# Solving the Dorabella Cipher

**Tim S Roberts**

**CQUniversity**

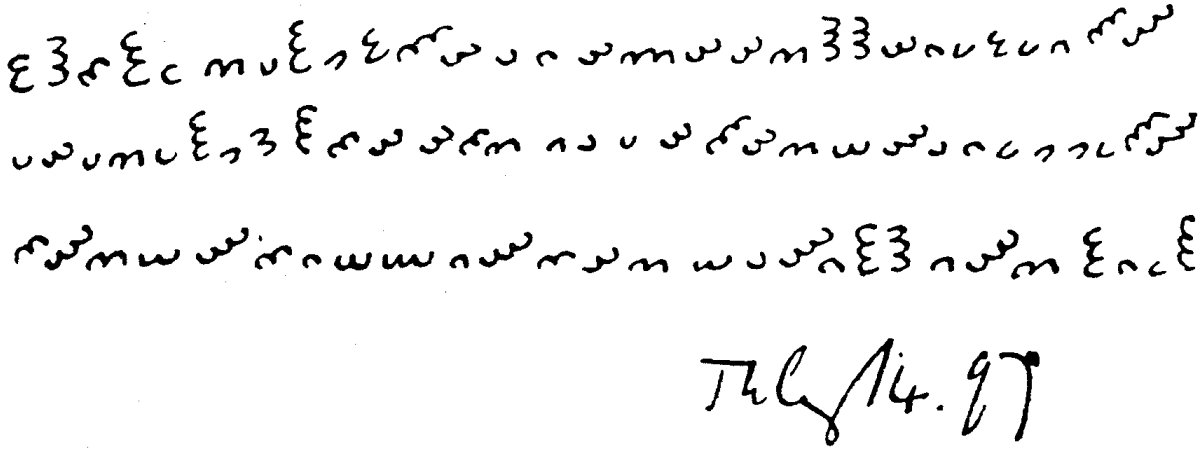
**Bundaberg, Queensland 4670, Australia**

t.roberts@cqu.edu.au

We are all accustomed to thinking of classical composers as elderly men. If you Google the image of Johann Sebastian Bach, for example, you will most likely find a portrait by Haussman painted in 1748, when Bach was aged 63; or Richard Wagner, and you will most likely find an image of him in 1871, aged 58; or Johannes Brahms, and you will find him in his sixties. Beethoven you will probably find aged 49. Almost universally, what we see are men in their senior years. The only exceptions to this seem to be those who died young; Frederic Chopin, for example, whose only known photograph was taken in the year of his death, 1849, aged 39; or Wolfgang Amadeus Mozart, aged 24, who died aged 35. The majority were old. But of course it was not always thus; all old men were young once.

And so it is with Edward Elgar. Though most of our mental images of Elgar are of a man in his fifties or sixties, at the beginning of 1897 he was still in his thirties, and had not yet written the works for which he was to become famous, such as the *Enigma Variations*, in 1899; *The Dream of Gerontius*, in 1900; the *Pomp and Circumstance Marches*, 1901 and onwards; *The Kingdom*, in 1906; and so on. And for all of which, in 1928, he would receive a knighthood. He had already established a solid reputation, however, based largely on *Froissart*, composed in 1890, and the *King Olaf* cantatas, composed the previous year, in 1896.

And so it was that in 1897, while he was working on *Caractacus*, he made the acquaintance of a young lady, named Dora Penny, the 22-year-old daughter of the Reverend Alfred Penny, rector of St.Peter's, in Wolverhampton. Elgar was married at the time, to one of his students, Caroline Alice Roberts, a marriage which was to last until her death in 1920, aged 72. Elgar's relationship with Dora was almost certainly platonic, but there is little doubt that he enjoyed her company; so much so, in fact, that variation 10 of his *Enigma Variations* is dedicated to her. And so it was that, in the middle of July 1897, just after he had celebrated his fortieth birthday, he sent her a short note. Not one written in English, however, but an apparent cipher, consisting of 87 characters, each in the form of one, two, or three semicircles, in one of eight orientations.



The note has withstood all attempts at decryption, and has become known as the *Dorabella Cipher*.

The cipher was featured in *The Musical Times* in 1970, in an article written by Eric Sams, together with a purported solution that has never found much favour. In 2007 and 2008, the Elgar Society offered a prize of £1500 for its successful decryption, but no entry proved to be deemed sufficiently worthy of being called a winner, and the prize was not awarded. The cipher therefore remained unsolved.

**Speculation**

Why would Elgar, a man who, in June 1897, had just turned 40, send such a note to a young lady, whom he had met on only a few occasions, and who apparently had no interest in puzzles or ciphers? Speculation abounds. Could it contain a clue to one his musical compositions? Could it be a quotation from Shelley or Shakespeare? Could it perhaps be an invitation to a sexual liaison?

