

FRIEDERICH JOHANN BUCK: ARITHMETIC PUZZLES IN CRYPTOGRAPHY

JOACHIM VON ZUR GATHEN

9th July 2004

Abstract. Much of modern cryptography relies on arithmetic—from RSA and elliptic curves to the AES. A little-known book by Comiers, published in 1690, seems to be the first recorded systematic use of arithmetic in cryptography. David Kahn’s authoritative *The Codebreakers* mentions another work whose title links algebra and cryptography—“by a German, F. J. Buck, as far back as 1772”. It turns out to deal with mathematical puzzles. Buck uses such brain teasers to encode numbers, and thus letters and whole messages. For decoding, one has to be clever enough to solve those puzzles. There is no secret key involved. Other well-known examples of such “keyless” cryptography are mentioned.

1. Introduction

This paper discusses a 15-page work from 1772 by Buck whose title brings together cryptography and algebra. Kahn (1967), page 405, writes about Lester S. Hill, who introduced linear algebra into cryptography: “Hill successfully used algebra as a process for cryptography. Probably many mathematicians had toyed with this idea; two proposals had even reached print—one by a German, F. J. Buck, as far back as 1772, the other by the young mathematician Jack Levine in a 1926 issue of a detective magazine.” Buck’s work was available to Kahn only as a citation in a bibliography by Maurits de Vries. The present analysis will show that it does not represent cryptography in the usual sense: there is no secret key, and the legitimate recipient has no advantage over an interceptor. Rather it is a game of hiding messages inside algebraical puzzles.

In the usual cryptographic scenario, someone sends an encrypted message to a correspondent who can decrypt it easily with the help of a secret key, and an interceptor cannot (easily) determine the plaintext from just the ciphertext. In Buck’s setting, the secret key is replaced by the general ability to solve certain types of mathematical puzzles. Thus, if used for secret communication, it

is secure against any interceptor who lacks this ability (and the funds to hire someone with the required ability). This might be called “keyless cryptography”. In Section 5, we put some other well-known cryptographic systems into this framework.

The core of Buck’s text consists of two sets of five puzzles, each set encrypting some plaintext. The first set is literally taken from Schwarzer’s 1762 *Arithmetic*, with acknowledgement. The second set is made up by Buck himself. The solution to each puzzle yields some (one to six) numbers. Each such number in turn provides some (up to six) letters in specified positions in specified words of the plaintext. This happens via lengthy but straightforward instructions and the usual conversion of the numbers from 1 to 24 into the 24 letters of the alphabet of his times.

For use as a system of secret communication, the sender has to devise a set of numerical puzzles plus instructions that specify each letter of his message. This is easy to do for a “doctor of world wisdom” like Buck, at least in principle. The puzzles and instructions are sent as the ciphertext. The recipient must solve the puzzles and follow the instructions to recover the plaintext, letter by letter.

There is no secret key, and the intended recipient has no advantage over an undesired interceptor. This could work in a circle of doctors of world wisdom, where any interceptor may be assumed to lack the necessary amount of world wisdom. It could not be considered as a general system of secure communication, not even in Buck’s times.

The present paper proceeds as follows. Section 2 lays out Buck’s story as told by him. In Section 3, a sample puzzle is solved. It turns out that both the puzzles and the instructions contain numerous errors, and their solution indeed requires a modicum of world wisdom. Section 4 describes Buck’s life and his university, with his famous colleague Immanuel Kant, and the works that he quoted, by Schwarzer and by Lindner. Section 5 briefly mentions other examples of such keyless cryptography throughout history.

The full text of Buck’s book is available at

<http://www.math.upb.de/~aggathen/Publications/>

with kind permission of the Martin-Luther-Universität at Halle-Wittenberg.

2. Buck’s book

The title page of the work by Buck is shown in Figure 1 and translates as:

