguously. Therefore, like solving a crossword without clues, we deciphered the entire ciphertext. This experience could be useful for everyone who deals with medieval cryptographic documents.

Key words: Crown of Aragon; Cryptography; Medieval Ciphers; Medieval Diplomacy; Methodology of Decipherment; Substitution Cipher.

Марат Астахов

Позднесредневековый шифр пропорциональной замены и методика его дешифровки (на примере неизученного испанского документа из архива СПбИИ РАН)

Недавние новости о том, что канадским ученым с помощью искусственного интеллекта удалось определить язык и прочитать первое предложение в знаменитом манускрипте Войнича (XV в.)[1], вселяют надежду, что самая таинственная рукопись Средневековья в обозримом будущем будет расшифрована. Однако оставим эту проблему, над которой уже более ста лет бьются специалисты в области самых различных научных дисциплин, лучшим умам планеты и обратимся к более незатейливым, но оттого не менее интересным и полезным для расширения нашего знания о прошлом вещам, в частности к повседневной средневековой тайнописи.

Различные шифрованные послания и тайный язык в целом применялись человеком с глубокой древности с целью скрыть какие-либо сведения от тех, кому они не предназначены (врагов, чужаков и просто непосвященных в самом широком смысле). Существование секретного языка и знаков фиксируется у ряда народов, находящихся на стадии родоплеменных отношений, например у папуасов Новой Гвинеи: так, у народа бонгу есть особый мужской тайный язык «жующих бетель» (пряное растение из семейства перечных), используемый мужчинами при рыболовстве и вообще при выходе в море. Грамматически тайный язык не отличается от повседневного языка бонгу, различие заключается лишь в именах существи-

1. По крайней мере, так заявил канадский лингвист Гжегож (Грег) Кондрак из лаборатории искусственного интеллекта Университета Альберты в городе Эдмонтоне. URL: https://www.ctvnews.ca/sci-tech/computer-scientist-claims-clues-to-deciphering-mysterious-voynich-manuscript-1.3773754 (дата обращения: 01.12.2018).

тельных, заменяемых описательными выражениями[2]. Система тайных знаков, согласно Тациту, была известна и древним германцам, использовавшим их в ритуальных целях[3].

Наиболее известными примерами шифров из античности являются древнегреческие шифровальные палочки (скиталы, сциталы)[4], на которые накручивались полоски с текстом, или так называемый сдвиг Цезаря, упоминаемый Светонием: Гай Юлий Цезарь при конфиденциальной переписке практиковал измененный порядок букв алфавита с определенным коэффициентом смещения[5]. Тайная переписка использовалась не только полководцами и политиками. Так, например, в знаменитом трактате индийского философа III–IV в. н. э. Ватсьяяны «Камасутра» в первом разделе, посвященном различным наукам и знаниям, женщинам предписывается тайно, в уединении, изучать шестьдесят четыре искусства, среди которых значатся «различные виды условного языка» (в русском научном переводе с санскрита А. Я. Сыркина)[6]. В оригинале это понятие передавалось словосочетанием «mlecchita vikalpa» и, по всей видимости, означало тайные значки (иероглифы), нанесенные на медь[7].

В раннем Средневековье искусство криптографии, хотя и не было забыто, на долгое время пришло в упадок, по крайней мере в Западной Европе. Это не означает, что шифрами перестали пользоваться: например, франкский император Лотарь I (817–855) посылал своим сторонникам различные сообщения, замаскированные под цитаты из Священного Писания[8]. Известны примеры шифрования у вестготов (с использованием курсива, небольшого искажения знаков и букв из других алфавитов)[9] и в раннесредневековой Ирландии (шифр на основе латинского алфавита, а также, вероятно, огамическое письмо)[10]. Однако в целом использовавшиеся системы тайнописи не имели широкого применения и были довольно простыми. Способность их разгадать зависела, возможно, не столько даже от таланта к дешифровке, сколько от общей грамотности:

2. *Леонтьев А. А.* Папуасские языки. М., 1974. С. 55.

3. *Корнелий Тацит.* О происхождении германцев и местоположении Германии / пер. с лат. и комм. А. С. Бобовича под ред. М. Е. Сергеенко // *Корнелий Тацит.* Сочинения в двух томах. Л., 1969. Т. 1. С. 357–358.

4. *Адаменко М. В.* Основы классической криптологии: секреты шифров и кодов. М., 2012. С. 86–87.

5. *Гай Светоний Транквилл.* Жизнь двенадцати цезарей / пер. с лат. М. Л. Гаспарова, изд. подг. М. Л. Гаспаров, Е. М. Штаерман. М., 1964. С. 24.

6. *Ватсьяяна Малланага.* Камасутра / пер. с санскрита, вступ. статья и комм. А. Я. Сыркина. М., 1993. С. 45.

7. *Kalyanaraman S.* Sarasvati Hieroglyphs and Bharatiya Cultural Continuum. Lecchita Vikalpa and Bharatiya Sabhyata // PILC Journal of Dravidic Studies. 2002. Vol. 12(1). P. 21.

