

ИСТОРИЯ МАТЕМАТИКИ И МАТЕМАТИЧЕСКОГО ОБРАЗОВАНИЯ.  
ПЕРСОНАЛИИ

УДК 511

ШИФР, КОТОРЫЙ РАЗГАДАЛ  
ХРИСТИАН ГОЛЬДБАХ\*

Н. С. Калинин

*Санкт-Петербургский Государственный Университет,  
Санкт-Петербург, Россия*

nikaanspb@gmail.com

Любое чётное число, большее двух, является суммой двух простых – такая гипотеза родилась в 1742 г. в переписке Христиана Гольдбаха (Петербург) с Эйлером (Берлин). Чуть менее известно, что именно Гольдбах заинтересовал Эйлера теорией чисел в их обширной переписке. Ещё менее известно, что с 1742 г. Гольдбах работал в «чёрных кабинетах» (Cabinet Noir), где занимался расшифровкой писем иностранных послов. В настоящей работе обсуждается письмо (с шифром и расшифровкой) французского посла маркиза де Шетарди от 15 февраля 1744 г., которое, будучи показанным императрице Елизавете, привело к высылке посла. Указано устройство шифра и приведены соображения о том, насколько сложно было его взломать.

*Ключевые слова:* шифр, шифрование, политика, Гольдбах, Академия Наук, Франция.

Приехав в 1743 г. в Россию во второй раз, Маркиз де Шетарди<sup>1</sup> рассчитывал на доброе к нему отношение императрицы Елизаветы. Он знал, что его письма во Францию перехватываются русскими, но был абсолютно уверен, что используемый им шифр разгадать невозможно, и потому писал открыто всё, что думает, желая своей осведомлённостью поразить французского короля. Например: «... Императрица, в силу лениости сложила все дела на

---

\*Работа выполнена при поддержке Российского научного фонда, грант №20-71-00007

<sup>1</sup>Jacques-Joachim Trotti marquis de la Chétardie, 1705–1759. Французский посол в России в 1739–1742, 1743–1744 гг. Принимал участие в перевороте 1741 г., при котором Елизавета стала императрицей, см. [2]. Часто упоминается в фильме «Гардемарины, вперёд!».

*Бестужева...*<sup>2</sup> — из его письма от 15 февраля 1744 г., которое мы и будем, в основном, обсуждать.

Как оказалось, Шетарди использовал так называемый Великий Шифр (Grand Chiffre), разработанный Антуаном Россиньолем<sup>3</sup>. В этом шифре трёхзначные числа кодируют слова, буквы, звуки и слоги, для часто повторяющихся слогов используются несколько чисел вперемешку. Кроме того, какие-то числа не означают ничего, их добавляют, чтобы шифр было сложнее взломать.

Бестужев-Рюмин<sup>4</sup> понимал необходимость расшифровки иностранной корреспонденции, и в 1742 г. переманил Христиана Гольдбаха<sup>5</sup> из Академии Наук на службу в Коллегию иностранных дел, с зарплатой 1500 рублей в год (примерно 200–400 тыс. рублей в месяц на 2021 г., сравнение основано на стоимости хлеба, водки и услуг извозчиков).

Гольдбах справился с шифром Шетарди не сразу — но к 1744 г. он уже имел двухлетний опыт разгадывания шифров, и если первые шифры он разгадывал весь первый год своей службы, то этот шифр он взломал за две недели.

Начало письма от 15 февраля выглядит так:

« 335 632 679 498 283 249 202  
97 996 752 786 983 95 155 900  
591 179 23 478 987 742 597 36 659  
933 894 126 527 97 99 813 865 780 898  
958 432 507 302 514 694 611 510 661 56  
414 506 406 359 95 358 712 562 715  
900 219 51 498 111 823 880 466 ...»

В этом фрагменте 335 632 679 не означают ничего (назовём такие числа мусорными), и добавлены для усложнения жизни читающего.

Далее, выпишем по одному слову в строчку (с примерным переводом):

498(Eπ)	
283(re)249(marq)202(ant)	заметим
97(que)	что

---

<sup>2</sup>Полностью: “Le mal augmentait sans doute par la mort de M. Brevern, si la Tsarine en donnant trop par indolences pour les affaires a l’habitude de se trouver vis a vis de vice chancelier le laissons seul en place.” В приведённом зашифрованном фрагменте это часть текста, начинающегося с 510 661 56 ...