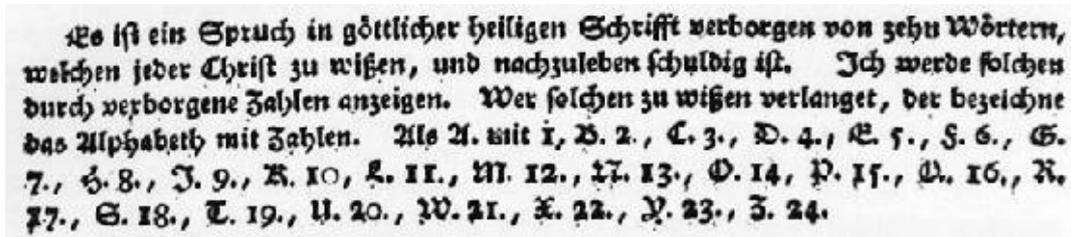


Figure 1: The title page of Buck's book

1) Zergliedere 96. in 2. progressionen, arithmetica & geometrica, jede von 3. terminis. Wenn man den kleinsten terminum der arithmetischen Progression mit dem kleinsten der geometrischen multipliciret, Kommt 24, das product derer medianorum auch vervielfältiget, Kommt 131, und die zwey terminos von beyden Zahlreihen multipliciret, entsteht 672. Wenn man zu der ersten Zahl der arithmetischen progression 12. addiret, so Kommt der erste Buchstaben des ersten Worts, und der dritte des zehnten, auch der erste des zweyten Worts. Wenn man von der zweyten Zahl der arithmetischen progression 2. subtrahiret, so zeigt der Rest den zweyten Buchstaben des dritten Worts, und den ersten Buchstaben des vierten Worts, wie auch den zweyten des fünfften und zweyten des sechsten, und den zweyten des siebenden, abermahl den zweyten des neunten Worts an. Dividiret in die dritte arithmetische progression mit 7., so Kommt der dritte Buchstaben des dritten Worts. Dividiret mit 3. in die geometrische progression der ersten Zahl, so Kommt der zweyten Buchstaben des ersten Worts, und der zweyte des achten. Addiret zu der zweyten geometrischen progression 7., so Kommt der dritte und vierte Buchstaben des ersten, und der erste des zehnten Worts. Dividiret abermahl mit 6. in die dritte Zahl, so wird der Quotient zeigen den zweyten Buchstaben vom zehnten Worte.

Figure 2: Schwarzer's first puzzle, as copied by Buck

1) Subdivide 96 into two progressions, one arithmetic and one geometric, of three terms each. If you multiply the smallest term of the arithmetic progression with the small one of the geometric sequence, you obtain 24. The product of the middle terms gives 131, and if you multiply the two final terms of both sequences, 672 arises. If you add 12 to the first term of the arithmetic progression, the first letter of the first word shows up, and the third of the tenth, and also the first of the second word. If you subtract 2 from the second number of the arithmetic progression, the remainder yields the second letter of the third word, and the first letter of the fourth word, as well as the second of the fifth, the second of the sixth, and the second of the seventh, and again the second of the ninth word. Divide the third term of the arithmetic progression by 7, then you get the third letter of the third word. Divide the first number of the geometric progression by 3, and you will find the second letter of the first word, and the second of the eighth one. Add 7 to the second geometric term to obtain the third and fourth letter of the first, and the first of the tenth word. Divide again the third number by 6, then the quotient will show the second letter of the tenth word.



Es ist ein Spruch in göttlicher heiligen Schrift verborgen von zehn Wörtern, welchen jeder Christ zu wissen, und nachzuleben schuldig ist. Ich werde solchen durch verborgene Zahlen anzeigen. Wer solchen zu wissen verlangt, der bezeichne das Alphabeth mit Zahlen. Als A. mit 1, B. 2., C. 3., D. 4., E. 5., F. 6., G. 7., H. 8., I. 9., K. 10, L. 11., M. 12., N. 13., O. 14, P. 15., Q. 16., R. 17., S. 18., T. 19., U. 20., W. 21., X. 22., Y. 23., Z. 24.

Figure 3: Buck’s conversion from letters to numbers, based on Schwarzer

There is an admonition of ten words hidden in the divine holy scripture, which every Christian has the duty to know and to follow. I will indicate it with hidden numbers. Whoever desires to know it, should designate the alphabet by numbers. Such as A. by 1, B. 2., C. 3., D. 4., E. 5., F. 6., G. 7., H. 8., I. 9., K. 10, L. 11., M. 12., N. 13., O. 14, P. 15., Q. 16., R. 17., S. 18., T. 19., U. 20., W. 21., X. 22., Y. 23., Z. 24.

Mathematical proof that algebra can comfortably be used to disclose some ways of secret writing. By Friederich Johann Buck, doctor of philosophy (“Weltweißeheit” = “world wisdom”) and jurisprudence, as well as professor of mathematics at the University of Königsberg. Königsberg, 1772. Published by the widow of J. D. Zeisen and the heirs of J. H. Hartung.