8. *Черняк Е. Б.* Пять столетий тайной войны. Из истории секретной дипломатии и разведки. М., 1972. С. 9.

9. *Galende Díaz J. C.* Elementos y sistemas criptográficos en la escritura visigótica // VIII Jornadas Científicas sobre Documentación de la Hispania altomedieval (siglos VI–X). Madrid, 2009. P. 176–183.

10. *Swift C.* Christian Communities in Fifth and Sixth Century Ireland // Trowel. The Journal of the Archaeological Society, University College Dublin. 1996. Vol. 7. P. 22–23.

для человека, просто умеющего читать, многие раннесредневековые шифры не были столь уж трудными[11].

В противоположность Западной Европе в арабском мире уже в раннее Средневековье активно интересовались криптографией: появлялись специальные трактаты, описывающие методы шифровки и дешифровки. В 855 г. вышла «Книга о большом стремлении человека разгадать загадки древней письменности» арабского ученого ан-Набати с описаниями шифров, в том числе с применением нескольких алфавитов. Также в IX в. арабский философ аль-Кинди в трактате «О разгадывании шифрованных сообщений» впервые описал метод частотного криптоанализа[12], о котором речь пойдет ниже.

В позднее Средневековье (XIII–XV вв.) с развитием международной торговли, дипломатии, военного дела умение хорошо шифровать или, наоборот, дешифровывать тексты становилось все более актуальным. Развивающиеся и усложняющиеся шифры помогали во многих случаях: купцу — передать из заморского консульства сведения о ценах, спросе и предложении; дипломату или шпиону — известить о настроениях того или иного правителя, его окружения и населения страны; военачальнику — доложить о передвижениях вражеского войска или флота и о тактических планах; ученому — сберечь тайные знания (например, Джефри Чосер зашифровал отдельные элементы астрономических вычислений в своем трактате «Экватор планет»; здесь, видимо, уместно вспомнить и об уже упоминавшемся манускрипте Войнича).

Оригинальным, хотя и не в полной мере соответствующим понятию зашифрованного, представляется составлявшееся на протяжении XIV–XV вв. в Англии «Бридлингтонское пророчество», изобилующее различного рода метафорами, иносказаниями, аллегориями, ребусами и отсылками к персонажам (порой весьма критическими) и важнейшим событиям английской истории времен Столетней войны[13]. Применялась тайнопись (наряду с различного рода эвфемизмами) и в более

11. *Селянинов О. П.* Тетради по дипломатической службе государств (История и современность). М., 1998. С. 53.

12. *Адаменко М. В.* Ук. соч. С. 90–91.

13. См. подробнее: *Калмыкова Е. В.* Образы войны в исторических представлениях англичан позднего Средневековья. М., 2010. С. 122–136.

щекотливых ситуациях, например, при записи популярных при дворе кастильского короля Альфонсо X Мудрого сатирических галисийско-португальских «песен насмешки и злословия» (cantigas de escárnio e maldizer), затрагивающих острые социальные и политические темы, изобилующих оскорблениями и специфической, порой обсценной лексикой, а также эротическими сюжетами[14]. Интересно здесь провести параллель с «Хожением за три моря» Афанасия Никитина (1468–1474), в котором купец наиболее тонкие моменты (цены за интимные услуги в подворьях, описание физиологических особенностей блудниц, соблюдение православным мусульманского поста[15]) описывал тюркскими и персидскими словами, которые для непосвященного русского читателя играли роль шифра.

Наиболее распространенным в Средневековье был *шифр простой замены*, или *подстановки*, при котором каждой букве исконного алфавита соответствовал один символ тайнописи (буква из латинского или греческого алфавита, цифра, геометрическая фигура). Как правило, пользователи этого шифра не прибегали к дополнительным мерам 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. п.[16]

Уязвимость шифра простой замены была осознана очень рано, его взлом обычно осуществлялся методом частотного анализа, предложенным еще в IX в. арабским ученым аль-Кинди. По тексту страницы из любой незашифрованной книги, написанной на предполагаемом языке шифра, устанавливалась частота встречаемости тех или иных букв. Затем выполнялся количественный анализ значков в шифре, данные которого соотносились с алфавитом предполагаемого языка, в котором буквы были распределены по частоте встречаемости.

В 1474 г. секретарь миланского герцога и служащий тайной канцелярии папской курии Франческо (Чикко) Симонетта

14. *Martínez Pereiro C. P.* Del combate singular al singular combate sexual en la sátira trovadoresca medieval gallego-portuguesa // Floema. Caderno de Teoria e História Literária. 2009. №5. P. 17–32.

15. Хожение за три моря Афанасия Никитина 1466–1472 гг. / пер. с древнерусс. А. Д. Желтякова и Л. С. Семенова, изд. подг. Я. С. Лурье, Л. С. Семенов. Л., 1986.

