Sample Questions for LP III

Machine Learning

1. Linear Regression is a supervised machine learning algorithm.

Yes, Linear regression is a supervised learning algorithm because it uses true labels for training. Supervised learning algorithm should have input variable (x) and an output variable (Y) for each example.

2. Linear Regression is mainly used for Regression.

Yes, Linear Regression has dependent variables that have continuous values.

3. It is possible to design a Linear regression algorithm using a neural network?

True. A Neural network can be used as a *universal* approximator, so it can definitely implement a linear regression algorithm.

4. Which of the following methods do we use to find the best fit line for data in Linear Regression?

A. Least Square Error
B. Maximum Likelihood
C. Logarithmic Loss
D. Both A and B

Least Square Error, In linear regression, we try to minimize the least square errors of the model to identify the line of best fit.

5. Which of the following evaluation metrics can be used to evaluate a model while modeling a continuous output variable?

A.UC-ROC
B. Accuracy
C. Logloss
D. Mean-Squared-Error

Mean-Squared-Error

Since linear regression gives output as continuous values, so in such case we use mean squared error metric to evaluate the model performance. Remaining options are use in case of a classification problem.

6. Which of the following is true about Residuals?

A) Lower is better
B) Higher is better
C) A or B depend on the situation
D) None of these

Lower is better

Residuals refer to the error values of the model. Therefore lower residuals are desired.

7. Overfitting is more likely when you have huge amount of data to train?

No,With a small training dataset, it’s easier to find a hypothesis to fit the training data exactly i.e. overfitting.

8. Which of the following statement is true about outliers in Linear regression?

A) Linear regression is sensitive to outliers
B) Linear regression is not sensitive to outliers
C) Can’t say
D) None of these

Linear regression is sensitive to outliers
The slope of the regression line will change due to outliers in most of the cases. So Linear Regression is sensitive to outliers.

9. What will happen when you fit degree 4 polynomial in linear regression?

A) There are high chances that degree 4 polynomial will over fit the data
B) There are high chances that degree 4 polynomial will under fit the data
C) Can’t say
D) None of these

There are high chances that degree 4 polynomial will over fit the data

Since is more degree 4 will be more complex(overfit the data) than the degree 3 model so it will again perfectly fit the data. In such case training error will be zero but test error may not be zero.

10. What will happen when you fit degree 2 polynomial in linear regression?

A) It is high chances that degree 2 polynomial will over fit the data
B) It is high chances that degree 2 polynomial will under fit the data
C) Can’t say
D) None of these

It is high chances that degree 2 polynomial will under fit the data

If a degree 3 polynomial fits the data perfectly, it’s highly likely that a simpler model(degree 2 polynomial) might under fit the data.

11.What are tree based classifiers?

Classifiers which form a tree with each attribute at one level b. Classifiers which perform series of condition checking with one attribute

12.What is gini index?

a. It is a type of index structure

b. It is a measure of purity

c. Both options except none

d. None of the options

It is a measure of purity

13.Tree/Rule based classification algorithms generate ... rule to perform the classification.

a. if-then.

b. while.

c. do while.

d. switch.

Ans:if-then.

14.Which of the following sentences are correct in reference to Information gain?

a. It is biased towards single-valued attributes

b. It is biased towards multi-valued attributes

c. ID3 makes use of information gain

d. The approact used by ID3 is greedy

Ans:It is biased towards multi-valued attributes , ID3 makes use of information gain ,The approact used by ID3 is greedy

15.Cost complexity pruning algorithm is used in?

a.CART

b. C4.5

c. ID3

d. All

Ans:CART

For the below questions answer as true / false

16. Multivariate split is where the partitioning of tuples is based on a combination of attributes rather than on a single attribute.