The booklet comprises 12 sections on 15 pages. The first sentence sets the author’s goal: “When I had the pleasure, a few months ago, of reading the nice memoir *de arte decifferatoria* of our praiseworthy professor Lindner, the following question came unexpectedly to my mind: whether one can also use algebra to decipher secret writing.”¹ He goes on to say how he ruminated a while on this possibility, and was pointed in the right direction by a miraculous incident: “A few weeks ago a diligent and disciplined student, Herr Studiosus Meltzbach the younger, handed me a little note asking me to resolve the mathematical problems written there without complaint. A teacher is always obliged to heed a noble request of his auditor, in order to satisfy his honest quest for knowledge and as well to entice him to similar endeavors in the future. For this reason I humbly accepted his writing, read it with alacrity in his presence, and added the promise to deliver to him the solutions to the submitted problems

¹Buck’s original words, in the quaint German of his times, are: Als ich vor wenigen Monathen das Vergnügen hatte, die schöne Disputation unseres ruhmwürdigen Herrn Professor Lindners *de arte decifferatoria* zu lesen; so fiel mir unvermuthet die Frage ein: Ob zur Entdeckung verborgener Schriften auch die Algebra angewendet werden könne?

the next day.”² These tasks were five simple arithmetic puzzles. The first one is shown in Figure 2, translated below, and asks, in modern terms, for three-term arithmetic and geometric progressions, say

$$(a, a + d, a + 2d) \text{ and } (b, bq, bq^2),$$

with the properties that

$$(1) \quad \begin{aligned} a + (a + d) + (a + 2d) + b + bq + bq^2 &= 96, & ab &= 24, \\ (a + d)bq &= 131, & (a + 2d)bq^2 &= 672. \end{aligned}$$

Buck says that certain letters are given by the numbers calculated, but only the next paragraph specifies that correspondence. Following some rather involved instructions, as starting on line 5 of Figure 2, each such number yields some letters in certain positions of the plaintext. Namely, $a + 12$ gives the first letter of the first word in the plain text, the third of the tenth, and the first of the second. If we find $a = 8$, then these three letters are all equal to the twentieth letter of the alphabet, that is **U**. (In fact, this could also be **V**, since at that time it was common not to distinguish between the two letters; see Figure 3.)

Buck gets frustrated with his failed attempt at solution: “after I [...] had used much time and paper, the first evening went by quickly and I saw on my scratchpad nothing but a miserably large heap of x ’s and y ’s thrown together, or rather a long and wide algebraical cipher.”³ The student Meltzbach then tells Buck that he copied the arithmetical problem from the book *Arithmetica Mercatorum* by Johann Michael Schwarzer, published in 1762.

The frontispiece and title of Schwarzer’s work are shown in Figures 3 and 5, and it also contains the standard conversion from letters to numbers, as shown in Figure 3. This encourages Buck to give it another try, but he fails miserably again: “I covered many and large sheets of paper with extensive and

²Vor wenigen Wochen überreichte mir ein fleißiger und ordentlicher Zuhörer, der jüngere Herr Studiosus Meltzbach einen kleinen Zettul, und ersuchte mich zugleich, die auf demselben aufgezeichnete mathematische Aufgaben ohne Beschwerde aufzulösen. Da ein Lehrer allemahl verbunden ist, dem edlen Bitten seines Zuhörers alles Gehör zu geben, um hiedurch sowohl seiner gerechten Wißbegierde ein Genüge zu leisten, als auch ihn selbst zu ähnlichen künftigen auszuführenden Bemühungen aufzumuntern; so nahm ich schuldigst diese Schrift an, durchlas sie in seiner Gegenwart mit einiger Eilfertigkeit, und that das Versprechen hinzu, an dem folgenden Tag die Auflösungen derer vorgelegten Aufgaben ihm zu überliefern.

³... nachdem ich ... viele Zeit und viel Papier angewendet hatte, so floß der erste Abend schnell vorbey, und ich erblickete auf meinen Zettuln nichts weiter als eine erbärmlich große Menge von zusammengeschriebenen x . und y , oder vielmehr ein langes und breites algebraisches Nichts.

rather horrible calculations ... and still I produced in the end another unhappy miscarriage, I mean, a thick bundle of long and meaningless algebraical computations.”⁴ In his narrative, Buck is then ready to throw everything into the fire, but finally receives a miraculous inspiration, gets all his math right, and finds the solution: **Vatter, vergib ihnen, sie wissen nicht, was sie thun.** (Father, forgive them, they know not what they do.)⁵ In Section 3, an example explains the two-step process: first solving puzzles to find numbers, and secondly turning these into letters at specified positions.

Buck goes on to pose a similar task of his own, gives in great detail the numerical calculations, and charms the reader with the decrypt: **Scopus vitae Christus** (The goal of life is Christ), the motto of the Roman Emperor Jovianus Flavius I, a Christian who ruled from 22 June 363 to 17 February 364.

His last words are: “there is no doubt that, following these instructions, secret messages can be both written and deciphered in any human language. This can present substantial benefit in peace and, particularly, in war at many occasions. May God give in mercy that this little tract may contribute even a little to the recognition of truth, and to the discovery of several errors which may sometimes be hidden in numbers!”⁶

And Buck stops here.

