An affine cipher can be anything in the form (ax+b) mod 26 (the mod 26 just means take off 26 if it's greater than that). a must be an odd number less than 26 other than 13 (there is a technical reason for this but I won't get into it here) b can be any number from 0-25. To find the reverse of the cipher you do ((a^-1)x-b) mod 26 (though this only helps if you know the encryption key) (also note that the a^-1 isn't 1/a it's the modular inverse. You can read about that here: [en.wikipedia.org/wiki/Modular\_multiplicative\_inverse](https://en.wikipedia.org/wiki/Modular_multiplicative_inverse))  
  
In terms of finding out weather it's Caesar or Affine or some other form of mono-alphabetic cipher there isn't really a good way to tell. I'd recommend trying frequency analysis first as that can really help. Also look for individual letters in the text. You'll know that these are either a or I (basically find a mini crib). Once you have two letters that you know you need to find the b value that would convert the plaintext letter into the ciphertext letter. For example if you wanted to make G (ciphertext letter) into i (plaintext letter) There are a number of ways to do that:

|  |  |
| --- | --- |
| a | b |
| 1 | 2 |
| 3 | -10 or 16 |
| 5 | 4 |

I've only done up to five here but you'd have to do all of the values up to 25. Repeat this for the other letter that you know and check for a pair that is common to both. This will be the decryption key (just plug it in, in the form (ax+b) mod 26. I know this seems quite complicated and it is a method best suited for computers but it may help you (especially if you can find that crib). There will be other methods available if you search for them, I'm sure.  
  
(BTW to get the b value you do plain\_letter-a\*cipher\_letter (remembering to count from 0 for the letters) in this example it was 8-a\*6 as i is the 8th letter and g is the 6th (counting from a=0))

The function used to encrypt the message can change provided it is of the form a\*x+b. However, a must be coprime (highest common divisor being 1) with 26 (assuming the message is in English). This means that the valid values of a are: 3,5,7,9,11,13,15,17,19,21,23,25 (if a=1, then it becomes a Caesar shift cipher).  
  
In terms of cryptanalysis, frequency analysis applies here in the same way as any other general substitution cipher. If you can guess the decryption of two letters, the values of a and b can be found by solving a pair of simultaneous equations. A Caesar cipher can be broken in the same way (a will be found to be 1) and so it is generally easiest to attempt to break the cipher as an affine cipher. Since guessing two letters is not much harder or time-consuming than guessing one, this is not too difficult.

As one of the largest problems facing cryptography and mathematics I think it would be good if we, some of the smartest young minds of our generation, tackled prime factorisation. How to split up big numbers quickly.  
There is the obvious method (try every prime up to the square root of the number) but I was wondering if anyone knew of (or could suggest) any short cuts to factorisation.  
  
BTW it may help if you start by proving the Riemann Hypothesis (this has the added bonus of a $1,000,000 reward).

|  |
| --- |
| Why start small and work your way up? Pick the largest number that you know is definitely a factor: e.g. 120 - Don't start with 2 x 60 as that will take the most steps...  120 = 10 x 12 120 = 5 x 2 x 3 x 4 120 = 5 x 2 x 3 x 2 x 2 120 = 23 x 3 x 5  Do as much as you can at the same time. Just a thought. Or use a computer. Or a scientific calculator that has a "FACT" function... ;) |
|  |

In all seriousness, however, I believe the Quadratic Sieve and General Field Sieve are the best algorithms for classical computers.

*Hi i have a question a bit off topic, but i'm a bit lost. In set theory, what is meant by "The Union of the sets Aα,α∈ I, is deﬁned to be the set {x | x ∈ Aα for at least one α ∈ I} ? (I means index set)*

Here is a venn diagram, to try and help get a handle on this:

***This image is hidden for guests.  
Please log in or register to see it.***

In this case, we just have two sets, A and B. (As it happens they are both contained in the larger set U.)  
An element x is in the union if x is in at least one of A or B (from your definition). This means that if x is in A but not B, we've got it. If it's in B but not A, we've got it. If it's in A and in B, we've got it. But if it's in neither (meaning it's outside both circles), then it isn't in the union.  
  
With more sets, the idea is the same. For x to be in the union of a family of sets, it only needs to be the case that it is in one of them (although it can be in many more).

The union of two sets A and B is the set that contains all the elements of A together with all the elements of B, and nothing else. It is important to note that if something belongs to both sets it still only belongs to the union once, so if A={1,2,3} and B={2,3,4} then AUB={1,2,3,4} not {1,2,2,3,3,4}.  
  
The same idea applies when taking the union of three sets, so if C={4,5,6,7} then AUBUC={1,2,3,4,5,6,7}.  
  
In general mathematicians like to be able to take the union of lots of sets at once, maybe even infinitely many. Here it can be difficult to keep track of the set names. If you have more than 26 of the sets you run out of letters, so typically you might want to use numbers to help name them, we call this indexing. So the first set might be called A1, the second A2 and so on. Usually the number would be a subscript or superscript, but that is hard to do in forum code! But that is that is meant by the index. If you are using that convention to name your sets then the index set is the natural numbers and an arbitrary set in your list is called Ai, where i represents the index and can be any one of 1,2,3, and so on. While the indexing set is the natural numbers in this case it can sometimes be useful to index sets by some other index, for example if you have a set for each real number r. In its most general form you could have any set you like as an indexing set, call it I and then for each element i in I associate a set Bi. In the definition you are giving above they are using the greek letter alpha to denote the index where I have used i, but it is the same idea.  
  
Then the definition of the union of all of the Bi is that you take the set whose elements are exactly those elements appearing in at least one of the Bi. And that is what the symbols in your definition above mean. The union is defined by the property that x is in the union of the sets Bi if and only if it is in a least one of the sets Bi.  
  
Hope that helps,  
  
Harry

Challenge 5:

I cracked part a and from the text

**Warning: Spoiler!** [ Click to expand ][ Click to hide ]

(which said it was vigenere)

and the key

**Warning: Spoiler!** [ Click to expand ][ Click to hide ]

(which was railfence)

I take it part b was a mix between the two. I failed to crack it though which leaves me with a few questions....  
1) Am I right about it's composition?  
2) Which order were they done in

**Warning: Spoiler!** [ Click to expand ][ Click to hide ]

3) How many rails  
4)What was the key for the vigenere?

(spoiler-ed just in case anyone wants to work it out for themselves but hasn't yet)  
I'm afraid it was far less ingenious... the key to part A was very interesting, but not very relevant to part B!

OK, so let's say 7A tells me the Cipher that's used in 7B like 6A did for 6B, and let's say I've managed to crack all possible combinations based on the clues given, but still haven't found anything that's English. Does this mean that from now on, any cipher methods used aren't carried out religiously, and the people running this may have tweaked it up a bit. Also, it is possible that the clue in 7A is lying?

Of course it could be possible... Many things are possible! Another possibility is that you've not implemented it "correctly", or at least that your interpretation of the implementation is not the same as the one that's been used.