<sup>3</sup>Antoine Rossignol, 1600–1682. В 1626 г. взломал шифр письма из осаждённой крепости Реальмон, что привело к её падению. Этим Россиньоль привлек к себе внимание Ришелье, который понимал важность шифрования в политических и военных делах. Россиньоль и его потомки возглавляли шифровальную службу при французском дворе.

<sup>4</sup>Алексей Петрович Бестужев-Рюмин, 1693–1766. Вице-канцлер (1741–1744) и затем канцлер (1744–1758) Российской Империи при императрице Елизавете Петровне.

<sup>5</sup>Christian Goldbach, 1690–1764. Математик, один из первых членов Академии Наук, основанной Петром I.

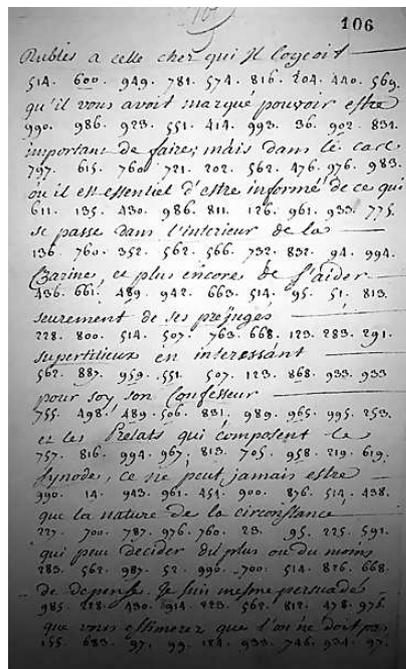
996(tout)	всё
752(est)	находится
786(мусор)	
983(dans)	в
95(la)	
155(meme)	той же самой
900(si)591(tu)179(ation)	ситуации
...	
359(par)95(la)358(m)712(ort) 562(de)715(Brevern)	
Par la mort de Brevern	со смертью Бреверна (см. вторую сноску).

Архив министерства иностранных дел (именно там хранятся расшифровки, сделанные рукой Гольдбаха) до сих пор закрыт для внешних посетителей. Возможно, так было не всегда – Соболева Т. А., автор книги [1], обильно его цитирует. Так или иначе, автору этой заметки пришлось искать французских историков и просить их добыть донесения Шетарди из французских архивов, которые как раз доступны для всех.

Во Франции полученные от Шетарди письма дешифрованы и хранятся в "Archives du ministère des Affaires Étrangères", 2 rue Suzanne Masson, 93120 La Courneuve, France. Большое спасибо Jean-Fred Warlin за фотографию писем! Ниже приведена фотография одной страницы из такого письма.

Текст на этой странице: «[600] roubles à celle chez qui il logeait, qu'il vous avait marqué pouvoir être important de faire, mais, dans les cas où il est essentiel d'être informé de ce qui se passe dans l'intérieur de la Tsarine, et plus encore de s'aider sûrement de ses préjugés superstitieux en intéressant pour soi son confesseur et les prélats qui composent son synode, ce ne peut jamais être que la nature de la circonstance qui peut décider du plus ou du moins de dépense. Je suis même persuadé que vous estimerez qu'on ne doit pas...»

Речь идёт о том, что Шетарди подкупил кого-то, кто живёт вместе с Михаилом Голицыным (1684–1764), и, чтобы лучше знать, что происходит в окружении Царицы, нужно подкупить её духовника и синод, чтобы затем пользоваться её суеверностью. Сколько понадобится денег, заранее предсказать невозможно [Шетарди просит о финансировании].



Не так просто разгадать шифр, даже имея расшифрованную версию перед глазами. Автор этой заметки сначала предположил, что слова в одной строчке соответствуют числам из следующей строчки, и пытался найти соответствия. Это не так. Человек, который расшифровывал письма, писал поверх шифра, заполняя строчки переводом до конца, и потому возникает рассинхронизация — обычно соответствующие числа идут несколькими строками ниже. Иногда перевод выполнен по смыслу, а не дословно, иногда дешифровщику не удаётся понять, что имеется в виду — может быть из-за опечаток, сделанных при шифровке.

Дело пошло быстрее, когда, после нескольких часов изучения текста, автор заметки предположил, что число 51 соответствует слову Tsarine (Царица<sup>6</sup>). Это позволило сопоставлять с соответствующим текстом до и после слова «Царица» числа немного после и немного ранее 51.