3. Solving the puzzles

I suffered almost the same fate as Buck, spending an hour or two filling reams of paper (plus a Maple worksheet). We now trace the solution process for Buck’s (and Schwarzer’s) first puzzle, shown in Figure 2. We have already translated it into the four equations (1) for four unknown integers a , d , b , and q . Later the solutions are converted to letters; for example $a + 12$ is the first letter

⁴Ich beschrieb viele und große Papiere mit weitläufigen und recht fürchterlichen Rechnungen. ... so brachte ich dennoch zuletzt wiederum eine unglückliche Geburth, ich meyne, ein dickes Packet von langen und nichts bedeutenden algebraischen Rechnungen herfür.

⁵This is in Luke 23:34 but not in every Christian’s book.

⁶so ist es unstreitig, daß nach dieser Lehrart geheime Sachen in allen menschlichen Sprachen theils geschrieben, theils dechifferiret werden können; welches gewiß sowohl im Frieden als auch vornehmlich im Kriege bey allerley Vorfällen seinen beträchtlichsten Nutzen haben kann. Gott gebe dahero aus Gnaden, daß diese kleine Abhandlung auch nur etwas zur Erkenntniß der Wahrheit, und zur Entdeckung mancher Irrthümer, die auch in Zahlen oftersmahl verstecket sich befinden, beytragen möge!

of the first and second words, and the third of the tenth word. This implies that $a + 12$ lies between 1 and 24. There are similar constraints on the other variables. Now 131 is a prime number, and so two of the three factors $a + d$, b , and q in the third equation in (1) equal 1, and the third one is 131. One verifies immediately that none of the resulting three possibilities gives an acceptable solution. No wonder Buck got frustrated: working on unsolvable puzzles is a thankless job. What now? Throw everything into the fire (respectively the trash folder)? My job was easier than Buck's, in that I already had his solution at hand. And indeed, replacing 131 by 132, one finds the two solutions $(4, 12, 6, 2)$ and $(8, 3, 3, 4)$ for (a, d, b, q) . The second of these solutions gives the letters

$$\begin{aligned} a + 12 = 20 = \mathbf{v}, & & a + d - 2 = 9 = \mathbf{i}, \\ (a + 2d)/7 = 2 = \mathbf{b}, & & b/3 = 1 = \mathbf{a}, \\ bq + 7 = 19 = \mathbf{t}, & & bq^2/6 = 8 = \mathbf{h}. \end{aligned}$$

Following the instructions in Figure 2, we then have the following partial decrypt, with 16 correct letters:

vatt.. v.. .ib i.... .i. .i... .i.. .a .i thu.

The lengths of the words are not known at this point, but I have simply used the lengths as they are known at the end of the decryption.

The other four puzzles can be solved in the same way and give **h**, **n**, **r**, and **s**, plus a guess for **e** and (another one) for **r**. This yields the plain text

(2) vatter ver ?i^b_e ihnen sie ?isen nⁱ_es sa ?i thun.

The ? places are not specified, and **b/e** and **i/i** are doubly specified. This solution is valid if we also change an original puzzle value of 289 to 189 and an 1806 to 1808. The latter value occurs in the fourth puzzle, where the pentagonal number 35 with pentagonal root 5 and the 49-gonal number 1773 with 49-gonal root 9 add up to 1808. The solution is acceptably close to what Buck reveals. Most of my time was spent on finding a consistent system of conditions with

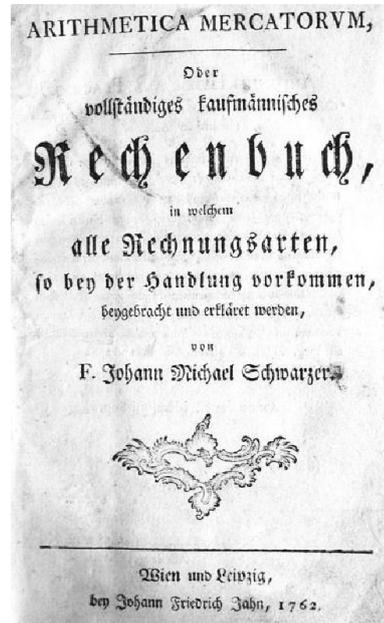


Figure 4: Title page of Schwarzer's *Arithmetic*

minimal edit distance to Buck's (inconsistent) conditions, and I needed help from Donald E. Knuth to solve the fourth puzzle. The second set of puzzles, invented by Buck himself, only took me 15 minutes by hand. It produces his solution, except that he had incorrectly coded his two i's as e.

