The Most Important Algorithms

After a long discussion with some of my RISC colleagues about what the 5 most important algorithms on the world are, we couldn't reach a consensus on this question. So, I suggested to perform a little survey. The criterion for suggestions was that these algorithms should be widely used. Further we restrict ourselves to the fields of computer science and mathematics. As I expected the number of different suggestions is close to

5 * (no. of participants).

In the following you find the results (in alphabetical order) of this survey (which of course is highly non-representative since most of the participants are computer scientists).

1. **A* search algorithm**
   Graph search algorithm that finds a path from a given initial node to a given goal node. It employs a heuristic estimate that ranks each node by an estimate of the best route that goes through that node. It visits the nodes in order of this heuristic estimate. The A* algorithm is therefore an example of best-first search.
2. **Beam Search**
   Beam search is a search algorithm that is an optimization of best-first search. Like best-first search, it uses a heuristic function to evaluate the promise of each node it examines. Beam search, however, only unfolds the first m most promising nodes at each depth, where m is a fixed number, the beam width.
3. **Binary search**
   Technique for finding a particular value in a linear array, by ruling out half of the data at each step.
4. **Branch and bound**
   A general algorithmic method for finding optimal solutions of various optimization problems, especially in discrete and combinatorial optimization.
5. **Buchberger's algorithm**
   In computational algebraic geometry and computational commutative algebra, Buchberger's algorithm is a method of transforming a given set of generators for a polynomial ideal into a Gröbner basis with respect to some monomial order. One can view it as a generalization of the Euclidean algorithm for univariate gcd computation and of Gaussian elimination for linear systems.
6. **Data compression**
   Data compression or source coding is the process of encoding information using fewer bits (or other information-bearing units) than an unencoded representation would use through use of specific encoding schemes.
7. **Diffie-Hellman key exchange**
   Cryptographic protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
8. **Dijkstra's algorithm**
   Algorithm that solves the single-source shortest path problem for a directed graph with nonnegative edge weights.
9. **Discrete differentiation**
   I.e., the formula f'(x) = (f(x+h) - f(x-h)) / 2h.
10. **Dynamic programming**
    Dynamic programming is a method for reducing the runtime of algorithms exhibiting the properties of overlapping subproblems and optimal substructure, described below.
11. **Euclidean algorithm**
    Algorithm to determine the greatest common divisor (gcd) of two integers. It is one of the oldest algorithms known, since it appeared in Euclid's Elements around 300 BC. The algorithm does not require factoring the two integers.

12. **Expectation-maximization algorithm (EM-Training)**
    In statistical computing, an expectation-maximization (EM) algorithm is an algorithm for finding maximum likelihood estimates of parameters in probabilistic models, where the model depends on unobserved latent variables. EM alternates between performing an expectation step, which computes the expected value of the latent variables, and a maximization step, which computes the maximum likelihood estimates of the parameters given the data and setting the latent variables to their expectation.
13. **Fast Fourier transform (FFT)**
    Efficient algorithm to compute the discrete Fourier transform (DFT) and its inverse. FFTs are of great importance to a wide variety of applications, from digital signal processing to solving partial differential equations to algorithms for quickly multiplying large integers.
14. **Gradient descent**
    Gradient descent is an optimization algorithm that approaches a local minimum of a function by taking steps proportional to the negative of the gradient (or the approximate gradient) of the function at the current point. If instead one takes steps proportional to the gradient, one approaches a local maximum of that function; the procedure is then known as gradient ascent.
15. **Hashing**
    A function for summarizing or probabilistically identifying data. Typically this means one applies a mathematical formula to the data, producing a string which is probably more or less unique to that data. The string is much shorter than the original data, but can be used to uniquely identify it.
16. **Heaps (heap sort)**
    In computer science a heap is a specialized tree-based data structure. Heaps are favourite data structures for many applications: Heap sort, selection algorithms (finding the min, max or both of them, median or even any kth element in sublinear time), graph algorithms.
17. **Karatsuba multiplication**
    For systems that need to multiply numbers in the range of several thousand digits, such as computer algebra systems and bignum libraries, long multiplication is too slow. These systems employ Karatsuba multiplication, which was discovered in 1962.
18. **LLL algorithm**
    The Lenstra-Lenstra-Lovasz lattice reduction (LLL) algorithm is an algorithm which, given a lattice basis as input, outputs a basis with short, nearly orthogonal vectors. The LLL algorithm has found numerous applications in cryptanalysis of public-key encryption schemes: knapsack cryptosystems, RSA with particular settings, and so forth.
19. **Maximum flow**
    The maximum flow problem is finding a legal flow through a flow network that is maximal. Sometimes it is defined as finding the value of such a flow. The maximum flow problem can be seen as special case of more complex network flow problems. The maximal flow is related to the cuts in a network by the Max-flow min-cut theorem. The Ford-Fulkerson algorithm computes the maximum flow in a flow network.
20. **Merge sort**
    A sorting algorithm for rearranging lists (or any other data structure that can only be accessed sequentially, e.g. file streams) into a specified order.
21. **Newton's method**
    Efficient algorithm for finding approximations to the zeros (or roots) of a real-valued function. Newton's method is also a well-known algorithm for finding roots of equations in one or more dimensions. It can also be used to find local maxima and local minima of functions.