16. *Домнина Е. Г.* Томмазо Спинелли и его шифры (из истории криптографии раннего Нового времени) [Электронный ресурс] // Материалы XIV Международной конференции студентов, аспирантов и молодых ученых «Ломоносов–2007». URL: https://lomonosov-msu.ru/archive/Lomonosov_2007/12/WH/Domnina.pdf (дата обращения: 01.12.2018).

создал трактат по криптоанализу, в котором подробно изложил этапы взлома шифра простой замены. Первым и главным шагом является установление языка, на котором написан зашифрованный текст. Автор на основании своих наблюдений за частотой встречаемости окончаний и служебных слов в латыни и итальянском привел ряд практических рекомендаций по различению этих языков: например, большинство итальянских слов оканчиваются на гласные, тогда как латынь демонстрирует гораздо большее разнообразие окончаний; в то же время для латинского языка, в отличие от итальянского, нехарактерно частое повторение 1-, 2-, 3-х буквенных слов[17]. После определения языка дальнейшие этапы дешифровки в трактате Симонетты по своему содержанию сходны с тем, что описал аль-Кинди. Главной заслугой итальянского секретаря, на наш взгляд, является пристальное внимание к лингвистической структуре языка, его, если можно так выразиться, «ритму»: этим до сих пор пользуются специалисты, работающие со средневековыми зашифрованными текстами (в том числе и с пресловутой рукописью Войнича: ее исходным языком, как после долгого анализа определил искусственный интеллект, скорее всего, был иврит).

17. *Русецкая И. А.* История криптографии в Западной Европе в раннее Новое время. СПб., 2014. С. 75.

Несмотря на то, что в Европе ненадежность шифра простой замены отмечалась как минимум с XV в., им продолжали пользоваться и в ранее Новое время. Так, шифр шотландской королевы Марии Стюарт и участников заговора Энтони Бабингтона в сущности представлял собой всего лишь несколько усложненную разновидность простой замены, что в конечном счете привело заговорщиков на плаху. Он состоял из двадцати трех символов, которыми заменялись буквы алфавита (кроме «j», «v» и «w»), и еще тридцати пяти символов, являющихся словами или словосочетаниями. Помимо этого, имелось четыре «пустых» знака. Не вдаваясь в подробности дела, отметим только, что молодому криптологу Томасу Филлипсу, служившему под началом сэра Фрэнсиса Уолсингема, занимавшегося

вопросами контрразведки в елизаветинской Англии, не составило большого труда провести частотный анализ и дешифровать перехваченные письма[18].

Усовершенствование принципа простой замены привело к появлению *шифра пропорциональной замены*. Он предполагал, что замена букв осуществляется несколькими символами пропорционально частоте использования этих букв в открытом тексте[19].

Первое описание принципа подобного шифрования встречается в трактате секретаря авиньонского антипапы Климента VII Габриеле де Лавинде «Книга шифров», или «Трактат о шифрах» (Liber zifrarum), составленном между 1379 и 1383 гг., а первые полные алфавиты с соответствующими каждой букве значками для замен появились к началу XV в.[20] Дальнейшее развитие шифр пропорциональной замены получил в труде итальянского гуманиста Леона Баттисты Альберти «О принципах составления шифров» (De componendis cifris, 1465). Для большей надежности автор предлагал использовать пустые, ничего не значащие символы, а также упростить орфографию: например, отказаться от шифрования сочетания «qu» двумя знаками в пользу одного и т.п. Он также советовал заменять отдельными буквами наиболее часто встречающиеся слоги, слова и словосочетания[21].

Такой подход позднее приобрел определенную популярность у шифровальщиков: так, например, в «генеральном» шифре (по сути — шифр пропорциональной замены) Католических королей, ключ к которому сохранился в библиотеке Королевской академии истории в Мадриде, слов, которые кодировались буквенными сочетаниями, было около 670. Это были обозначения частей света, стран, провинций и городов, названий народов (англичане, венецианцы т.д.), титулов (французский король, миланский герцог и т.д.), типов кораблей (галея, галеас, фуста, нава и т.д.), месяцев и дней недели, числа, местоимения, предлоги, наиболее распространенные

18. *Barksdale-Shaw L. M.* "That You Are Both Decipher'd". Revealing Espionage and Staging Written Evidence in Early Modern England // A Material History of Medieval and Early Modern Ciphers. Cryptography and the History of Literacy / ed. K. Ellison, S. Kim. New York; London, 2018. P. 122–126.

19. *Адаменко М. В.* Ук. соч. С. 93

20. *Balard M.* Le chiffre à la chancellerie ducale de Gênes dans la seconde moitié du XVe siècle // La communication dans l'histoire. Tricentenaire de Colbert. Reims, 1985. P. 170.

21. *Русецкая И. А.* Ук. соч. С. 70–71.