4. Buck's life and sources

Buck (1722–1786) was born in Königsberg, registered as a student on 4 June 1737 at the local university (Erlor (1911), page 371), and received his Master's degree at the Faculty of Philosophy on 18 July 1743 (Komorowski (1988), page 80) and his doctoral degree in law from the University of Frankfurt an der Oder



Figure 5: Frontispiece of Schwarzer's Arithmetic.

in 1748 (Koch (1987)). Buck became an associate professor (außerordentlicher Professor) of mathematics at the University of Königsberg in East Prussia in 1753, a full professor (ordentlicher Professor) of logic and metaphysics in 1759, and of mathematics in 1770. He published about thirty works, some of them on mathematical subjects such as “diagonal and polygonal numbers” and “the usefulness of mathematics on travels”, but also on topics such as “teleological considerations about smoke” and “the happiness of those who die young” (Poggendorf (1863), Koch (1987)).

Albrecht (1522-1557), margrave of Brandenburg, established the *Albertina* University at Königsberg in 1544. According to the lists of course announcements (Oberhausen & Pozzo (1999)), Buck taught a variety of subjects from the summer of 1753 to 1786, the year of his death at 64 years of age. In fact, he had started teaching already before 1753; junior faculty were not listed in these announcements, and the one from 1753 talks about his courses taking place “at the usual times and days”. Buck’s courses were mainly in mathematics and philosophy—Immanuel Kant was his colleague on the faculty from 1755 on. Both Buck and Kant applied in 1759 for a vacant professor position in logic and metaphysics. According to the University senate’s vote, Buck obtained the position. Kant was not pleased. The formal appointment was made by Nicolaus Freiherr von Korff, the Tsar’s governor of Prussia. Russian troops occupied Königsberg and other parts of Prussia from 1758 to 1762, during the seven-year war. [They then left, until 1945.] It took eleven years until a mathematics professor’s death on 15 March 1770 opened up a position. Not wasting any time, Kant wrote on 16 March to Berlin proposing a swap. The positive reply dated 31 March 1770 gave as the first reason that Kant had lectured as well as the “diligent and successful” mathematics professor Buck; Kant’s books were given second place. Thus he obtained the full professorship in logic and metaphysics, and Buck was moved into the corresponding appointment in mathematics (Krollmann (1941)), without even having been consulted by Kant about his proposal. Buck was not pleased (Kuehn (2001)).

Buck and Kant signed, with four others, on 1 October 1781 a petition to Frederick the Great, King of Prussia, asking to reduce the use of Latin to tutorials, and to liberate the lectures of this requirement which severely limited the number of students capable of following the courses. The petition was adamantly refused, and Latin teaching at the high school level reinforced. [When this author offers to teach a course in English, an overwhelming majority of the students vote for German.]

Buck also lectured on theoretical and experimental physics, geography, politics, artillery, civil and military architecture—an academic breadth quite

unimaginable today. His timetable for the summer term of 1772 is typical: on Monday, Tuesday, Thursday, Friday he taught geometry and trigonometry from 8 to 9, arithmetic and geometry 10–11, logic 2–3, algebra 3–4. On Wednesday and Saturday it was civil architecture 8–9, geography, chronology and gnomonics 9–10, experimental physics 11–12, practical philosophy 2–3, plus a colloquium (3–4 in other terms). This comes to a total of about 26 hours per week. The year was divided into two semesters, with short breaks of one to four weeks between them. Not all announced courses may have been held, but Buck was a successful lecturer. As an example, in the winter term 1775/76 Buck had 28 students in his class on metaphysics (and Kant had 30 in his version of the course; they both offered metaphysics courses repeatedly in parallel), 53 in experimental physics, 49 in arithmetic and geometry, 30 in military and civil architecture, 20 in a seminar, and 25 in trigonometry and astronomy. All but the last course were taught “privatim”, where students had to pay a tuition fee directly to Buck. He was Dean of Philosophy repeatedly, and Rector of the University in 1784.

Buck centers his narrative around the interaction with his pushy student Meltzbach, who brings him Schwarzer’s puzzles, reveals their source only later, and provides Buck with the motivation to attack Schwarzer’s puzzles and write the report under consideration. Indeed, Bernhard Meltzbach from Königsberg was inscribed on 21 April 1769 at the University of Königsberg as a law student. Johann Christoph Meltzbach, also from Königsberg, had been registered on 8 May 1764 (Erler (1911), pages 512 and 492). We may assume that Bernhard is the “younger” student who bugged Buck, and Johann Christoph—possibly an older brother or cousin—had left the university by then. 122 freshmen began their studies in the summer term of 1770, and the typical duration of studies at that time was between two and three years.

Much of Buck’s material is taken from Schwarzer’s book. This is an 840-page encyclopedia of commercial arithmetic whose title (Figure 4) translates as:

The Merchants’ Arithmetic, or a complete commercial computing book, in which all manners of calculation that arise in commerce are being taught and explained, by Brother Johann Michael Schwarzer.

