I don't offer here a general complete solution, but rather some small ways to cut down on the necessary execution time, for every little bit helps. To follow and understand this partial solution, it helps to be familiar with the material covered in a standard first semester graduate level course in abstract algebra: specifically group theory, ring theory, module theory and field theory.

First, for a crash course on group theory:

A group is a set G together with a binary operation * defined on it, such that the following properties are true:

1. For any a,b in G, a*b is in G too.
2. There is an element e (called the identity element) such that for any a in G, a*e = e*a = a.
3. For any a in G, there is a b in G (called the inverse of a) such that a*b=b*a=e, the identity element. and
4. For any a,b,c in G, (a*b)*c=a*(b*c) (the associativity of *).

If the additional property, called the commutativity of *, is also true, that is, for all a,b in G, if a*b=b*a, then the group is called an abelian (or commutative) group. A group such as the set G with the binary operator * is usually identified simply as the group G. A subset S of a group G that is itself a group under the same binary operator is called a subgroup, so if a and b are in S, then a*b is in S too and a*b in S is the same as a*b in G, and the identity element of G is also the identity element of S, and if a is in S, then the inverse of a in G is also the inverse of a in S.

One important example of a group, which is not an abelian group, by the way, is the set of permutations of a set of n elements, where the identity permutation is the identity element of the group, and where the group operation is the composition of permutations. A permutation is basically a one to one function from the set of n elements to itself, and the identity permutation takes every element of the set to itself, while the composition of permutations is the composition of the functions that they represent. Another important example of a group is the set of symmetries of a geometric shape, with every symmetry thought of a function of the geometric shape to itself, that maps the shape to itself, although not every point is taken to itself. The identity symmetry is the function that takes every point to itself.

Two groups G and H, involving the binary operators * and @, respectively, are called isomorphic if there is a one to one map f from G onto H, called an isomorphism, for which every element of H is the image under this isomorphism of an element of G, such that for any a,b,c in G such that a*b=c, f(a) @ f(b) = f(c) too, and such that the image under f of the identity element of G is the identity element of H. Isomorphic groups are basically the same groups after renaming all of the elements and the binary operator. An example is if G is the integers modulo 6, with addition + as its binary operator, and H is the integers, that are not divisible by 7, modulo 7, with multiplication as its binary operator. The identity element of G is 0 mod 6 and the identity element of H is 1 mod 7. In G, the inverses of 0,1,2,3,4 and 5, mod 6, are 0,5,4,3,2 and 1, mod 6, respectively, and in H, the inverses of 1,2,3,4,5 and 6, mod 7 are 1,4,5,2,3 and 6, mod 7, respectively. G and H are isomorphic with f as an isomorphism such that f(0)=1, f(1)=3, f(2)=2, f(3)=6, f(4)=4 and f(5)=5. Notice that G (and therefore H) is isomorphic with itself with the isomorphism g such that g(0)=0, g(1)=5, g(2)=4, g(3)=3, g(4)=2 and g(5)=1. Such an isomorphism from a group to itself is called an automorphism.

Every finite group is isomorphic to a subgroup of the group of permutations of a finite set. The direct sum F of two groups G and H (I will represent their binary operation here as addition) is a group which has subgroups G(F) and H(F) that are isomorphic to G and H, respectively, such that any element of F can be expressed, uniquely, as the sum of an element of G(F) with an element of H(F), that is, for any c in F, there is a unique element a in G(F) and there is a unique element b in H(F), such that c=a+b. Also, in such a direct sum, if d is also in F, h is also in G(F) and k is also in H(F) and if d=h+k, then the unique expression of c+d in F as the sum of an element in G(F) and an element of H(F) is c+d = (a+h) + (b+k). The direct sum can also be extended to any number of groups in a sequence, so that their direct sum is a group with subgroups isomorphic to every group in the original sequence such that any element of the direct sum group can be expressed uniquely as the sum of elements in the respective subgroups, in the same order. This direct sum also has the property that the sum of two elements c and d in the direct sum group is the sum of the elements in the respective subgroups that are themselves the sums of the corresponding components of c and d in those respective subgroups. That is, you can think of an element in the direct sum group as a vector whose components are in the respective groups in the original sequence of groups, and the sum of two such vectors is the vector whose components are the sums of the corresponding components of the original two vectors. Of course, if the groups are abelian, then the order of the groups in the sequence doesn't matter. If the group binary operation is represented as multiplication, the this direct sum is usually called the direct product.

