D. [Symmetric Key Encryption+Classical Ciphers]

D.2

“iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc hwwhbsqvqbre hwq vhlq”

Frequency of characters (in descending order) appearing above:

‘q’ – 10

‘h’ – 7

‘c’ – 6

‘b’, ‘r’, ‘w’ : 5

‘f’, ‘v’ – 4

‘l’, ‘n’ – 3

‘d’, ‘i’ – 2

‘a’, ‘e’, ‘j’, ‘s’, ‘z’ – 1

Replace ‘q’ with ‘E’:

iE ifcc vEEr fb rdE vfllcE na rdE cfjwhwz hr bnnb hcc hwwhbsEvEbre hwE vhlE

Replace ‘h’ with ‘T’:

“vhlE” → “vTlE”. This looks wrong (w.h.p) as no meaningful English word can probably have T in second position and end with E.

Replace ‘h’ with ‘A’:

iE ifcc vEEr fb rdE vfllcE na rdE cfjwAwz Ar bnnb Acc AwwAbsEvEbre AwE vAlE

Note “Ar” can decode meaningfully if ‘r’ is replaced with ‘T’. There are also other choices for ‘r’, e.g., ‘M’, ‘S’, ‘N’ etc. However, ‘T’ is a high frequency letter in English alphabet. Also, note that ‘c’ is the next most frequency letter in the text – but it possibly doesn’t make sense to replace ‘c’ with ‘T’ (as “Acc” is replaced with “ATT”). So we guess this substitution and have:

iE ifcc vEET fb TdE vfllcE na TdE cfjwAwz AT bnnb Acc AwwAbsEvEbTe AwE vAlE

We have exhausted three most frequent characters in English texts, namely ‘E’, ‘T’, ‘A’.

The next four most frequent characters in English alphabet are ‘O’, ‘I’, ‘N’ and ‘S’.

Replace ‘c’ with ‘O’:

“ifcc” → “ifOO”. This looks wrong (w.h.p) as no meaningful 4-lettered English word can end with two ‘O’s.

Replace ‘c’ with ‘I’: “Acc” → “AII” doesn’t make sense.

Replace ‘c’ with ‘N’: “Acc” → “ANN” doesn’t make sense.

Replace ‘c’ with ‘S’:

“Acc” → “ASS” probably doesn’t make sense. ☻ But let’s still stick with this a bit! So we have

iE ifSS vEET fb TdE vfllSE na TdE SfjwAwz AT bnnb ASS AwwAbsEvEbTe AwE vAlE

Notice “TdE” appears twice. We guess ‘d’ to be ‘H’ w.h.p. So we further have:

iE ifSS vEET fb THE vfllSE na THE SfjwAwz AT bnnb ASS AwwAbsEvEbTe AwE vAlE

Some higher-frequency characters are not yet exhausted: ‘O’, ‘I’, ‘N’.

Replace ‘b’ and ‘w’ with ‘O’ or ‘I’: (Note we have already replaced ‘r’ with ‘T’ before.)

Replacing ‘b’ with ‘O’ means a possible replacement of ‘n’ is ‘T’ or ‘P’ (i.e., we get “OTTO” or “OPPO” for “bnnb”). But we have already exhausted ‘T’. So we are left with “OPPO”. But then replacing ‘n‘ with ‘P’ in “na” doesn’t make sense as the ‘a’ in “Pa” cannot possibly decode to anything meaningful.

Replacing ‘b’ with ‘I’ means “bnnb” → “InnI”. This doesn’t decode to anything meaningful for a repeated occurrence of the two ‘n’s in between.

Replacing ‘w’ with ‘O’ means “AwwAbsEvEbTe” → “AOOAbsEvEbTe”. This also doesn’t decode to anything meaningful for a repeated occurrence of the two ‘ww’ in between.

Similarly ‘w’ cannot be replaced with ‘I’ too.

Let’s try next probable combinations with most frequent characters in English: ‘N’, ‘S’ and ‘H’.

Replace ‘b’ and ‘w’ with ‘N’ or ‘H’: (Note ‘r’ also has the same frequency of occurrence as that of ‘b’ and ‘w’. But we have already replaced ‘r’ with ‘T’ before. We also exhausted ‘S’ for replacing ‘c’.)

Replacing ‘b’ with ‘N’ means “bnnb” → “NnnN”. This makes sense only when ‘n’ is replaced with ‘O’. (Recall ‘O’ is not yet exhausted.) Let’s fix ‘b’ (and ‘n’) to be ‘N’ (and ‘O’). So we get

```
iE ifSS vEET fN THE vfllSE Oa THE SfjwAwz AT NOON ASS AwwANsEvENTe AwE vAlE
```

Replacing ‘w’ with ‘H’ doesn’t make sense for “AwE” → “AHE”.

So we proceed as follows.

Replace ‘w’ with ‘R’:

This immediately gives us

```
iE ifSS vEET fN THE vfllSE Oa THE SfjRARz AT NOON ASS ARRANsEvENTe ARE vAlE
```

The longest word in the above string can now be guessed as “ARRANGEMENTS’ with a reasonable probability. However, this means we replaced:

- ‘s’ by ‘G’
- ‘v’ by ‘M’
- ‘e’ by ‘S’ (this implies our prior substitution of ‘c’ with ‘S’ was incorrect!)

With this, we get the following (reverting all ‘S’ with ‘c’ again and further forming new words).

```
iE ifcc MEET fN THE MfllcE Oa THE cfjRARz AT NOON Acc ARRANGEMENTS ARE MAlE
```

Note ‘I’, ‘H’ are not yet exhausted.

Above, we replace ‘f’ with ‘I’ (‘O’ also makes sense, but we already exhausted it.) Further, we had already analyzed before ‘I’ cannot replace ‘c’. So we have

```
iE iIcc MEET IN THE MIllcE Oa THE cIjRARz AT NOON Acc ARRANGEMENTS ARE MAlE
```

Above, note that “Oa” should form a two-lettered preposition w.h.p. (as there is already such a preposition “IN” appearing before). So let’s us replace “Oa” as “OF”. (“ON” could also make sense, but we already exhausted ‘N’.) As a consequence we also replace ‘a’ by ‘F’. So we have

```
iE iIcc MEET IN THE MIllcE OF THE cIjRARz AT NOON Acc ARRANGEMENTS ARE MAlE
```

A close look into the sub-string “MEET IN THE MIllcE OF THE” reveals “’MEET IN THE MIDDLE OF THE” w.h.p. However, this again means we replaced:

- ‘l’ with ‘D’
- ‘c’ with ‘L’

From the above, we have

```
iE iILL MEET IN THE MIDDLE OF THE LIjRARz AT NOON ALL ARRANGEMENTS ARE MADE
```

A closer look immediately reveals we can replace ‘i’ with ‘W’, ‘j’ with ‘B’ and ‘z’ with ‘Y’. These last three guesses put the final nail in the coffin! ☺

```
WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE
```