After discussing the arithmetic operations and linear equations in one variable (“regula tribus” or “regula detri”), the body of the work is dedicated to conversion calculations between the various measures and currencies in different cities and countries. His list of currencies alone comprises 32 pages. What an effort those old Europeans had to spend on their conversions!

On the last three pages, Schwarzer gives the puzzles later reprinted by Buck and the letter-to-number conversion, but not a solution to his cryptogram. Buck found the correct decryption of Schwarzer's puzzles. Thus he must have realized the typographic errors in their statements, such as the 131 for the correct 132. Why did he not correct those errors?

Schwarzer was responsible for economic affairs (Wirtschaftsverwalter) at the Löwenburg convent in Vienna. The Chamber of Commerce (Handlungsgesellschaft) of Vienna published his book, which is dedicated to its leading members.

The 20 pages of the *Elementa artis decifratioe* (Elements of the art of deciphering) that Buck mentions were published anonymously in 1770 at Königsberg in Eastern Prussia. On page 3, we find "L.B." as signature, and "L.E.B." on the last page. Buck's work is presumably the first to make the author's name "Lindner" public. The "B" and "E.B." are unlikely to indicate first names, since these were written before the last name, also at that time. In Klüber (1809), we find "Sam. Lindner", and the bibliographies of Galland (1945) and Shulman (1976) give "Samuel Lindner". There is no Samuel Lindner in the standard biographies of Poggendorf (1863) and Koch (1987). Buck's wording "our professor Lindner" seems to indicate a colleague at his university. Indeed, Johann Gotthelf Lindner (1729–1776) taught literature, theology and French at Königsberg, and Theodor Gottlieb von Hippel (1741–1796), a student of Buck's, held the funeral speech at his grave (Lenning (1822), volume 2, pages 59–62 and 305). But the first names do not match each other or the initials, and the author's identity remains somewhat of a mystery.

The book starts with a long-winded introduction and notational discussion, a bibliography of 24 items, and a history of cryptography. Then Lindner discusses the cryptanalysis of a simple substitution (with word divisions). He briefly mentions frequency analysis, but then focusses on grammatical and structural properties: q followed by u , single-letter words, doubled letters. He then gives particular rules for German, Latin, and French, including frequent bigrams and trigrams. The book ends with a sample decipherment by Wallis, and a cryptographic challenge.

5. Puzzles and keyless cryptography

Little arithmetical puzzles had been en vogue for over a hundred years. Charming collections like those of Bachet de Méziriac (1612), Schwenter (1636), and Ozanam (1741) contain hundreds of such brain teasers. Easy?

Buck's basic mistake is his hidden assumption that an attacker of the system

will be substantially less clever than sender and receiver, namely unable to solve those little puzzles. Generally speaking, cryptographers would have an easier life if they could always assume their attackers to be computationally challenged.

It was a major step forward by Comiers (1690) to realize that the famous Vigenère tableau is nothing but the group table for modular addition (although not in these words; see von zur Gathen (2003)). Buck’s work does not contain any such advance.

There are other examples in history of such keyless cryptography, where encryption and decryption can be performed by a person in the know, but not by a “layman”. Presumably writing itself had this character at its beginning. Egyptian cryptography substituted invented symbols for regular letters. The inventions follow a simple pattern: the pronunciation (usually the first letter) of the new symbol (which is not a standard hieroglyph) is used, like writing  for h in English. Examples exist mainly from the 18th dynasty (see Drioton (1933–1934)).

In medieval manuscripts, the vowels were sometimes replaced by dots:

a	e	i	o	u
·	:	.:	::	:::

In many countries, hobos and gypsies have a system of symbols they draw on house walls to indicate the possibilities. These were taught by relatives and friends, and there are even dictionaries compiled by experts, such as Günther (1919)—but if you find one on your wall, you probably will not be able to understand it. (Hint: erase it unless it is $\vee\vee =$ dangerous dog.)

Thus in keyless cryptography, we have a group of people with the knowledge required to encrypt and decrypt messages, while outsiders cannot do this. We might also include juvenile “Pig Latin” in this category.

Early encrypted signatures also used keyless cryptography. Huyghens published a 63-letter anagram of his discovery of Saturn’s ring, basically just the number of times each letter occurs in his text: aaaaaaa ccccc d eeeee g h iiiiii llll mm nnnnnnnn oooo pp q rr s ttttt uuuuu. In today’s language, he assumed this to be a sufficiently secure hash function. It was solved by Wallis almost at once: **annulo cingitur tenui plano, nusquam cohaerente, ad eclipticam inclinato**⁷; see Librarian (1924) and Kahn (1967), page 773. Sir Christopher Wren (1632–1723) invented three astronomical instruments in 1714 but did not want to divulge their secrets. So he composed a text

⁷It is girdled by a thin flat ring, nowhere touching, inclined to the ecliptic.

describing them and published only an encryption of it; see Brewster (1855), page 263 and Kahn (1967), page 773.