глаголы (в различных временах и залогах, в т.ч. императиве: «напиши́те» — *screevid*, «имейте» — *tened* и т.д.) и производные от них существительные, различные конкретные (король, купец, свидетель, мавр, граница и т.д.) и абстрактные понятия (доблесть, любовь, честь, власть и т.д.). Принцип записи зашифрованных буквенных сочетаний никак не указывал на изначальные слова: например, Португалия (Portugal) кодировалась как «zoz», король Англии (rey de Inglaterra) — как «bag»[22]. Не имея ключа к такому шифру, его было крайне трудно, если вообще возможно, дешифровать, особенно при уровне развития криптологии в Средние века и раннее Новое время: например, донесения испанского посла при дворе английской королевы Марии Тюдор (1553–1558) были разгаданы только три столетия спустя, в 1868 г.[23]

И все-таки на практике было неудобно составлять большие списки заменяемых слов и обновлять базу используемых символов, поэтому чаще всего применялись более простые системы, а полюбившиеся шифры не выходили из употребления на протяжении десятилетий, подвергаясь лишь незначительным изменениям. Для шифров XV–XVI вв. было даже характерно сочетание зашифрованного и открытого текста ввиду трудоемкости самого процесса шифрования. Именно такая ситуация наблюдается, например, в личных письмах начала XVI в. Томмазо Спинелли (1472–1522), итальянского дипломата на службе у Тюдоров, кодировавшего только определенные части своих текстов и при этом практически одним и тем же шифром (пропорциональной замены с небольшим количеством символов-«пустышек») на протяжении всей своей жизни[24].

Обратимся теперь к конкретному примеру по практике дешифровки. В Западноевропейской секции Научно-исторического архива Санкт-Петербургского института истории РАН (СПбИИ РАН) хранится зашифрованное письмо 1460 г., за указание на которое мы приносим благодарность А. В. Чирковой,

22. *Galende Díaz J. C.* La escritura cifrada durante el reinado de los Reyes Católicos y Carlos V // Cuadernos de estudios medievales y ciencias y técnicas historiográficas. 1993–1994. № 18–19. P. 167–172.

23. *Селянинов О. П.* Ук. соч. С. 53.

24. *Домнина Е. Г.* Шифры в дипломатии ранних Тюдоров: на материале личной переписки Томмазо Спинелли // Искусство и культура Европы эпохи Возрождения и раннего Нового времени. Сборник трудов в честь В. М. Володарского / под ред. Т. П. Гусаровой. М.; СПб., 2016. С. 259–260.

(ЗЕС НИА СПбИИ РАН. Колл. 14. Карт. 292. №12) из канцелярии короля Арагонской Короны Хуана (Жоана) II (1458–1479), отца Фернандо Арагонского. Судя по печатям на документе, в обширную коллекцию академика Н. П. Лихачева (1862–1936) он попал из собрания итальянского историка и нумизмата Дамиано Муони (1820–1894). Во время своих поездок в Ленинград (1982, 1983) на эту грамоту обратил внимание выдающийся испанский медиевист Эмилио Саес (1917–1988), однако из-за гибели ученого в автокатастрофе она так и не была расшифрована. В посмертном издании испанских документов из ленинградского архива, осуществленном сыном Эмилио — филологом и палеографом Карлосом Саесом (1953–2006), представлено лишь описание внешнего вида письма 1460 г. с небольшим комментарием по содержанию незашифрованного латинского введения (без его публикации) и указанием на то, что оставшаяся бóльшая часть грамоты зашифрована[25]. В настоящее время (2018) текст документа нами дешифрован, переведен и опубликован[26]. В данной статье мы ограничимся только общими замечаниями по примененной нами методике дешифровки.

В тексте письма на двух с половиной страницах представлены: вводная латинская часть (титул отправителя, титул адресата, приветствие и преамбула), основной зашифрованный текст, незашифрованные конечная латинская формула прощания («Если что-то будет необходимо в наших краях…»), дата и место (Барселона, 23 мая 1460 г.), зашифрованный постскриптум, подписи короля и писца.

Первый этап любой дешифровки — *определение языка*. В нашем документе были расставлены пробелы (наиболее часто встречающаяся ситуация для шифрованных документов позднего Средневековья), поэтому имелась возможность представить себе общий «ритм» текста. Практика работы с канцелярскими документами и дипломатической перепиской Арагонской Короны показывает, что двуязычные тексты

25. *Sáez E., Sáez C.* El fondo español del Archivo de la Academia de las Ciencias de San Petersburgo. Alcalá de Henares, 1993. P. 122 (doc. №72).

26. *Астахов М. А.* Расшифрованное письмо Хуана II Арагонского: тайный план захвата Генуи // Средние века. 2018. Вып. 79(4). С. 57–93.

