

Submit your entry on the form at <http://www.cipher.maths.soton.ac.uk/entryform.phtml>

National Cipher Challenge 6 Part A

Vanguard, July twentieth, Seventeen Ninety Eight

My dear Sir,

It is an old saying, ' the Devil's children have the Devil's luck.' I cannot find, or to this moment learn, beyond vague conjecture where the French Fleet and its precious Oriental cargo are gone to. From every information off Malta I believed they were gone to Egypt. Therefore, on the 28th, I was communicating with Alexandria in Egypt, where I found the Turks preparing to resist them, but know nothing beyond report. From thence I stretched over to the Coast of Caramania, not meeting a single Vessel that could give me information. I am as ignorant of the situation of the Enemy as I was twenty-seven days ago. I sincerely hope, that the Dispatches which I understand are at Cape Passaro, will give me full information. I shall be able for nine or ten weeks longer to keep the Fleet on active service, when we shall want provisions and stores. In about six days I shall sail from hence, and if I hear nothing more from the French, I shall go to the Archipelago, where if they are gone towards Constantinople I shall hear of them. I shall go to Cyprus, and if they are gone to Alexandretta, or any other part of Syria or Egypt, I shall get information. Martin has at last broken the ciphers of Marlowe and Walsingham (among them the wretched Alberti and Trimethius ciphers) and believes that that Marlowe's interest in coining might lie at the heart of the mystery. Rumours of a French Line of Battle Ship off Cape Passaro carrying all the riches of the East lend weight to Martin's proposition that Napoleon's flagship L'Orient may be the key to the entire mystery and its destruction should be our highest goal.

SIR HORATIO NELSON, K.B., REAR-ADMIRAL OF THE BLUE, ETC. X

Submit your entry on the form at <http://www.cipher.maths.soton.ac.uk/entryform.phtml>

NOTES

Part A was encrypted by a transposition cipher in blocks of 7 using the keyword Vanguard. The cipher clerk is careless. The Numerals 28 are omitted in the phrase "on the 28th", and the name of the Trithemius cipher is mis-spelled as the Trimethius cipher, no doubt causing a certain amount of confusion since it is the Trithemius cipher which is used to encrypt part B. The Trithemius cipher is a forerunner of the infamous Vigenere cipher, and can be viewed as a special case of the Vigenere using a keyword consisting of the alphabet. Of course the alphabet used here is the 24 character alphabet omitting j and v so this hampers the analysis slightly. Since the cipher is polyalphabetic with a long keyword (24 characters) frequency analysis is close to useless, though the index of coincidence can be used to deduce the length of the keyword, or if you are patient you can try Babbage-Kasiski deciphering.

Submit your entry on the form at <http://www.cipher.maths.soton.ac.uk/entryform.phtml>

National Cipher Challenge 6 Part B

Dear Kit,

Essex hath discoured the existence of our friend and through avarice for our secretes hath set in train a plot against thee for to force our hand. Poems stirring up against foreigners with allusion to thy plays have been posted.

The Council is minded to call thee to account. Whitgift is urging thy detention on charge of blasphemie. Burghley resisteth in private, but may be outplayed.

Against such event Kit we must make plans. Make sure all is recorded safely and deliver it unto me at Greenwich forthwith.

T