A group G, with binary operator *, is called cyclic if it has an element g that generates the group, that is, if there is a g in G such that for every h in G, h = g*g*g*…*g, or h = k*k*k*…*k, where k is the inverse of g, a certain number of times (which may be 1 or even 0). g is called a generator of the cyclic group. All groups (and they are abelian groups) that are the integers modulo some positive integer, with binary operator addition, are cyclic, with 1 as one possible generator. Relatively prime integers are defined to be those whose greatest common factor is 1, so integers relatively prime to g are those that don't have any prime factors in common with g. For any integer g, it is known and has been proven that the integers modulo g that have multiplicative inverses modulo g are exactly those that are relatively prime to g. That is, integer h and integer g are relatively prime if and only if there is an integer j such that the product of h and j is 1 modulo g. From here on, I will call the abelian group of integers modulo g under the binary operator of addition, <g,+> and the abelian group of integers, relatively prime to g, modulo g, under the binary operator of multiplication, <g,*>. It is also known and has been proven that for any prime number p, that <p,*> is cyclic. Furthermore, it is known and has been proven that the same is true for <q,*>, for q a perfect power of p, as long as p is an odd prime. And it is known and has been proven that <r,*>, for r a perfect power, greater than 1, of 2 (that is, for r=4,8,16,etc.), is isomorphic to the direct sum of the following two groups of binary operator addition: the integers modulo 2 and the integers modulo some (other) perfect power of 2. For any cyclic group <q,*> for q some perfect power of p, and for any generator s of <q,*>, there is an isomorphism to a group <r,+> that maps s to 1."

Now consider <g,*> for any positive integer g. Let w(1),w(2),w(3),…,w(n) be the n (and only n) prime numbers that are factors of g, for some positive integer n. Let m(1),m(2),m(3),…,m(n) be the maximum positive integers such that for any i, w(i) to the m(i) power is a factor of g. It is known and has been proven that G is isomorphic to the direct product of the groups <s(i),*>, where s(i) = w(i) to the m(i) power, for i=1,2,3,…,n.

Next, for a crash course on ring and field theory:

A Ring R is an abelian group, with a group operation that I will call addition (+), with the identity element, which is called the additive identity element (0) with the following extra properties:
1. There is a second binary operator defined on the set, which I will call multiplication (*). For any two elements a and b in R, a*b is also in R.
2. * is associative, that is, for any a,b and c in R, (a*b)*c = a * (b*c)
3. * is distributive over addition, that is, for any a,b and c in R, a*(b+c) = (a*b) + (a*c) and (b+c)*a = (b*a) + (c*a)
4. There is a unique multiplicative identity element, which I will call 1, such that for any a in R, 1*a = a*1 = a.
5. I will call the inverse of a, as a member of the abelian group R, with respect to +, -a. It is called the additive inverse of a .

One important example (there will be others) of a ring is the set of square n by n matrices for positive integer n. + is simply the addition of matrices, and * is the multiplication of matrices. 0 is simply the zero matrix and 1 is the identity matrix.

A commutative ring is a ring R with an additional important property, that is * is commutative, that is, for any a and b in R, a*b = b*a. Important examples of commutative rings are the set of polynomials under normal polynomial addition and multiplication, where the additive and multiplicative identities are the 0 and 1 constant, zero degree, polynomials, respectively, the set of integers modulo n, for n any positive integer, under addition and multiplication modulo n, where the additive and multiplicative identities are 0 and 1 mod n, respectively, and the set of integers under normal addition and multiplication. A field is a commutative ring with the additional important property of the existence of the multiplicative inverse. That is, for any a in a field F that is not 0, there is a unique b in F such that a*b = b*a = 1. Important examples of fields are the rational numbers, the real numbers and the complex numbers under ordinary addition and multiplication, the set of rational functions under normal addition and multiplication, where the additive and multiplicative identities are the 0 and 1 constant rational functions, respectively, and the integers modulo p for prime number p, under addition and multiplication modulo p, where the additive and multiplicative identities are 0 and 1 mod p, respectively.