Обратите внимание на старое правописание — *logeoit* вместо современного *logeait*, *seurement* вместо *sûrement*. Иногда Шетарди кодирует записанное слово (именно то, как оно пишется), иногда лишь его произношение, иногда пользуется сокращениями, когда слово понятно из контекста.

Например, *deux* = 136(d')755(eu), *faits* = 216(fait)816(s), *ulcéré* = 339(u)574(l')438(cé)283(ré).

Как же Гольдбах мог разгадать такой шифр? Дадим ему слово (из письма Гольдбаха Бестужеву-Рюмину<sup>7</sup>):

*«Милостивый государь мой!*

*Принося Вашему сиятельству первые плоды третьяго цифирного ключа, надеюсь, что вместо нареkania мне какого-либо в том медленя, паче моей поспешности удивляться причину иметь будут, ежели когда-нибудь соизволено будет сличать самой ключ с разобранными письмами и когда усмотрится, что потребно было каждое число или каждую цифру весьма прилежно свидетельствовать, нежели возможно было познать содержание хотя б одного письма. Но понеже сия работа уже сделана, то я в состоянии нахожусь, в день по одной пиесе разобрав, отдавать, ежели я, однако ж, другими делами от того отторгнут не буду.*

*Что же касается до четвёртого и пятого ключей, от которого я ещё несколько штук [писем] в руках имею, то оныя ключи несравненно труднее первых нахожу...»*

Как только правильно разгаданы хотя бы несколько чисел (или известно примерное содержание письма), дальнейшая дешифровка многократно упрощается. Мы можем предполагать, что Гольдбах знал французский, имел представление о текущей политической обстановке и понимал, что числа шифруют не буквы, а слоги или даже слова.

---

<sup>6</sup>Вопрос, можно ли называть Елизавету Императрицей, был вопросом политическим. Елизавета требовала этого, но другие правители далеко не сразу разрешили своим послам титуловать её Императрицей.

<sup>7</sup>Из АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 16. Л. 178–178 об., см. [1]

Мы можем также предполагать, что Гольдбах получал все письма Шетарди — технология перехватывания писем, их распечатки, копирования и обратного запечатывания без видимых следов к тому времени была хорошо отработана.

Даже в этом случае совсем неясно, как разгадывать такой шифр: потому Шетарди, по возвращении во Францию, 27 сентября 1744 г., заключил своего слугу-секретаря Dupré (который имел доступ к шифру) в Бастилию<sup>8</sup>, подозревая предательство с его стороны. Секретаря допрашивали пять месяцев, потом отпустили, найдя совершенно невиновным и наивным простым человеком (и Людовик XV даже назначил ему компенсацию за время, проведённое в тюрьме).

Однако, что-то угадать можно и без доступа к шифру. Например, частотный анализ чисел показывает, что некоторые числа встречаются намного чаще других. Приведём те, что встретились более 20 раз в этом письме:

95(la) — 35 раз,  
97(que) — 31 раз,  
204(à) — 33 раз,  
283(râi) или (r, ré) — 27 раз,  
451(le) — 24 раза,  
507(s') — 21 раз,  
562(de) или (dé) — 39 раз,  
813(et) — 22 раза,  
989(pour) — 22 раза.

Так что, хотя частотный анализ напрямую и не применим, Гольдбах мог сопоставить этим числам наиболее частые французские слоги, что значительно сокращало перебор вариантов.

Далее, в письме встречаются числа, и они не зашифрованы, например, *dépêches des 18 et 25 janvier* выглядит как 444 984 18 813 25 246. Письма доходили не всегда, Шетарди посылал некоторые письма по два раза, и, значит, должен был об этом писать — упоминая датировку писем. Отсюда мы узнаём, что 813 — это *et* (и), а 246 — *janvier* (январь).

В словах, вообще говоря, довольно редко бывают повторы слогов: *superstitieux* — 123(su)868(pers)933(ti)933(ti)55(eux). Безусловно, Гольдбах имел список слов с повторами слогов. Иногда Шетарди начинал или заканчивал письма абзацем незашифрованного текста (например, говоря, что он посылал уже это письмо, и дублирует его на всякий случай). В случае неосмотрительности, такие письма могли быть не абсолютно идентичны — что дало бы информацию, какие числа обозначают одно и то же. В конце концов, в руки Гольдбаха мог попасть какой-то черновик письма из мусора, который можно было сличить со всеми зашифрованными письмами, и этого бы уже хватило для расшифровки.