The German algebraist and computer Johannes Faulhaber (1580-1635) ended a 1604 work with an arithmetic puzzle whose solution is a name (and would indicate mastery of the material by the solver). In a 1631 book, he published closed formulas for sums like

$$\sum_{1 \leq k < n} k^i$$

for some values of i up to 17. He then proves that he actually knew how to go up to 25 by writing down those formulas for the sums for $22 \leq i \leq 25$ not explicitly, but rather with indeterminate coefficients, and calculating five values x_1, \dots, x_5 from those coefficients. With the standard conversion, as also used by Schwarzer and Buck, a correct calculation of those formulas is supposed to yield the reply **iesus** to his challenge of a “highly praised name”⁸ and thus to establish Faulhaber’s priority.

Alas, his calculation gives only x_2 exactly, x_5 is totally obscure (and hence only a guess), and the other values can be obtained by a minor (but not obvious) modification of his instructions. Knuth (1993) has written a wonderful account of Faulhaber’s achievements; a true Renaissance man. Schneider (1993) gives a detailed biography of Faulhaber, an analysis of his work, and explains polygonal numbers. (For the latter, see also Beiler (1964), Chapter 18.)

These methods have one thing in common with Buck’s: once you know the system and are clever enough, you can read any message. But Kerckhoffs’ wise Second Principle says: “[The system] must not require secrecy, and must be able to fall into the enemy’s hands without disadvantage.”⁹ So all of these had their place, time, and clever users, but do not obey this principle.

6. Conclusion

Buck proposes to encode secret messages by arithmetic puzzles, using the natural correspondence between letters and numbers. The recipient has to solve those puzzles, and a legitimate correspondent has no advantage (such as a secret key) over an unwanted interceptor. The proposal is more of a mathematical parlor game than a serious method for secret communication.

We may view Buck as a late representative of baroque culture, and note the rise during his later years of one of the stars of crystal-clear thinking and

⁸hochgerühmte Nam

⁹Il faut qu’il n’exige pas le secret, et qu’il puisse sans inconvénient tomber entre les mains de l’ennemi.

Enlightenment, Immanuel Kant.

However, we may apply Luke 23:34 to Buck's writing.

Acknowledgement

The author thanks David Kahn for his kind invitation to write about Buck, and for his numerous suggestions which improved the presentation. Don Knuth pointed me to the solution of the fourth puzzle. The library of the Martin-Luther-Universität at Halle-Wittenberg has kindly furnished a microfilm with Buck's work, and given permission to make this available on our web site. Thanks go to Leander Pflüger for a pointer to the literature.

References

CLAUDE GASPAR BACHET DE MÉZIRIAC (1612). *Problèmes plaisans et délectables, qui se font par les nombres*. Pierre Rigaud, Lyon.

ALBERT H. BEILER (1964). *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains*. Dover Publications, Inc., New York.

DAVID BREWSTER (1855). *Memoirs of the Life, Writings, and Discoveries of Sir Isaac Newton*, volume 14 of *The Sources of Science*. Edinburgh, 478 pages. Reprint edited by Harry Wolf, Johnson Reprint Corporation, New York und London, 1965.

CLAUDE COMIERS (1690). *L'Art d'Écrire et de Parler Occultement et sans Soupçon*. Michel Guerout, Paris, 72.

ETIENNE DRIOTON (1933–1934). La cryptographie égyptienne. *Revue Lorraine d'Anthropologie, Nancy* **6^e Année**, 5–28.

GEORG ERLER (editor) (1911). *Die Matrikel der Albertus-Universität zu Königsberg i. Pr.. Die Immatrikulation von 1657-1829*, volume 2. Verlag von Duncker & Humblot, Leipzig, 772 pages. Reprint herausgegeben von Kraus Reprint, Nendeln/Liechtenstein.

JOHANNES FAULHABER (1604). *Arithmetischer Cubicossischer Lustgarten. Darinnen Hundert und Sechtzig Blümlein/ das ist/ außerlesner schöner künstlicher Exempel mit Newen Inventionibus gepflantzet werden. Welche theils auß Hieronymo Cardano/ vnnnd andern Lateinischen Scribenten versetzt vnnnd gezogen: Theils aber insonderheit die liebliche Polygonalische Röslein/ von newen zum Lust erzogen worden*. Erhard Cellius, Tübingen, 43 leaves.

JOHANNES FAULHABER (1631). *Academia Algebrae. Darinnen die miraculossische Inventiones/ zu den höchsten Cossen weiters continuirt und profitiert werden.* Johann Ulrich Schönigk, Augsburg, 22 leaves.