22. **Q-learning**
    Q-learning is a reinforcement learning technique that works by learning an action-value function that gives the expected utility of taking a given action in a given state and following a fixed policy thereafter. A strength with Q-learning is that it is able to compare the expected utility of the available actions without requiring a model of the environment.
23. **Quadratic sieve**
    The quadratic sieve algorithm (QS) is a modern integer factorization algorithm and, in practice, the second fastest method known (after the number field sieve, NFS). It is still the fastest for integers under 110 decimal digits or so, and is considerably simpler than the number field sieve.
24. **RANSAC**
    RANSAC is an abbreviation for "RANdom SAmple Consensus". It is an algorithm to estimate parameters of a mathematical model from a set of observed data which contains "outliers". A basic assumption is that the data consists of "inliers", i. e., data points which can be explained by some set of model parameters, and "outliers" which are data points that do not fit the model.
25. **RSA**
    Algorithm for public-key encryption. It was the first algorithm known to be suitable for signing as well as encryption. RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys.
26. **Schönhage-Strassen algorithm**
    In mathematics, the Schönhage-Strassen algorithm is an asymptotically fast method for multiplication of large integer numbers. The run-time is O(N log(N) log(log(N))). The algorithm uses Fast Fourier Transforms in rings.
27. **Simplex algorithm**
    In mathematical optimization theory, the simplex algorithm a popular technique for numerical solution of the linear programming problem. A linear programming problem consists of a collection of linear inequalities on a number of real variables and a fixed linear functional which is to be maximized (or minimized).
28. **Singular value decomposition (SVD)**
    In linear algebra, SVD is an important factorization of a rectangular real or complex matrix, with several applications in signal processing and statistics, e.g., computing the pseudoinverse of a matrix (to solve the least squares problem), solving overdetermined linear systems, matrix approximation, numerical weather prediction.
29. **Solving a system of linear equations**
    Systems of linear equations belong to the oldest problems in mathematics and they have many applications, such as in digital signal processing, estimation, forecasting and generally in linear programming and in the approximation of non-linear problems in numerical analysis. An efficient way to solve systems of linear equations is given by the Gauss-Jordan elimination or by the Cholesky decomposition.
30. **Strukturtensor**
    In pattern recognition: Computes a measure for every pixel which tells you if this pixel is located in a homogenous region, if it belongs to an edge, or if it is a vertex.
31. **Union-find**
    Given a set of elements, it is often useful to partition them into a number of separate, nonoverlapping groups. A disjoint-set data structure is a data structure that keeps track of such a partitioning. A union-find algorithm is an algorithm that performs two useful operations on such a data structure:
    Find: Determine which group a particular element is in.
    Union: Combine or merge two groups into a single group.
32. **Viterbi algorithm**
    Dynamic programming algorithm for finding the most likely sequence of hidden states - known as the Viterbi path - that result in a sequence of observed events, especially in the context of hidden Markov models.