The characteristic of a ring (including a field) is the smallest positive integer n such that for any element a of the ring, n*a is always 0. If there is no such positive integer, then the characteristic is said to be 0. The characteristics of the following rings are all 0: the set of matrices whose elements are the real numbers (or rational numbers, or complex numbers, or integers), the set of polynomials or the set of rational functions whose coefficients are the real numbers (or rational numbers, or complex numbers, or integers), the integers, the rational numbers, the real numbers and the complex numbers. The characteristic of the integers modulo n, for positive integer n, is n. The characteristic of a field is always either 0 or a prime number.

A subring of a ring R is a subset of R that is a ring in itself, that is, such that 0 and 1 are in that subset, the result of applying + or * to any two elements of that subset results in another element of that subset, and such that the additive inverse of any element of that subset is again in that subset. Similarly, a subfield of a field F is a subset of F that is a field in itself, that is, that is a subring of F such that the multiplicative inverse of any nonzero element of that subset is again in that subset. An example is that the integers are a subring of the rational numbers. Another is that the rational numbers are a subfield of the real numbers, which are a subfield of the complex numbers.

If F is a subfield of the field H, then H is called an extension field of the field F. An extension field H of F is called algebraic over F if every element of H is the root of a polynomial whose coefficients are in F. Otherwise, H is called transcendental over F. If H is the smallest field that contains the field F and the root of a polynomial whose coefficients are in F (it is said that H is the field generated by F and that polynomial root), then H will always be algebraic over F, that is, any element of H will also be the root of a polynomial whose coefficients are in F. If the field H is the smallest field containing the field F and a root of the polynomial p whose coefficients are in F, and p is irreducible over F, (that is, cannot be factored anymore over F, that is, there are no two non-constant polynomials q and r, whose coefficients are in F, such that q*r=p), then the degree of H over F is the degree of p. The degree of an extension field will always be the same, for any irreducible polynomial p over F, with coefficients in F, one of whose roots, together with F, also generates H, that is, the degree of any such irreducible polynomial will always be the same. The complex numbers are algebraic over the real numbers, with degree 2, but the rational functions over the real numbers are transcendental over the real numbers. Obviously, any algebraic extension field of F with degree 1 has to be F itself! If H is algebraic over F with degree n, w, then every element of H can be expressed as a polynomial of degree n-1 with coefficients in F, where, if the variable of the polynomial is x, then x^n = s(x), where s is a polynomial of degree (at most) n-1. So the complex numbers are all linear polynomials over the real numbers, with polynomial variable i, where i^2 = -1.

An algebraic extension can also have an infinite degree, which means that there is no finite polynomial over the subfield (that is, whose coefficients are in that subfield), whose roots, together with the subfield, generate the entire extension, although every one element of the extension is the root of a polynomial of finite degree over the subfield. The algebraic closure of a field F is the unique greatest algebraic extension field possible that contains F. Any algebraic extension of a field has the same algebraic closure as the field itself. An extension field of field F always has the same characteristic as F, and a subfield of field F always has the same characteristic as F. The same is true of rings in general. The finite field of p^n elements, for prime number p and positive integer n, is the algebraic extension field of degree n of the field of the integers modulo p, and the algebraic closure of a finite field has an infinite degree over the finite field. The algebraic closure of the rational numbers also has infinite degree over the rational numbers, and is not the field of complex numbers, for there are complex numbers that are transcendental over the rational numbers, but the complex numbers are a transcendental extension of the algebraic closure of the rational numbers.