JOSEPH S. GALLAND (1945). *An historical and analytical Bibliography of the literature of Cryptology.* Northwestern University, Evanston. ISBN 1-57898-092-5, 209 pages. Reprinted ca. 1996 by Martino Fine Books, Mansfield Centre CT.

JOACHIM VON ZUR GATHEN (2003). Claude Comiers: the first arithmetical cryptography. *Cryptologia* **XXVII**(4), 339–349.

L. GÜNTHER (1919). *Die deutsche Gaunersprache und verwandte Geheim- und Berufssprachen.* Reprinted in 2000 by Reprint-Verlag-Leipzig, Holzminden.

DAVID KAHN (1967). *The Codebreakers.* The Macmillan Company, New York. xvi + 1164 pages.

AUGUSTE KERCKHOFFS (1883). La Cryptographie Militaire. *Journal des Sciences Militaires* **9**, 161–191. URL http://www.cl.cam.ac.uk/users/fapp2/kerckhoffs/la_cryptographie_militaire_ii.htm.

D. JOH. LUDW. KLÜBER (1809). *Kryptographik. Lehrbuch der Geheimschreibekunst (Chiffrir- und Dechiffirkunst) in Staats- und Privatgeschäften.* J. G. Cotta'sche Buchhandlung, Tübingen, xvi + 30 pp. + 10 tables + 472 pp.

DONALD E. KNUTH (1993). Johann Faulhaber and sums of powers. *Mathematics of Computation* **61**(203), 277–294.

HANS-ALBRECHT KOCH (1987). Buck. In *Deutsches biographisches Archiv*, volume 1. Saur, München. ISBN 3-598-30410-2.

MANFRED KOMOROWSKI (1988). *Promotionen an der Universität Königsberg 1548-1799.* K. G. Saur, München. ISBN 3-598-10760-9, 98 pages.

CHRISTIAN KROLLMANN (editor) (1941). *Altpreußische Biographie*, volume 1, 416 pages. Reprint 1974 by N. G. Elwert Verlag, Marburg/Lahn. ISBN 3-7708-0502-X.

MANFRED KUEHN (2001). *Kant. A Biography.* Cambridge University Press. German translation by Martin Pfeiffer, published 2003 by C.H. Beck Verlag, 639 pages.

C. LENNING (1822). *Encyclopädie der Freimaurerei.* F. A. Brockhaus, Leipzig.

LIBRARIAN (1924). Round the Library Table. *The Saturday Review* **126**(3573), 418.

SAMUEL LINDNER (1770). *Elementa artis deciftratoriae.* Litteris Hartvngianis, Regiomonti, 20 pp.

MICHAEL OBERHAUSEN & RICCARDO POZZO (editors) (1999). *Vorlesungsverzeichnisse der Universität Königsberg (1720–1804)*. Frommann-Holzboog, Stuttgart.

JACQUES OZANAM (1741). *Recreation Mathematiques et Physiques, qui contiennent plusieurs problemes d'Arithmetique, de Geometrie, de Musique, d'Optique, de Gnomonique, de Cosmographie, de Mecanique, de Pyrothechnie, & de Physique. Avec un Traité des Horloges Elementaires*. Charles-Antoine Jombert, Paris, three volumes.

JOHANN C. POGGENDORF (1863). Buck, Friedrich Johann. In *Biographisch-Literarisches Handwörterbuch zur Geschichte der exacten Wissenschaften*, volume 1, 331. Reprint 1970 by B. M. Israël, Amsterdam.

IVO SCHNEIDER (1993). *Johannes Faulhaber 1580-1635. Rechenmeister in einer Welt des Umbruchs*, volume 7 of *Vita Mathematica*. Birkhäuser, xiv, 271 pages.

JOHANN MICHAEL SCHWARZER (1762). *Arithmetica Mercatorum, Oder vollständiges kaufmännisches Rechenbuch, in welchem alle Rechnungsarten, so bey der Handlung vorkommen, beygebracht und erkläret werden*. Johann Friedrich Jahn, Wien und Leipzig.

DANIEL SCHWENTER (1636). *Deliciae Physico-Mathematicae*. Jeremias Dümmler, Nürnberg. Reprint by Keip Verlag, Frankfurt am Main, 1991.

DAVID SHULMAN (1976). *An Annotated Bibliography of Cryptography*. Garland Publishing, New York, London, xvi + 154 + 154 + 14 + 47 + 2 + pp.

JOACHIM VON ZUR GATHEN
Fakultät für Elektrotechnik, Informatik
und Mathematik
Universität Paderborn
D-33095 Paderborn, Germany
gathen@uni-paderborn.de