It is also not clear that there is indeed a coded message contained within. Perhaps it is just a piece of paper on which Elgar had written various symbols, almost at random. But what would have been Elgar's purpose in so doing? To contend that it is just a meaningless stream of symbols would seem extremely unlikely, to say the least.

So if we assume that the text is indeed intended to convey some meaningful text, the next question is: what method could Elgar have used?

**Simple Substitution**

A simple substitution cipher seems by far the most likely. Remember, this was way before the age of computers; the word "byte", meaning eight binary digits, was half-a-century away. All cryptographic techniques were therefore necessarily based on pencil-and-paper. Since Dora was a novice code-breaker at best, why go beyond simple substitution – one symbol, one letter?

One problem is immediately apparent. With one, two, or three semi-circles in one of eight orientations, there are only 3 * 8 = 24 possible symbols. And yet there are 26 letters in the English alphabet. However, this is no real problem, and there seem to be at least three possible solutions: first, ignore Q and Z, the two most infrequently-used letters in the English alphabet; second, use the same symbol for X, Y, and Z, the three letters at the end of the alphabet; third, use a scheme common in Elgar's time, which was to use the same symbol for I and J, and for U and V. These are amongst the most likely – other possibilities also exist.

The main problem with this idea is that, if the cipher was a simple substitution based on the above principles, it would surely have been solved by now. Actually, not so surely, since with 24! (that is, 24*23*22*….*3*2*1) possible arrangements of symbols to letters, it is not possible to actually examine every possibility, even with computers able to examine billions of possibilities per second.

If you calculate this number, 24!, it turns out to be 620,448,401,733,239,439,360,000. Suppose with really clever programming we can use our computer to examine one billion (1,000,000,000) possibilities per second. Then it would take our program some 20 million years to examine all possibilities!

So, perhaps it is not surprising that it has not been solved. And yet, not so: with reasonable assumptions – that 'A' is more frequent than 'J' , for example, and 'E' is more frequent than 'K' – the number of possibilities can be reduced dramatically.

**Initial Efforts**

My own initial efforts included comparing the Dorabella cipher with passages from the Bible, Shakespeare, and many other authors who may have been known to Elgar, in the hope that Elgar's message was a simple quotation from some well-known source, transcribed using the symbols previously described. Such efforts produced no significant outcome.

Simple substitutions, but with the cipher based on another language, were investigated: French, Italian, German, and Latin were examined, without success.

Then followed an examination of possible transpositions, based on all key-lengths from 2 to 30, and reading the resultant rectangles in 16 different ways (starting from any of the 4 corners of the rectangle, going in any of 2 directions, and either proceeding in the same way, or reversing direction).

No significant results were found from the 29*16 = 462 transcriptions produced. This is perhaps not surprising, since there appear to be no examples of Elgar using transposition in any other puzzles or ciphers.

**The Path to the Solution**

With literally hundreds of billions of unsuccessful efforts behind me (or rather, my computer, working tirelessly), I decided to re-examine some of the basic assumptions.

Should the passage contain text of worldwide significance? Of course not. This was, after all, a note from a semi-successful composer to a young lady acquaintance, whom he had met on only a few previous occasions.

Should the passage be free of errors? Of course not. It was probably written in a hurry, perhaps as an afterthought. Elgar would certainly have been bemused to think that the note had survived for over a century, and that many potential decrypters had spent thousands of hours trying to make some sense of his little note.

Should the passage be in English? Presumably so. Why not? It would seem to be fanciful in the extreme that an English speaker should communicate to another English speaker in French or Italian.

Should the passage be encrypted using some advanced method? Presumably not. What would be the point? Dora was not known as a code-breaker, even of the simplest of codes.

So, that leaves a simple substitution cipher, written in English, with a content of perhaps minor significance, and probably containing some errors.

But this had all been tried before. What other assumptions, common to all would-be code-breakers, had been made? Well, the most obvious one was that there was a one-to-one correspondence between cipher characters and the letters of the alphabet.

Suppose instead that two different symbols could both represent the same letter. If this should seem strange, this was exactly the key idea that was required to decode the Mayan hieroglyphics, which had defied all attempts at decryption for centuries.