If fields G and H are algebraic extensions of field F, and the degree of H over F is n and the degree of G over F is m, and if furthermore H is an extension field of G, then n has to be divisible by m. For finite fields of the same characteristic p (which therefore have as numbers of elements perfect powers of p), the finite field of p^n elements is isomorphic to an extension field of the finite field of p^m elements if and only if n is divisible by m. In fact, if G is an algebraic extension of F of degree m and H is an algebraic extension of G of degree p, then the degree of H over F is pm. Also, in consideration of things I said earlier, every element of the finite field of p^n elements can be thought of as a polynomial of degree < n with coefficients in the field of the integers modulo p, and the field has characteristic p.

The concept of algebraic extension can also be applied to rings in general, as the rings generated by the original ring and the roots of a polynomial with coefficients in the ring. Also the concept of transcendental extension. An algebraic extension of a ring or field of degree 2 is called a quadratic extension, and consists of the result of extending the ring by the square root of a previous element of the ring. Two rings R and S, involving the multiplication operators * and @, respectively, and addition operators + and #, respectively, are called isomorphic if there is a one to one map f from R onto S, called an isomorphism, for which every element of S is the image under this isomorphism of an element of R, such that for any a,b,c in R such that a+b=c, f(a) # f(b) = f(c) too, such that for any a,b,c in R such that a*b=c, f(a) @ f(b) = f(c) too, such that the image under f of the additive identity element of R is the additive identity element of S, and such that the image under f of the multiplicative identity element of R is the multiplicative identity element of S. Isomorphic rings are basically the same rings after renaming all of the elements and the binary operators. An example is if R is the set of 2 x 2 matrices whose elements are real numbers, where the top left and bottom right elements are equal to each other and the top right and bottom left elements are additive inverses (negatives) of each other, under normal matrix addition and multiplication, and S is the set of complex numbers under normal addition and multiplication, where the image under the isomorphism of the identity matrix is the complex number 1 and the image of the matrix, whose top left and bottom right elements are 0 and whose top right element is a and bottom left element is -1, is i (the square root of -1). An automorphism of a ring is an isomorphism of the ring to itself. An example is the set of complex numbers, where the automorphism maps every complex number to its complex conjugate.

There is an automorphism of quadratic extensions of rings, of which the complex numbers as a quadratic extension of the real numbers is an example, that interchanges r and -r, where the square of r was an element of the original ring, R, but r itself was not (so that the extension is generated by r). Any element of the extension of R generated by r can be expressed as s + tr, where s and t are in R. The automorphism of the quadratic extension of R that interchanges r and -r also interchanges s + tr and s - tr. s + tr and s - tr are called conjugates (this generalizes the concept of complex conjugates), and I will call this automorphism the "conjugate automorphism".

A finite field is a field with a finite number of elements, which will always have a characteristic of p for some positive prime number p. The integers modulo p, for prime number p, is a finite field of p elements, with characteristic p. Every finite field has p^n elements, for some prime number p and some positive integer n, and that field has characteristic p. For any prime number p and any positive integer n, and for any two fields F and H with p^n elements, F and H are isomorphic.

The nonzero elements of any field form an abelian group, and if the field is finite, the group is cyclic. Therefore, they have generators, and every nonzero field element has a discreet logarithm based x, for any generator x of the cyclic group of nonzero field elements. If x is not a generator, then there is a positive integer n > 1 such that exactly 1/n of the nonzero field elements have a discreet logarithm based x, and they all have n such discreet logarithms.

An integral domain is a commutative ring that has the property that if the product of any two members is 0, then one of the factors must be 0. The ring of integers and the rings of polynomials in any number of variables, whose coefficients are integers, rational numbers, real numbers or complex numbers, are all integral domains, and every field is an integral domain. The ring of integers modulo 30 (30 is the product of 2,3 and 5) is not an integral domain, because, for example, the product of 6 mod 30 and 5 mod 30 is 0 mod 30. Every integral domain has a unique field of fractions, which is the field of fractions whose numerators and whose denominators are all from that integral domain. So the field of fractions of a field is the field itself, the field of fractions of the integers is the rational numbers, the field of fractions of the ring of polynomials over a given set of variables and with coefficients in a given field is the set of rational expressions over the same variables and with coefficients in the same field, and the field of fractions of the ring of complex integers, that is, the complex numbers with integer real and pure imaginary components, is the set of complex rationals, that is, the complex numbers with rational real and pure imaginary components.