---

<sup>8</sup>Стр. 379 и Аппеке 75 в [3].

То, что некоторые числа означают целые слова, не видится проблемой – обычно из контекста ясно, о чём речь. Например,

4 Moscou	Москва
6 S.M. (Sa Majeste?)	Людовик XV
10 Frédéric II (rois de Prusse), Prusse	Фридрих II, или Пруссия
14 com или comme	слог «ком», слово «как»
17 l'empereur (Charles VII)	император Карл VII
21 maison	дом
23 que	слоги «кё», «ке», слово «который»
25 Stockholm	Стокгольм
26 meditation	размышления
36 vous, vou	слог «ву», слово «вы»
40 insinuer	
41 assuré	
48 tran	
51 Tsarine	
52 circonstance	
56 augment	
70 Danemark	
81 Copenhague	
84 Suède, Suédois	
94 pas	
99 vous	
103 Cologne	

Хотя взлом такого шифра поначалу кажется совершенно безнадёжной задачей, мы видим, что у Гольдбаха было множество способов найти зацепку, ведь Шетарди, будучи уверенным в том, что шифр взломать невозможно, вряд ли следил за частотностью чисел или упоминанием дат.

Так или иначе, 17 июня 1744 г. в три часа ночи к Шетарди пришли казаки во главе с генералом Ушаковым и приказали маркизу покинуть Москву в течение дня и Россию в течение восьми дней, силой отобрали портрет Елизаветы, ему подаренный самой императрицей.

В январе 1744 г. с Гольдбахом был перезаключён договор о службе в России именно на основании его успехов в дешифровальной деятельности. Из протоколов докладов Елизавете от 3 января 1744 г.: «... 18. *Слушать же и всемилостивийше апробовать соизволила проект заключаемого статским советником Гольдбахом о вступлении его в российскую службу контракта. И при том по всеподданнейшему докладу, не соизволено ль будет ему, Гольдбаху, за прилежные его труды и особливое искусство в разбирании цифирных секретных писем в награждение до 1000 рублей пожаловать, Ея Императорское Величество на сие всемилостивийше соизволила*»<sup>9</sup>.

---

<sup>9</sup>Из АВПРИ. Ф. Секретнейшие дела. Оп. 6/1. Д. 16. Л. 154. , см. [1].

Краткое содержание (на русском языке) всех дипломатических писем Шетарди из французских архивов можно найти в [4].

Содержание письма Гольдбаха к Эйлеру, где сформулировано то, что впоследствии станет называться гипотезой Гольдбаха, историю продвижений и историографических ошибок в атрибуции успехов в тернарной гипотезе Гольдбаха можно найти в [5].

Для любопытного читателя приведём большой кусок обсуждаемого письма (знаком ? отмечены числа, которые плохо видны на фотографиях письма):

roubles à celle chez qui il logeoit (Michel Galitzine, lettre 77)

514 600 949 781 574 816 204 440 569

qu'il vous avoit (avait) marqué pouvoir être

990 986 923 551 414 993 36 902 831

important de faire, mais, dans les cas

797 615 760 721 202 562 476 976 983

où il est essentiel d'être informé de ce qui

611 135 430 986 811 126 961 933 775

se passe dans l'intérieur de la (d'Élisabeth),

136 760 352 562 566 732 832 94 994

Tsarine et plus encore de s'aider

436 661 489 942 663 514 95 51 813

[seurement] de ses préjugés

228 800 514 507 763 668 123 283 291

superstitieux en intéressant

562 887 959 551 507 123 868 933 933

pour soy son confesseur

755 498 489 506 831 989 965 995 253

et les prélats qui composent le (son)

575 816 994 967 813 705 958 219 619

synode, ce ne peut jamais être

990 14 943 961 451 900 876 514 438

que la nature de la circonstance

227 700 787 976 760 23 95 225 591

qui peut décider le plus ou moins

283 562 987 52 990 700 514 826 668

de dépense. Je suis même persuadé

985 228 430 914 223 562 812 478 975

que vous estimerez qu'on ne doit pas,

155 683 97 99 124 933 746 934 95

telle (quelque) qu'elle soit, y avoir regret,

834 227 912 307 501 661 451 264 961

quand par l'expérience que  
309 178 779 283 571 831 638 359 ?

de Brümmer en a fait plusieurs  
474 942 498 438 23 580 562 516 ?

fois et notamment pour le  
550 204 765 152 228 939 694 813 ?

mariage avec la Jeune [de] Sophie [d'Anhalt]-  
746 146 989 611 510 942 519 277 ?