Ans: True

17. CART system cannot find multivariate splits.

Ans: False

18. Gain ratio tends to prefer unbalanced splits in which one partition is much smaller than the other.

Ans: True

19. The gini index is not biased towards multivalued attributed.

Ans: False

20. Gini index does not favour equal sized partitions.

Ans: False

21. When the number of classes is large Gini index is not a good choice.

Ans: True

22. Attribute selection measures are also known as splitting rules.

Ans: True

23.Which one of these is not a tree based learner?

a. CART

b. ID3

c. Bayesian classifier

d. Random Forest

Bayesian classifier

24. Which one of these is a tree based learner?

a. Rule based

b. Bayesian Belief Network

c. Bayesian classifier

d. Random Forest

Ans: d

25. What is the approach of basic algorithm for decision tree induction?

a. Greedy

b. Top Down

c. Procedural

d. Step by Step

Ans: a

26. Which of the following classifications would best suit the student performance classification systems?

a. If...then... analysis

b. Market-basket analysis

c. Regression analysis

d. Cluster analysis

Ans: a

27. How will you counter over-fitting in decision tree?

a. By pruning the longer rules

b. By creating new rules

c. Both By pruning the longer rules' and ' By creating new rules'

d. None of the options

Ans: a

28.Which of the following sentences are true?

a. In pre-pruning a tree is 'pruned' by halting its construction early.

b. A pruning set of class labelled tuples is used to estimate cost complexity.

c. The best pruned tree is the one that minimizes the number of encoding bits.

d. All of the above

Ans: d

29.Which of the following distance metric can not be used in k-NN?

A) Manhattan
B) Minkowski
C) Tanimoto
D) Jaccard
E) Mahalanobis
F) All can be used

Solution: F

All of these distance metric can be used as a distance metric for k-NN.

30.Which of the following option is true about k-NN algorithm?

A) It can be used for classification
B) It can be used for regression
C) It can be used in both classification and regression

Solution: C

We can also use k-NN for regression problems. In this case the prediction can be based on the mean or the median of the k-most similar instances.

31.Which of the following statement is true about k-NN algorithm?

1. k-NN performs much better if all of the data have the same scale
2. k-NN works well with a small number of input variables (p), but struggles when the number of inputs is very large

3. k-NN makes no assumptions about the functional form of the problem being solved

A) 1 and 2
B) 1 and 3
C) Only 1
D) All of the above

Solution: D

The above mentioned statements are assumptions of kNN algorithm

32. Which of the following machine learning algorithm can be used for imputing missing values of both categorical and continuous variables?

A) K-NN
B) Linear Regression
C) Logistic Regression

Solution: A

k-NN algorithm can be used for imputing missing value of both categorical and continuous variables.

33. Which of the following is true about Manhattan distance?

A) It can be used for continuous variables
B) It can be used for categorical variables
C) It can be used for categorical as well as continuous
D) None of these

Solution: A

Manhattan Distance is designed for calculating the distance between real valued features.

34. Which of the following distance measure do we use in case of categorical variables in k-NN?

1. **Hamming Distance**
2. **Euclidean Distance**
3. **Manhattan Distance**

A) 1
B) 2
C) 3
D) 1 and 2
E) 2 and 3
F) 1,2 and 3

Solution: A

Both Euclidean and Manhattan distances are used in case of continuous variables, whereas hamming distance is used in case of categorical variable.

35.Which of the following will be Euclidean Distance between the two data point A(1,3) and B(2,3)?

A) 1
B) 2
C) 4
D) 8

Solution: A

sqrt((1-2)^2 + (3-3)^2) = sqrt(1^2 + 0^2) = 1

36. Which of the following will be Manhattan Distance between the two data point A(1,3) and B(2,3)?

A) 1
B) 2
C) 4
D) 8

Solution: A sqrt(mod((1-2)) + mod((3-3))) = sqrt(1 + 0) = 1

37.Which of the following will be true about k in k-NN in terms of Bias?

A) When you increase the k the bias will be increases
B) When you decrease the k the bias will be increases
C) Can’t say
D) None of these

Solution: A - large K means simple model, simple model always consider as high bias

38.Which of the following will be true about k in k-NN in terms of variance?

A) When you increase the k the variance will increases
B) When you decrease the k the variance will increases
C) Can’t say
D) None of these

Solution: B Simple model will be consider as less variance model

39.Below are two statements given. Which of the following will be true both statements?