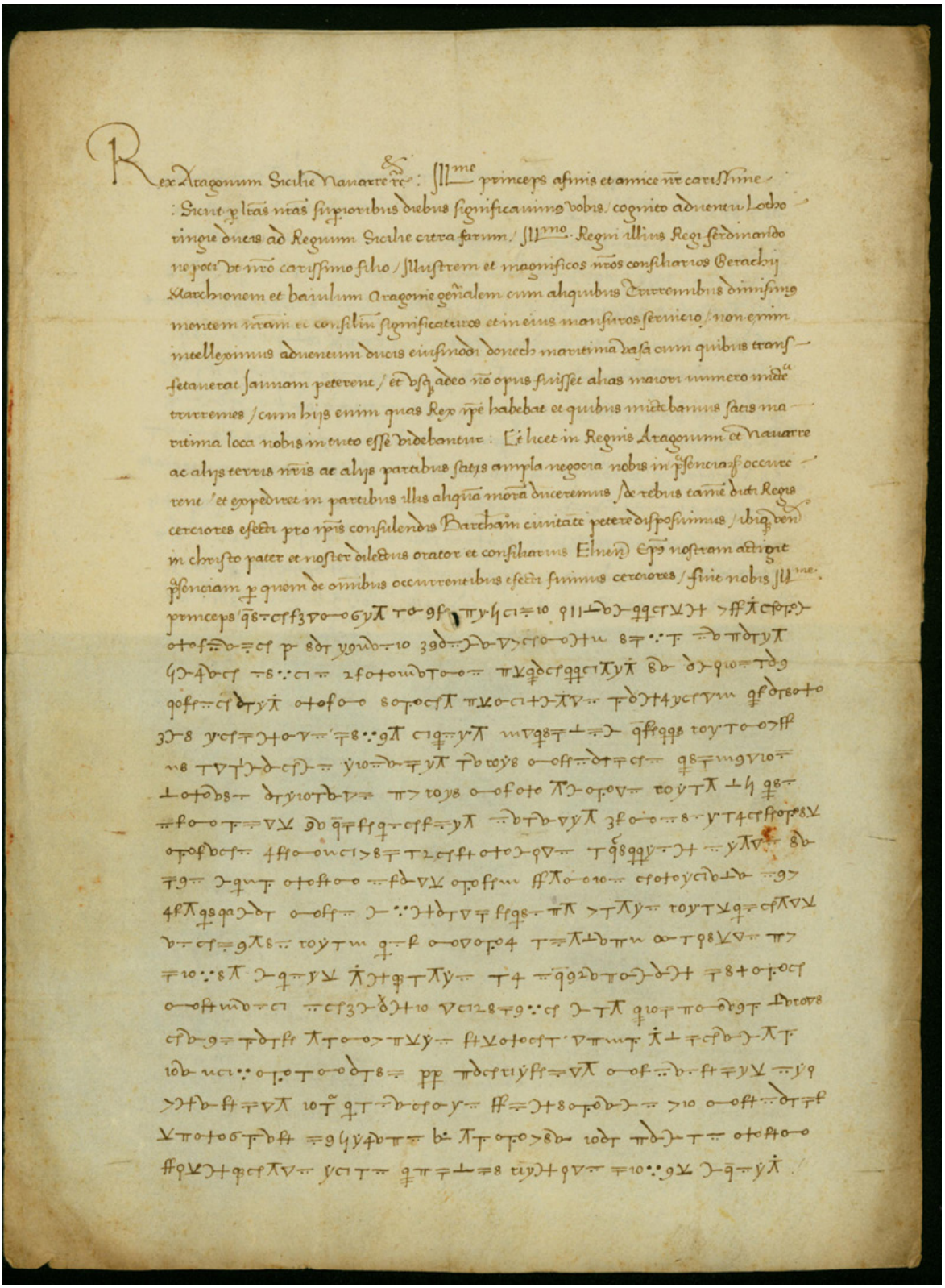

Рис. 1. Лист 1г зашифрованного послания. 1460. Западноевропейская секция Научно-исторического архива Санкт-Петербургского института истории РАН. Коллекция 14: Акты и письма политических деятелей Испании IX–XIX вв. Картон 292. №12.

Рис. 2. Лист 1v зашифрованного послания. 1460. ЗЕС НИА СПбИИ РАН. Колл. 14. Карт. 292. №12.

Рис. 3. Лист 2r зашифрованного послания. 1460. ЗЕС НИА СПбИИ РАН. Колл. 14. Карт. 292. №12.

Рис. 4. Лист 2v зашифрованного послания. 1460. ЗЕС НИА СПбИИ РАН. Колл. 14. Карт. 292. №12.

встречаются очень редко: вкрапления второго языка иногда бывают при цитировании или в устойчивых формулах-клише. Открытый латинский текст, а также незначительная частота встречаемости коротких, особенно однобуквенных слов (в случае со старокаталанским мы бы часто имели дело с предлогом «а», союзами «е» и «о») позволили предположить, что, с высокой долей вероятности, мы имеем дело с текстом, полностью составленным на латыни, — что в итоге оказалось верным.

Вторым этапом является *непосредственный анализ шифра*. Вначале необходимо *определить количество всех имеющихся элементов*. При шифровке нашего документа использовано свыше семидесяти различных символов — видоизмененные латинские и греческие буквы, в том числе с дополнительными элементами, цифры, геометрические фигуры (например, треугольник), сочетания точек и различных неясных по происхождению значков. В алфавитах латинского или любого средневекового и современного романского языка количество букв по крайней мере в два раза меньше, даже с учетом снабженных диакритическими знаками. Следовательно, очевидно, что для шифровки отдельных букв использовалось сразу несколько символов, то есть был применен шифр пропорциональной замены.