**The Solution**

The solution turns out to be based on a simple substitution cipher, though without a one-to-one correspondence. It relies for its coherence on a previous conversation (or letter) between Elgar and Dora in which he had described his effort at gardening – in particular, his pruning back (far too heavily, as it turned out) – of a particular garden bed, perhaps containing beautiful roses. Then:

**PSNOWDROCPBEIGEWEEDSSETINITBU**
**REIDIOCYONEENDTIREBEDLUIGICCIBU**
**NUDLVNGLYTUNEDLIUTOSTUDOTWO**

or, with spaces and punctuation included:

**P.S. Now droop beige weeds set in it – pure idiocy – one entire bed! Luigi Ccibunud lovingly tuned liuto studio two.**

This is based on a simple substitution, except that four letters – I, N, W and Y – have been encoded using two different symbols. In addition, the letter 'A' does not appear at all, which is a remarkable occurrence on its own in a passage of some 87 characters. As for the decrypted message itself:

**P.S.:** exact substitution - the cipher was contained with another letter, so this seems a natural start.

**now drocp**: a ‘c’ has been coded instead of an ‘o’, remainder is exact

**beige weeds set in it**: exact substitution

**bure idiocy**: a ‘b’ has been coded instead of a ‘p’, remainder is exact

**one endtire bed!**: exact substitution. An extra ‘d’ is included in ‘entire’.

**Luigi Ccibunud**: a seemingly meaningless string, but Luigi happens to be the first name of one of Elgar’s favourite composers, whose surname just happens to be Cherubini.

**luv’ngly**: exact substitution. A single character represents both U and V, and the mysterious dot in the ciphertext turns out to be a simple apostrophe.

**tuned liuto**: exact substitution – “liuto” is the Italian word for “lute”. Note that “Luigi”, the name earlier on, is also Italian. Elgar wrote his “Lute Song” using words written by Alice in 1897.

**studo two**: exact substitution. The word “studio” is the Italian equivalent of etude, meaning a musical composition.

**But What About…?**

It should be noted that the solution above accounts for all of the symbols, all words follow one another logically and make sense, and all words are common to Elgar’s day. As such, the probability of it being incorrect in any major way is extremely small. Nevertheless, there are four identifiable problems:

(1) Why did Elgar not use a one-to-one correspondence? Would this not have been more natural?

(2) If a one-to-one correspondence was not to be used, why double up on some relatively obscure letters – I, N, W and Y – rather than, say, A, E, S and T, which are far more common in English usage?

(3) Why leave the ‘I’ out of *studio*, and add a ‘d’ to *endtire*?

(4) Why include that string of characters LUIGI CCIBUNUD in the middle of what otherwise makes perfect sense?

**The Discovery of the Key**

And then, all became clear, on a chance observation that the name PENNY was entirely coded within the set of eight symbols all with two semi-circles. And the word WRITING appeared to be entirely (well, almost) coded within the set of eight symbols with one semi-circle. In fact, we have

**L A D P E N N Y**

**W R I T I G I C**

**O S U H B Y W K**

Elgar used the key

***Lady Penny, writing in code is such busy work!***

Omitting spaces and using upper case, this is

**LADYPENNYWRITINGINCODEISSUCHBUSYWORK**

But there are only 24 symbols. The first group of 8, corresponding to the symbols with two semi-circles, is beautiful:

**LADPENNY**

which plays on the sound of the D. There are two N's already, so delete the remaining two Ns, and then delete every letter that's repeated, starting at the end and working back (this is the absolutely natural way to do it, if you think about it), until you get 24 characters:

**LADPENNY WRITIGIC OSUHBYWK**

which is exactly what we have.

**Elgar's Wordplay**

Not only does the discovery of the key explain both (1) and (2), but in fact it also provides the vital clues to both (3) and (4). The first word of the key is LADY, but Elgar leaves out the Y, playing on the sound of the letter D (LAY-DEE). Dora's name would have been very amusing to Elgar, since of course a "penny" was indeed represented by the letter "d". And so it can be seen that he also does this – always with the letter D, and no other – in three places in the cipher. First, in ENDTIRE (the letter D is silent), second, in LUIGICCIBUNUD (pronouncing the last part as BU-NU-DEE), and third in STUDO (STU-DEE-O). Presumably because D stands for Dora, and this was his first little word play.

The second word play explains LUIGICCIBUNUD. Now, LUIGI is a famous Italian name, of course. If one looks for any LUIGI in the index of Jerrold Northrop Moore's excellent biography of Elgar [1], one finds only one LUIGI – a composer Elgar had been very familiar with throughout his earlier years. His name was Luigi Cherubini. Exactly the same hard consonants, C, then B, then N. The odds against this being a chance occurrence are vast. And what was Dora famous for above all else? Her stutter. So it seems likely that she stumbled over the name – *"Chi- chi-bunudi"?* And Elgar was teasing her a little…

**Final Words**

And thus the message turns out to be a simple substitution cipher after all, written in English. Not containing anything profoundly important, alas, but just an innocent note that a man recently turned 40 – one interested in gardening and music - might send to a young lady companion; one encoded in such a way, however, that it proved too hard for over a hundred years.

*Further correspondence is welcomed. The author would be pleased to hear from anyone interested in the cipher. He can be reached at t.roberts@cqu.edu.au.*

**References**

[1] Moore, J N, (1984), *Edward Elgar: A Creative Life*, Oxford University Press.