1. **k-NN is a memory-based approach is that the classifier immediately adapts as we collect new training data.**
2. **The computational complexity for classifying new samples grows linearly with the number of samples in the training dataset in the worst-case scenario.**

A) 1
B) 2
C) 1 and 2
D) None of these

Solution: C Both are true and self explanatory

40.In k-NN it is very likely to overfit due to the curse of dimensionality. Which of the following option would you consider to handle such problem?

1. **Dimensionality Reduction**
2. **Feature selection**

A) 1
B) 2
C) 1 and 2
D) None of these

Solution: C In such case you can use either dimensionality reduction algorithm or the feature selection algorithm

41 A company has build a kNN classifier that gets 100% accuracy on training data. When they deployed this model on client side it has been found that the model is not at all accurate. Which of the following thing might gone wrong?

Note: Model has successfully deployed and no technical issues are found at client side except the model performance

A) It is probably a overfitted model
B) It is probably a underfitted model
C) Can’t say
D) None of these

Solution: A In an overfitted module, it seems to be performing well on training data, but it is not generalized enough to give the same results on a new data.

42) You have given the following 2 statements, find which of these option is/are true in case of k-NN?

1. **In case of very large value of k, we may include points from other classes into the neighborhood.**
2. **In case of too small value of k the algorithm is very sensitive to noise**

A) 1
B) 2
C) 1 and 2
D) None of these

Solution: C Both the options are true and are self explanatory.

43.Which of the following statements is true for k-NN classifiers?

A) The classification accuracy is better with larger values of k
B) The decision boundary is smoother with smaller values of k
C) The decision boundary is linear
D) k-NN does not require an explicit training step

Solution: D

Option A: This is not always true. You have to ensure that the value of k is not too high or not too low.

Option B: This statement is not true. The decision boundary can be a bit jagged

Option C: Same as option B

Option D: This statement is true

44.True-False: It is possible to construct a 2-NN classifier by using the 1-NN classifier?

A) TRUE
B) FALSE

Solution: A You can implement a 2-NN classifier by ensembling 1-NN classifiers

45. In k-NN what will happen when you increase/decrease the value of k?

A) The boundary becomes smoother with increasing value of K
B) The boundary becomes smoother with decreasing value of K
C) Smoothness of boundary doesn't dependent on value of K
D) None of these

Solution: A The decision boundary would become smoother by increasing the value of K

46.Following are the two statements given for k-NN algorthm, which of the statement(s) is/are true?

1. **We can choose optimal value of k with the help of cross validation**
2. **Euclidean distance treats each feature as equally important**

A) 1
B) 2
C) 1 and 2
D) None of these

Solution: C Both the statements are true

47. Movie Recommendation systems are an example of:

1. **Classification**
2. **Clustering**
3. **Reinforcement Learning**
4. **Regression**

Options:

B. A. 2 Only

C. 1 and 2

D. 1 and 3

E. 2 and 3

F. 1, 2 and 3

H. 1, 2, 3 and 4

Solution: (E)

Generally, movie recommendation systems cluster the users in a finite number of similar groups based on their previous activities and profile. Then, at a fundamental level, people in the same cluster are made similar recommendations.

In some scenarios, this can also be approached as a classification problem for assigning the most appropriate movie class to the user of a specific group of users. Also, a movie recommendation system can be viewed as a reinforcement learning problem where it learns by its previous recommendations and improves the future recommendations.

48. Sentiment Analysis is an example of:

1. **Regression**
2. **Classification**
3. **Clustering**
4. **Reinforcement Learning**

Options:

A. 1 Only

B. 1 and 2

C. 1 and 3

D. 1, 2 and 3

E. 1, 2 and 4

F. 1, 2, 3 and 4

Solution: (E)

Sentiment analysis at the fundamental level is the task of classifying the sentiments represented in an image, text or speech into a set of defined sentiment classes like happy, sad, excited, positive, negative, etc. It can also be viewed as a regression problem for assigning a sentiment score of say 1 to 10 for a corresponding image, text or speech.

Another way of looking at sentiment analysis is to consider it using a reinforcement learning perspective where the algorithm constantly learns from the accuracy of past sentiment analysis performed to improve the future performance.

49.Can decision trees be used for performing clustering?