Далее, общей рекомендацией еще со времен аль-Кинди является *подсчет частоты встречаемости каждого из символов* (частотный анализ) для последующего соотнесения с частотой встречаемости букв в том или ином языке. Например, историк Е. Г. Домнина занимается итальянскими и английскими шифрами именно с помощью такого метода[27]. Особенно успешно применима такая тактика при дешифровке шифров простой замены. Однако при работе с нашим текстом мы исходили из того, что примененный в нем шифр пропорциональной замены как раз и был нужен для того, чтобы исказить данные по частоте встречаемости и тем самым затруднить взлом. Уровень встречаемости гласных в индоевропейских языках в целом выше, чем у согласных, а применение для зашифровки гласных бóльшего

27. *Домнина Е. Г.* Шифры в дипломатии ранних Тюдоров. С. 260.

числа символов, чем при для согласных, в значительной степени нивелирует частотные различия. В нашем случае, как показала в дальнейшем дешифровка, гласные шифровались четырьмя символами, а согласные — двумя-четырьмя символами. Вероятно, при допущении, что *несколько похожих друг на друга значков могут кодировать одну и ту же букву*, и, соответственно, игнорировании различий между ними при подсчете частотный анализ мог бы быть результативным. Скажем даже больше, в итоге оказалось, что действительно многие (но не все!) сходные по своей форме символы, отличающиеся друг от друга только отдельными дополнительными элементами, шифровали одни и те же буквы. Однако на этапе дешифровки мы решили не позволять себе такого смелого предположения и считать даже немного отличающиеся друг от друга значки отдельными элементами. В любом случае, историку, работающему с средневековыми шифрами, будет нелишним вначале применить частотный анализ, а затем, в случае если распределение символов окажется практически равномерным, пробовать другие подходы.

Мы же, с самого начала отказавшись от подсчета частоты встречаемости, пошли по иному пути — *каталогизации символов*. Пронумеровав их, мы создали таблицу в программе *Microsoft Excel*, в которой каждое слово шифра с помощью получившихся цифр записывалось с новой строки. Для такого рода простой компьютерной дешифровки было вполне достаточно внести в таблицу данные только одной шифрованной страницы, на которой, по визуальному впечатлению, встречается 90–95% всех использованных символов.

Далее мы решили воспользоваться наблюдениями Симонетты и *проанализировать «ритмику» текста*. При внимательном рассмотрении было обнаружено, что один значок (похожий на своеобразную лигатуру греческих букв «тау» и «омикрон»: τo) всегда употреблялся только в начале слова или на третьем месте с конца (как в сочетании «-que», которое пишется слитно с предыдущим словом). Данное наблюде-

ние позволило идентифицировать названный символ как «q», а все варианты следующих за ним символов — как «u» (как раз об этом нюансе и предупреждал в своем трактате Альберти). В сочетании «-qu + 1 буква» в большинстве случаев идет буква «e», за исключением шестибуквенных форм «aliqui», «aliqua» и «aliquo». Данные исключения нам не подходят, поскольку в таблице мы сталкиваемся с двумя пятибуквенными сочетаниями, у которых не может быть другого окончания, кроме как «-que».

После произведенной замены в таблице появилось пятибуквенное слово-палиндром, имевшее следующий вид: «2-u-17-u-2». В латинском языке существует только одно широко распространенное слово, отвечающее данным критериям, — это форма первого лица множественного числа глагола «esse» — «sumus». Таким образом, была дешифрована часть символов, соответствующих буквам «s» и «m». Сравнение форм «q-u-41-m», «41-7-q-u-e» и «s-7-41-35-u-u-m» дало наиболее вероятные слова «quam», «atque» и «statuum», а, следовательно, символ для «a» и целых два символа для «t». Форма «u-33-s-t-20-u-m» соответствует слову «uestrum», что привело к открытию еще двух символов: для букв «e» и «r» соответственно.

Таким образом, работа дешифровщика средневековых шифров сродни разгадыванию кроссворда без подсказок. Внося дешифрованные символы, мы получали все новые и новые сочетания открытых букв и значков, которые можно было однозначно интерпретировать. Использование таблицы *Microsoft Excel* позволяло видеть текст «в перспективе». В итоге нам удалось дешифровать весь текст на первой странице и, в дальнейшем, с помощью полученного ключа прочесть и остальные. Трудность составили только пять одиночных символов, один из которых мы, как оказалось, верно интерпретировали исходя из содержания документа как «папа Римский».

Впоследствии, благодаря помощи Е. Г. Домниной, удалось установить, что шифр происходит из канцелярии миланских герцогов Сфорца. Он был включен Франческо Транкедини

(ок. 1441 — ок. 1491), наставником которого был уже упоминавшийся Ф. Симонетта[28], в трактат-коллекцию шифров, рукопись которого ныне хранится в Австрийской национальной библиотеке (Oesterreichische Nationalbibliothek, Wien. Codex Vindobonensis 2398. Fol. 23r)[29]. Соответственно, автором нашего шифра является либо сам Ф. Симонетта, либо его ученик Ф. Транкедини: они оба на протяжении долгих лет были секретарями династии Сфорца и занимались криптографией.

