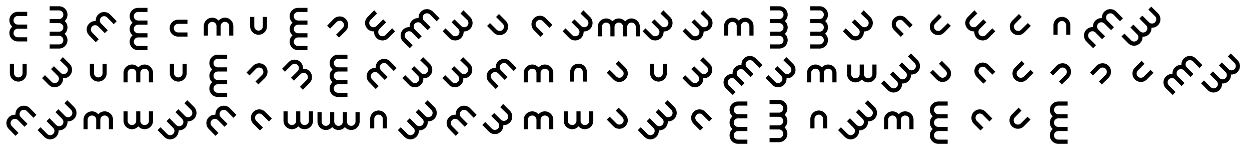
The Dorabella Cipher Solution

First, having solved it, I understand why it has been a problem. Elgar was a horrible puzzle author. I had a partial solution doing the normal cryptanalysis steps, but it was very frustrating. I have been developing a hill climbing program and I was using the Dorabella text as a short test. At about 4:00am EDT on May 7, 2019, the program gave me a solution but I didn't discover it until I looked through the files. Not bad since I only discovered this on April 23, 2019. As I am still working on some things, the final solution may change slightly from what is presented here. Admittedly, I'm not completely sure of a few things. Once you see the results, I'm sure you'll understand the problem.

Below is the ciphertext reconstructed using a font I put together.



So the first thing was to transcribe the symbols. I found two transcriptions from faked solutions and there may be more I didn't find. I even transcribed it twice myself and then went back a third and fourth time and changed a couple letters. The original ciphertext is that bad and I still don't completely trust my transcription.

```
AIBJQ CUJTD KEWXE NEECI IEXSD SVKLU EUCUJ THJBE EBCVW

UEKEC FLWXS TTSKL BLCFL BXFMV LBECF WLXJI VLCJX SJ
```

The frequency count gives an IC of 0.058540. There are only 24 letters possible in the cipher and a few more are unused. If you chart the numbers, it gives a reasonable profile of normal English.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	6	8	2	11	4	0	1	4	7	4	8	1	1	0	0	1	0	5	4	5	4	4	6	0	0

This is my most recent hand decryption using a simple program that allows quick letter substitutions. The program saves on erasers, but it does little else except display the ciphertext, plaintext and the current key along with the frequency count and the IC.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	s	t		e	h					r	i							o	l			n	c		

And this is the ciphertext that results from the partial key.

```
AIBJQ CUJTD KEWXE NEECI IEXSD SVKLU EUCUJ THJBE EBCVW
  s   t  l  rence  eet   eco  o ri  e t   l  se est n

UEKEC FLWXS TTSKL BLCFL BXFMV LBECF WLXJI VLCJX SJ
 eret hinco llori sithi sch   iseth nic    it c o
```

Please withhold any judgments at this point as the plaintext shown is actually correct. At this point, I did nothing except try letters according to frequency and knowledge of typical word construction. The shotgun hill climber really only helped me fill in the blanks. With all its warts and problems, there is nothing contrived or forced.

The hill climbing program came about because I finally decided to write one. The current program is written in C, probably worthy of being a beta version, and as near as I can tell it is without any major defects. The command line is used to program the hill climber and allows me to chose different limits, the key generator function, and which N-gram table it uses for scoring. Think of it as a Swiss army knife program because I plan on building modules for various cipher systems. I had just finished some changes to the save function when I ran the Dorabella test run. The alphabet is used as the default start key. I didn't try to help it at all.

Iteration 46 revealed something that looked like plaintext. The text generates quadgram scores in approximately the 7500 to 11500 range. The Dorabella solution had a score of 10375 and it filled in the blanks. Below is the the plaintext with some probable word divisions. It may take a committee to decide what this actually says. So now you know why no one solved it. It is a nightmare of abbreviations and odd spelling. From what I understand, this is Elgar speak.

```
AIB JQC UJTDKEWXE NEEC I IE XSD SVK LUE UCU JTHJBE
PBS AFT DALYRENCE MEET B BE COY OUR IDE DTD ALWASE

EBC VWUEK E CFLWX STT SK LB LC FLB XFM VLB ECFWLX
EST UNDER E THINC OLL OR IS IT HIS CHG UIS ETHNIC

JIVLC JXSJ
ABUIT ACOA
```

And the key:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
PSTYEHKWBARIGMXJFVOLDUNCZQ
```

At this point, my transcription appears to be accurate. There are a some problems though. Given the odd text, I can't be completely sure of anything. There is still a chance that some of the single letters could be wrong. The often combined letters of I/J or U/V may or may not be a factor here and there is only 24 ciphertext symbols

I will continue to pick a this. I still haven't tried very hard at finding a key word or words for mixing the alphabet. I still need to look at some of the original symbols and make sure there are no errors. Then I'll probably have to rewrite this or at least make some changes if I find anything. Eventually I'll put the files on my github account. The hill climber will also go there with the rest of the crypto programs when I get more done.

If you want to reach me, it's best if you forget I have an FB account. Try my gmail shadowwolf63 account or shadowwolf387 for both my github and tumblr accounts. I'm not on those accounts a lot, but I'm on them a whole lot more than FB.