Zerbst, que la parenté semblait  
478 998 725 301 296 181 431 97 ?

rendre impossible, suivant le  
167 935 501 883 414 585 342 183 ?

rite grec ; il est démontré que cette  
942 501 571 515 986 811 514 306 ?

voie est toujours infaillible pour  
23 529 969 752 144 119 596 896 ?

déterminer la Tsarine [Élisabeth.]  
425 947 445 219 51

Je vous représenterai encore  
335 787 961 763 661 105 ?

Monsieur, avec la même franchise  
514 99 283 381 426 277 95 155 ?

qu'il est fâcheux que ce portrait, que  
821 832 993 752 596 569 755 97 ?

S.M. lui destine, loin d'être achevé,  
877 182 307 23 6 984 933 227 ?

ne fût pas commencé le 17  
119 136 760 204 569 997 227 169 ?

janvier. Je vous deguise la verite  
941 14 576 438 451 17 246 478 99

en ne vous disant point qu'autant  
514 815 756 994 952 95 160 550 376

ces sortes de choses, lorsqu'elles ont  
36 911 202 226 484 180 982 968 562

été annoncées, demandent à être  
442 234 264 404 126 501 818 317 527

consommées promptement pour en  
126 563 508 133 760 253 324 649 47

retirer l'utilité qu'on s'en promet,  
989 498 283 953 426 574 269 991 816

autant elles produisent souvent un  
550 886 429 180 842 886 989 357 491

mauvais effet et détruisent  
792 890 978 252 813 514 957 357 491

gratuitement ce qu'on en  
658 591 511 501 146 438 97 834 498

espérait quand on les fait attendre si  
392 414 638 261 375 765 847 861 794

longtemps.  
900 834 850

### Литература

- [1] Соболева Т. А. История шифровального дела в России. Олма-Пресс Образование, 2002. 512 с. <https://www.litmir.me/br/285925&p=25>
- [2] Лиштенан Ф.-Д. Елизавета Петровна. Императрица, не похожая на других. АСТ, 2012. [https://royallib.com/book/lishtenan\\_fransina\\_dominik/elizaveta\\_petrovna\\_imperatritsa\\_ne\\_pohogaya\\_na\\_drugih.html](https://royallib.com/book/lishtenan_fransina_dominik/elizaveta_petrovna_imperatritsa_ne_pohogaya_na_drugih.html)
- [3] Jean-Fred Warlin. Représenter la France à la cour des tsarines. Les deux ambassades de Joachim-Jacques de La Chétardie de 1739 à 1744. THÈSE pour obtenir le grade de docteur de l'université Paris-Sorbonne.  
<https://hal.archives-ouvertes.fr/tel-01727686/document>
- [4] Сборник Императорского Русского исторического общества. — С.-Петербург, 1867–1916. Т. 105: [Дипломатическая переписка французских посланников и агентов при русском дворе. Ч. 13]. — С.Петербург: Типография М. Стасюлевича, 1899. Донесения французского посла при русском дворе маркиза де-ла-Шетарди и уполномочен. министра д'Аллиона с 1743 по 1745 г.  
<https://www.prlib.ru/item/363601>
- [5] Вавилов Н. А. Компьютер как новая реальность математики. IV: Проблема Гольдбаха // Компьютерные инструменты в образовании. 2020. № 2. С. 2–59.

Поступила 08.05.2021

## A CIPHER BROKEN BY CHRISTIAN GOLDBACH

*N. S. Kalinin*

Each even number bigger than two is a sum of two prime numbers. This conjecture is well-known, it was born in 1742 in the correspondence between Christian Goldbach (Saint Petersburg) and Leonard Euler (Berlin at that time). It is considerably less known that it was Goldbach who excited the Euler's curiosity in number theory in his innumerable letters. Even much less known is that since 1742 Goldbach leaded so-called Cabinet Noirs in the Russian Empire. In plain words, he was deciphering letters of foreign ambassadors. In this paper we discuss one of such letters (dated 15 February 1744) which, being shown to Empress Elizabeth, resulted in the deportation of marquise de Chetardie. We describe the cipher and guess how it could be broken by Goldbach.

*Keywords:* cipher, politics, Goldbach, Russian Academy of Sciences, France.