Рис. 5. Восстановленный ключ к шифру, использованному при составлении документа.

28. См. Доклад Е. Г. Домниной на конференции в Линчёпингском университете (Швеция, 2018 г.): *Domnina E.* Nicodemo Tranchedini's Diplomatic Cipher: New Evidence. Linköping, 2018. P. 5 [Электронный ресурс]. URL: http://www.ep.liu.se/ecp/149/007/ecp18149007.pdf (дата обращения: 1.12.2018).

29. Рукопись опубликована два раза в 1970 г. в Австрии и Италии: Diplomatische Geheimschriften. Codex Vindobonensis 2398 der Oesterreichischen Nationalbibliothek / hrsg. W. Höflechner. Graz, 1970; *Cerioni L.* La Diplomazia sforzesca nella seconda metà del Quattrocento e i suoi cifrari segreti. Roma, 1970. Vol. 1–2. В доступном Е. Г. Домниной итальянском издании дано факсимиле венской рукописи, в котором наш шифр опубликован на странице 23.

Данные рукописи Ф. Транкедини показывают, что нам с помощью примененного компьютерного метода удалось правильно дешифровать практически все (95%) символы. Оставшиеся одиночные значки кодировали слова «Papa», «Neapolis», «exercitus» и «galee». Пятый одиночный символ оказался пустым. Стоит также отметить, что арагонский писец, использовавший миланский шифр, по всей видимости, изменил значение одного из значков, довольно часто встречающегося в грамоте: у Транкедини он указывал на правителя Наварры, тогда как в королевском письме шифровал просто букву «t».

Знание одиночных символов позволило уточнить отдельные моменты в тексте исследованного нами документа, хотя и не повлияло существенно на понимание его общего смысла — таким образом, изначально примененный нами компьютерный метод обработки шифра пропорциональной замены действительно оказался плодотворным.

Подводя итог, следует отметить, что изучение и дешифровка средневековых зашифрованных документов требует от исследователя усидчивости, внимательности, наличия языковой подготовки (в том числе в области сравнительной лингвистики, хотя бы на элементарном уровне), а также, в определенной мере, находчивости. Дешифровку текста необходимо выполнять поэтапно: определение языка, частотный анализ (там, где он возможен), изучение структурных особенностей текста (то есть выявление устойчивых буквосочетаний, окончаний слов и т. п.) и самый трудоемкий этап работы — установление всех буквенно-символьных сочетаний. Разумнее всего выполнять данные задачи с использованием компьютера, а не вручную: это не только сэкономит много времени, но и позволит исследователю увидеть весь текст «в перспективе».

Приложенные усилия, несомненно, окупятся. Зашифрованные документы не только представляют большой интерес с точки зрения получения дополнительной информации для углубления наших знаний по истории того или иного периода, но и, в некоторых случаях, позволяют скорректировать суще-

ствовавшие ранее представления о ключевых событиях эпохи[30]. В нашем случае дешифрованное письмо Хуана II в Милан вскрыло отдельные детали подготовки арагонского короля к военной кампании против лотарингского герцога и Генуэзской республики, посягнувших на подконтрольное Арагонской Короне Неаполитанское королевство.

30. *Домнина Е. Г.* Томмазо Спинелли и его шифры.

СПИСОК НЕОПУБЛИКОВАННЫХ ИСТОЧНИКОВ

1. Западноевропейская секция Научно-исторического архива Санкт-Петербургского института истории РАН (ЗЕС НИА СПб ИИ РАН). Коллекция 14: Акты и письма политических деятелей Испании IX–XIX вв. Картон 292. №12. Л. 1r, 1v, 2r, 2v.

СПИСОК ОПУБЛИКОВАННЫХ ИСТОЧНИКОВ

1. *Ватсьяяна Малланага.* Камасутра / пер. с санскрита, вступ. статья и комм. А. Я. Сыркина. Москва: Наука; Издательская фирма «Восточная литература», 1993. (Памятники письменности Востока; CXI).
2. *Гай Светоний Транквилл.* Жизнь двенадцати цезарей / пер. с лат. М. Л. Гаспарова, изд. подг. М. Л. Гаспаров, Е. М. Штаерман. Москва: Наука, 1964. (Литературные памятники).
3. *Корнелий Тацит.* О происхождении германцев и местоположении Германии / пер. с лат. и комм. А. С. Бобовича под ред. М. Е. Сергеенко // *Корнелий Тацит.* Сочинения в двух томах. Ленинград: Наука, 1969. Т. 1. Анналы. Малые произведения / изд. подг. А. С. Бобович, Я. М. Боровский, М. Е. Сергеенко. С. 353–372. (Литературные памятники).
4. Хожение за три моря Афанасия Никитина 1466–1472 гг. / пер. с древнерусс. А. Д. Желтякова и Л. С. Семенова, изд. подг. Я. С. Лурье, Л. С. Семенов. Ленинград: Наука, 1986. (Литературные памятники).
5. *Sáez E., Sáez C.* El fondo español del Archivo de la Academia de las Ciencias de San Petersburgo. Alcalá de Henares: Servicio de Publicaciones de la Universidad de Alcalá, 1993.

