WRITING TO CONCEAL ONE'S THOUGHTS.

Diplomatists have for many ages been in the habit of corresponding in cipher, when their communications are of a nature intended only for the sovereign or ministers of their own country. There is a key or clue to render the cipher intelligible; each government keeps its own cipher, with its own key to unlock it; and—truth to tell—is not averse to getting hold of the key of any cipher used by a foreign government, if it can be done. Messengers, couriers, spies, scouts, in war time, sometimes carry secrets into or out of the enemy's country, at peril of death if captured. The writing is sometimes on small bits of thin paper, enclosed in a quill, and concealed by the carrier in some inscrutable way. It was by means of this kind that Havelock, Outram, Inglis, and Clyde kept up a scant and uncertain communication, during the eventful scenes at Lucknow. The most humorous and effectual mode of sending a cryptogram, perhaps was that attributed to a Greek, in the old days; he shaved the head of a slave, wrote on the bald pate with indelible ink, allowed the hair to grow again, and sent off the slave; the correspondent or addressee shaved the head again, and there read the message on the pate. The slave carried the cryptogram, not in his brain, but outside it.

Writing with invisible or sympathetic ink is an amusing expedient, but scarcely secret enough for important communications. Many chemical liquids may be used as inks, to produce writing which is invisible until warmed before the fire, or until steeped in some other liquid. Two persons may exercise their ingenuity in this way. Each writes out an extract from a book, no matter what, in ordinary ink; then, with invisible ink, makes dots under such letters, and dashes under such words as suffice to make up the message. The addressee, on receiving the written extract, knows how to read between the lines, by making the invisible ink visible.

More frequently, however, the cryptogram is prepared by taking some liberty or other with the ordinary language in which you write—a liberty known only to you and your correspondent. For instance, you may write out your message, leaving spaces between the words at intervals, and then put nonsensical words in those spaces, so as to make the entire sentence meaningless; your correspondent will know how to separate the wheat from the chaff. Or you may comprise your message in the left-hand half of the several lines, and fill up the right-hand half with words which give a totally different meaning to them; this process requires, however, a good deal of tact. Or you may use all the proper words, but arrange them in a non-syntactical order, so as to destroy their collective meaning; you agree beforehand with your correspondent as to the precise mode of disarrangement, and he will use this clue in interpreting the gibberish you send him. Suppose your message to be "Do not communicate the fact to him until I have supplied you with additional details from headquarters;" by a transposition of words according to a certain rule, this may become, "The until you details do fact I with communicate not to have from head him supplied additional quarters;" how much a stranger could get out of this, the stranger must say. Or you may agree with your correspondent that the message shall form a sort of square, the words exactly under one another in vertical columns; that some lines shall be read forwards, some backwards; some columns downwards, others upwards; some diagonally to the right, others to the left; some lines or columns skipped over, and brought into requisition afterwards. You may indulge in such dodges in great variety, always taking care that you and your correspondent agree on your mode of operation. Or you may melt many words into one, in the belief that outsiders would hardly detect your meaning when you say for instance, "Ishallnotbeattheofficeto-morrow;" and may make it all the more obscure by reversing the order of the letters, "Worromoteciffoehttaebtonllahsi," a word that looks as if it would well suit a Zulu Caffre. Or you may offer a mare's nest to an inquisitive intruder, by placing the letters in their proper order, and then separating them at random into different words, perhaps with a capital letter here and there, as thus, "Is hallno TB eattheof Ficet omo RR ow," a somewhat mysterious affair. Or you may use the proper words, separated in the proper manner, but with the letters of each word (treated singly) reversed; in this way our supposed sentence would become, "I llahs ton eb ta eht eciffo worromot." Or you may place the letters in each word in the array called by children higgledy-piggledy; as thus, "I lalsh nto eb ta teh focefi romotrow." It is really curious to observe how utterly the appearance of a sentence may change under these different modes of treatment.

Anyone can see that this tossing about and overturning of letters and syllables may be varied in an almost infinite number of ways. It is found, however, that the secret may soon be wormed out by a little attention; and that more complexity is needed if the cryptogram is to be intelligible to the sender and the receiver only. A method of substitution is more available—substitution of one letter for another, or of a numeral for a letter. The variations are almost endless. Let our words (anything will do) be "Lord Dundreary and Brother Sam," and let us use, step by step, the next following letters in alphabetical order instead of the proper ones, as *b* for *a*, *c* for *b*, *d* for *c*, and so on; then the words become "Mpse Evoesfbsz boe Cspuifs Tbn," which would certainly be a "widdle" to the noble lord himself. Take the letters next preceding, instead of those next following, the proper ones, and the words present a totally different appearance, "Knqc Ctmcqdzqx zmc Aqnsgdq Rzl." Quite as unintelligible as before. The reader will not need to be told that the letter selected may be two, three, or more removed from the proper one in each case, and may either alphabetically precede it or follow it. Many of the queer looking advertisements in the "agony column" of *The Times* and other daily papers are constructed in this way. A damsel and her swain not unfrequently do a little billing and cooing by this cryptogrammic agency, but it is well for the lovers to bear in mind that, once the key or clue found out, the message is no longer a secret; and it can without much difficulty be found out if the substituted letter is not many removes from the proper one. For this reason additional difficulties ought to be thrown in, such as some of those already noticed. All the letters of the sentence may be run together as one word; they may be separated into other words or apparent words at random; they may be reversed in position, each word separately, or the whole of them collectively; or capitals may be interspersed among the small letters, for the additional bewilderment of the uninitiated. And there is another wholly distinct course of complication sometimes adopted, of having one system of substitution for the first word, another for the second, another for the third, and so on. A decipherer, not up to the secret, if he succeeded in the first word, might be brought to a standstill at the second, by finding that the key he had used would not unlock the second door. If we had space, and the reader had patience, we might show how many other stumbling-blocks may be introduced in this machinery of substitution; but he can work out this truth for himself.

According to Cocker, 2 and 3 make 5; but in cryptography they may have a great number of equivalents. For instance, 1 may stand for *a*, 2 for *b*, 3 for *c*, and so on up to 0 for *j*; and these numerals may be used instead of these letters throughout a sentence, all being packed together as one word. Thus, for "Captain Webb, the Channel swimmer," we might say, "31pt-19nw522th5381nn51sw9mm5r." Or, the whole may be in numerals, using doublets after the ten single numerals have been appropriated. Or we may form a magic square of twenty-five cells, one for each letter—such as many schoolboys are familiar with in another fashion—with the five numerals running along the top and also down one side; each letter could then be represented by the two numerals at the top and side of the cell in which it stands. The outer world may further be thrown off the scent by giving to the numerals values known only to you and your correspondent; instead of the first ten letters being represented by the ten numerals in their proper order, the latter might assume the form, say, 5806371429—5 standing for *a*, 8 for *b*, and so on.

The cryptographic armoury is by no means exhausted by the use of letters and numerals; dots may be brought in as additional weapons. Thus, *a* may be used for *b*, but *a.* for *c*; *b* for *c*, but *b.* for *d*, etc. Some ciphers or cryptogram keys have been adopted in which dots have various kinds of significance given to them, according as they are placed over or under, on the right or the left of letters or numerals.—*All the Year Round.*