The sieving algorithm.

The 'sieving' algorithm compares cipher words that have letters in common and finds the corresponding plaintext words by consulting word lists.

For example, take the cipher words WZQXTQU and ZXTWQUM. Either one of them alone represents thousands of words. But because they share so many letters the correct plaintext can be found by looking through a word list of 7-letter words and seeking a pair where:

The 1st letter of word 1 is the same as the 4th letter of word 2;
2nd 1st
3rd 5th
4th 2nd
7th 6th

There is just one pair that fits and that is 'cleaner' and 'lancers'. Of course searching a word list is a pain for a human but the computer can do it in a jiffy.

Usually there are many more than just two words in a piece of ciphertext but the solving process is the same. For every pair of cipher words, lists are made of possible plain words. I will call these list1 for the first word of the pair and list2 for the second.

The two lists are sorted by common letters. Then starting with the first word in list1, words in list2 are examined for a match on the common letters.

For example let us say the two cipher words are NMXMZOQ and NXMZW. Word lists are made for each and sorted by common letters. The lists begin:

NMXMZOQ	NXMZW
List1	List2
AUGURED	ABETS
ARMREST	ABHOR
BEDEVIL	ABIDE
BEHEADS	ABLER
BALANCE	many words
BOLOGNA	BLADE
BENEFIT	BLAME
BENEATH	**BLAND**
	BLANK
	BLARE

Note the lists are in alphabetical order of the common letters. So AUGURED comes before ARMREST because the second letter is not common in the cipher words.

Beginning at the top of list 1, AUGURED is dropped because then the second word would have to read AGUR- and no such word is found in list 2. ARMREST, BEDEVIL, BEHEADS are dropped for the same reason. Then BALANCE, seeking a word BLAN- in list 2, finds BLAND and BLANK which are both retained so BaALANCE is retained in list 1 and BLAND, BLANK in list 2.

BLARE is the next word in list 2 and is not a fit, so consideration goes back to list 1. There the next word is BOLOGNA which is rejected as are many more until CARAFE which seeks CRAF- in List 2. It starts where it left off, rejects BLARE and all that follow until it finds CRAFT. The next word CRAMP does not fit, so control goes back to list 1 to the word that follows CARAFE.

And so the process continues down the two lists until the end of one of the lists is reached.

Then another two cipher words are chosen and the winnowing process starts again. This is repeated with every possible combination of cipher words, until no further winnowing is possible. At that stage hopefully there remains just one word in each list and they form the solution.

Of course this algorithm will only work when the ciphertext is written with a space after each word. This is the case for Aristo ciphers and Headline puzzles.