СПИСОК ЛИТЕРАТУРЫ

1. *Адаменко М. В.* Основы классической криптологии: секреты шифров и кодов. Москва: ДМК Пресс, 2012.
2. *Домнина Е. Г.* Томмазо Спинелли и его шифры (из истории криптографии раннего Нового времени) [Электронный ресурс] // Материалы XIV Международной конференции студентов, аспирантов и молодых ученых «Ломоносов – 2007» URL: *https://lomonosov-msu.ru/archive/Lomonosov_2007/12/WH/Domnina.pdf* (дата обращения: 1.12.2018).
3. *Домнина Е. Г.* Шифры в дипломатии ранних Тюдоров: на материале личной переписки Томмазо Спинелли // Искусство и культура Европы эпохи Возрождения и раннего Нового времени. Сборник трудов в честь В. М. Володарского / под ред. Т. П. Гусаровой. Москва; Санкт-Петербург: Центр гуманитарных инициатив, 2016. С. 254–265.
4. *Калмыкова Е. В.* Образы войны в исторических представлениях англичан позднего Средневековья. Москва: Квадрига, 2010. (Исторические исследования).
5. *Леонтьев А. А.* Папуасские языки. Москва: Наука, 1974. (Языки народов Азии и Африки).
6. *Русецкая И. А.* История криптографии в Западной Европе в раннее Новое время. Санкт-Петербург: Центр гуманитарных инициатив, Университетская книга, 2014.
7. *Селянинов О. П.* Тетради по дипломатической службе государств: История и современность. Москва: Анкил, 1998.
8. *Черняк Е. Б.* Пять столетий тайной войны. Из истории секретной дипломатии и разведки. 2-е, перераб. изд. Москва: Международные отношения, 1972.
9. *Balard M.* Le chiffre à la chancellerie ducale de Gênes dans la seconde moitié du XVe siècle // La communication dans l'histoire. Tricentenaire de Colbert. Colloque de Reims, septembre 1983. Reims, 1985. P. 169–187. (Travaux de l'Académie Nationale de Reims; 164).
10. *Barksdale-Shaw L. M.* "That You Are Both Decipher'd". Revealing Espionage and Staging Written Evidence in Early Modern England // A Material History of Medieval and Early Modern Ciphers. Cryptography and the History of Literacy / ed. by K. Ellison, S. Kim. New York; London: Routledge, Taylor & Francis Group, 2018. P. 118–136. (Material Readings in Early Modern Culture).
11. *Cerioni L.* La Diplomazia sforzesca nella seconda metà del Quattrocento e i suoi cifrari segreti. Roma: Il centro di ricerca, 1970. Vols. 1–2.

12. Diplomatische Geheimschriften. Codex Vindobonensis 2398 der Oesterreichischen Nationalbibliothek / Faksimileausg. Einf. W. Höflechner. Graz: Akademische Druck- und Verlagsanstalt, 1970. (Codices selecti phototypice impressi; 22).
13. *Domnina E.* Nicodemo Tranchedini's Diplomatic Cipher: New Evidence. Linköping: Linköping University Electronic Press, 2018. P. 5 [Электронный ресурс]. URL: http://www.ep.liu.se/ecp/149/007/ecp18149007.pdf (дата обращения: 1.12.2018).
14. *Galende Díaz J. C.* La escritura cifrada durante el reinado de los Reyes Católicos y Carlos V // Cuadernos de estudios medievales y ciencias y técnicas historiográficas. 1993–1994. №18–19. P. 159–178.
15. *Galende Díaz J. C.* Elementos y sistemas criptográficos en la escritura visigótica // VIII Jornadas Científicas sobre Documentación de la Hispania altomedieval (siglos VI–X) / dir. J. C. Galende Díaz, J. de Santiago Fernández, ed. N. Ávila Seoane, M. J. Salamanca López, L. Zozaya Montes. Madrid: Universidad Complutense de Madrid, 2009. P. 173–183.
16. *Kalyanaraman S.* Sarasvati Hieroglyphs and Bharatiya Cultural Continuum. Lecchita Vikalpa and Bharatiya Sabhyata // PILC Journal of Dravidic Studies. 2002. Vol. 12(1). P. 17–36.
17. *Martínez Pereiro C. P.* Del combate singular al singular combate sexual en la sátira trovadoresca medieval gallego-portuguesa // Floema. Caderno de Teoria e História Literária. 2009. №5. P. 17–32.
18. *Swift C.* Christian Communities in Fifth and Sixth Century Ireland // Trowel. The Journal of the Archaeological Society, University College Dublin. 1996. Vol. 7. P. 21–32.