An ideal I of a ring R is a subset of R with the property that the sum of any two members of I is again in I and the product of any member of I with any member of R is a member of I. Examples of ideals are the set of even integers among the ring of integers, the set of integers that are multiples of 30 or any other fixed integer, the subset of the ring of polynomials in the variable x that have a 0 constant term, the subset of the ring of three variable polynomials in the variables x,y and z all of whose nonzero terms are multiples of x or y, and the subset of the ring of integers modulo 30 that are divisible by 3. The product of two ideals I1 and I2 is the ideal formed by the products of any j1 in I1 and any j2 in I2. In the ring of polynomials in the four variables w,x,y,and z with integer coefficients, if one ideal is the set of all polynomials whose only nonzero terms are multiples of x or y, and another ideal is the set of polynomials whose only nonzero terms are multiples of z and all of whose coefficients are even, that is, all of the nonzero terms are multiples of 2z, then the product ideal is the set of polynomials whose only nonzero terms are multiples of 2xZ or 2yz. One ideal being a multiple or factor of another has the same meaning as for integers or for elements of any ring. Similarly, factorization of an ideal has the same meaning as for elements of any ring. A prime ideal is an ideal whose only factors are itself and 1, 1 being the "ideal" that is the entire ring. A principal ideal of a ring is an ideal that consists entirely of multiples of a given member of the ring, for example, the ideal of the ring of integers that are the multiples of a given integer, or the ideal of the ring of polynomials in the two variables x and y that are all the polynomials that are multiples of xy. An example of an ideal that is not principal in the ring of polynomials in the two variables x and y is the set of all polynomials all of whose nonzero terms are multiples of either x or y.

Next, the DLP problem.

The problem is to solve for x in $a^x = b \pmod p$, where p is a prime number and it is assumed that a, b and p are known. Because the multiplicative group of nonzero elements of all the finite fields are cyclic, including the integers modulo p, the problem can be converted to that of solving for y such that $cy = d \bmod (p-1)$, where for some unknown generator z of the multiplicative group of integers modulo p, $z^c = a$ and $z^d = b$. There is a solution if and only if the greatest common factor between c and p-1 divides the greatest common factor between d and p-1 and in that case the number of solutions between 1 and p-1 is the ratio of the latter to the former.

Now the real object of the discreet logarithm problem is to solve for the discreet logarithm in a shorter amount of time when the known integers involved are prime and very large. I don't offer here a general complete solution, but rather some small ways to cut down on the necessary execution time, for every little bit helps. In solving for x in $a^x = b \pmod p$, where p is a prime number and it is assumed that a, b and p are known, but that p is extremely large, so that trial and error is expected to take a lifetime even with the fastest computers. It turns out that a generator z of the multiplicative group of integers modulo p does not have to be found. It follows from the analysis in the preceding paragraph that if m is a factor of p-1, then $a^m = 1 \pmod p$ if and only if a is a perfect (p-1)/m power, mod p. So let y_a and y_b be the greatest possible respective factors of p-1 such that a is a perfect y_a power, mod p, and b is a perfect y_b power, mod p. If y_b is an integral multiple of y_a, then not only is the first solution for x between 1 and $(p-1)/y_a$, x must also be an integral multiple of y_b/y_a. This greatly cuts down the search space. Of course, this won't help if $y_a = y_b = 1$. But it is also the case that x cannot be any integral multiple $w(y_b/y_a)$ of y_b/y_a if w has any factor (> 1) in common with $(p-1)/y_b$. That is, x has to be coprime with p-1. This further cuts down the search space.