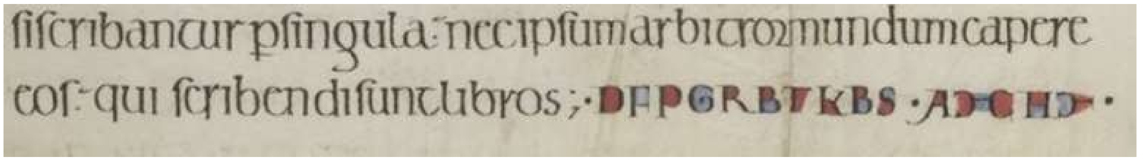
Vowel Replacement

When I start prattling on about period codes and ciphers, especially to someone that hasn't figured out that I'm just a huge dork for this stuff, I will almost always get the question "what is the earliest cipher?". Unfortunately, for some reason, a lot of people don't like the real answer (a couple thousand BCE) and I think that is because what they are really trying to ask is actually a two-part question. I think that the question they are trying to ask more along the lines of "what is the earliest known cipher, in period, that I would recognize as a cipher", or something like that. This is a perfectly reasonable question.

First we should answer the question as asked. The earliest known examples of encoded messages that we currently know of date to around 2000 BCE from Egypt, from the tomb of Khumhotep II (Kahn, 1996). In these examples, extent examples being found in tombs, we see various glyphs replaced with ones from other dialects or embellished in discrete ways, for those knowledgeable enough to pick out the subtle shift in language or presentation. This served two purposes. First, it could highlight aspects of the epitaph to draw attention to desired sections. Second, the use of multiple languages or dialects displays the skill of the author. Think of it as self-advertising for scribes (D'Agapeyeff, 2006). As interesting as this may be, this answer never seems to slake the thirst so let's take a look at the question that I think they are asking.

What is the earliest known recognizable period cipher? There is a little bit going on in there so let's unpack it bit. We are defining the 'period' in accordance with the SCA, so roughly 600 to 1600 CE. The next question we need to address is 'what is a cipher'. For the purpose of this discussion we're defining a cipher as any reproducible system that can be used to conceal and then reveal a message through an encoding process. Now for the doozy of a question. What is 'recognizable' as a cipher? This question gets into the difference between cryptography and steganography. Cryptography is, by nature, overt. A cipher doesn't hide the fact that it is a cipher, it is just out there (as in the example presented here). Steganography, on the other hand, is covert. That is, it aims to conceal the message rather than to make it unreadable. Based on these definitions we are looking solely at those boldly proclaim "I'm a cipher and you can't read me! Neener. Neeener."

The answer to the above question is that there was lots of stuff! All kinds of stuff! ATBASH, for example, is a Hebrew cipher that dates to at least 500 BCE and was in use by the Knight's Templar throughout our defined period (Singh, 1999). Another somewhat common cryptographic scheme that is seen early in period is to replace each vowel with the consonant that is next to it. A is represented as B. E is represented as F. Then the pattern continues. For an example, we have this folio[1] from the 9th century (Figure 1). Let's focus on the colored letters between the first two dots. The script reads DFPGRBTKBS. This may appear to be garbled nonsense but it is, as you may have guessed, an enciphered message. Following the system outlined above we will pay special attention to the characters that come after each vowel. D[F][P]GR[B]T[K][B]S[2]. Replacing these characters with their vowel values we derive the following, DEOGRATIAS. With word spacing we get the obvious "Deo Gratias" which translates from the Latin to "thanks be to God". Clearly a scribe that was pleased to be done with their labors.



ſiſcribantur pſingula: necipſumarbitro2mundumcapere
coſ: qui ſcribendiſuntlibros ;· DFPGRBTKBS ·ADCHD·

Figure 1

[1] Manuscrits de la Bibliothèque Carnegie de Reims. Quatuor evangelia, cum prologis; 0801-0900, folio 154r, URL: https://gallica.bnf.fr/ark:/12148/btv1b8449025s/f311.item?lang=EN

[2] Remember that in this period the I/J were combined so the next consonant would be the letter K