A. True

B. False

Solution: (A)

Decision trees can also be used to for clusters in the data but clustering often generates natural clusters and is not dependent on any objective function.

50.Which of the following is the most appropriate strategy for data cleaning before performing clustering analysis, given less than desirable number of data points:

1. **Capping and flouring of variables**
2. **Removal of outliers**

Options:

A. 1 only

B. 2 only

C. 1 and 2

D. None of the above

Solution: (A)

Removal of outliers is not recommended if the data points are few in number. In this scenario, capping and flouring of variables is the most appropriate strategy.

51.What is the minimum no. of variables/ features required to perform clustering?

A. 0

B. 1

C. 2

D. 3

Solution: (B)

At least a single variable is required to perform clustering analysis. Clustering analysis with a single variable can be visualized with the help of a histogram.

52. For two runs of K-Mean clustering is it expected to get same clustering results?

A. Yes

B. No

Solution: (B)

K-Means clustering algorithm instead converses on local minima which might also correspond to the global minima in some cases but not always. Therefore, it's advised to run the K-Means algorithm multiple times before drawing inferences about the clusters.

However, note that it's possible to receive same clustering results from K-means by setting the same seed value for each run. But that is done by simply making the algorithm choose the set of same random no. for each run.

53.Is it possible that Assignment of observations to clusters does not change between successive iterations in K-Means

A. Yes

B. No

C. Can't say

D. None of these

Solution: (A)

When the K-Means algorithm has reached the local or global minima, it will not alter the assignment of data points to clusters for two successive iterations.

54.Which of the following can act as possible termination conditions in K-Means?

1. **For a fixed number of iterations.**
2. **Assignment of observations to clusters does not change between iterations. Except for cases with a bad local minimum.**
3. **Centroids do not change between successive iterations.**
4. **Terminate when RSS falls below a threshold.**

Options:

A. 1, 3 and 4

B. 1, 2 and 3

C. 1, 2 and 4

D. All of the above

Solution: (D)

All four conditions can be used as possible termination condition in K-Means clustering:

1. This condition limits the runtime of the clustering algorithm, but in some cases the quality of the clustering will be poor because of an insufficient number of iterations.
2. Except for cases with a bad local minimum, this produces a good clustering, but runtimes may be unacceptably long.
3. This also ensures that the algorithm has converged at the minima.
4. Terminate when RSS falls below a threshold. This criterion ensures that the clustering is of a desired quality after termination. Practically, it’s a good practice to combine it with a bound on the number of iterations to guarantee termination.

55.Which of the following clustering algorithms suffers from the problem of convergence at local optima?

1. **K- Means clustering algorithm**
2. **Agglomerative clustering algorithm**
3. **Expectation-Maximization clustering algorithm**
4. **Diverse clustering algorithm**

Options:

A. 1 only

B. 2 and 3

C. 2 and 4

D. 1 and 3

E. 1,2 and 4

F. All of the above

Solution: (D)

Out of the options given, only K-Means clustering algorithm and EM clustering algorithm has the drawback of converging at local minima.

56. Which of the following algorithm is most sensitive to outliers?

A. K-means clustering algorithm

B. K-medians clustering algorithm

C. K-modes clustering algorithm

D. K-medoids clustering algorithm

Solution: (A)

Out of all the options, K-Means clustering algorithm is most sensitive to outliers as it uses the mean of cluster data points to find the cluster center.

57.How can Clustering (Unsupervised Learning) be used to improve the accuracy of Linear Regression model (Supervised Learning):

1. **Creating different models for different cluster groups.**
2. **Creating an input feature for cluster ids as an ordinal variable.**
3. **Creating an input feature for cluster centroids as a continuous variable.**
4. **Creating an input feature for cluster size as a continuous variable.**

Options:

A. 1 only

B. 1 and 2

C. 1 and 4

D. 3 only

E. 2 and 4

F. All of the above

Solution: (F)

Creating an input feature for cluster ids as ordinal variable or creating an input feature for cluster centroids as a continuous variable might not convey any relevant information to the regression model for multidimensional data. But for clustering in a single dimension, all of the given methods are expected to convey meaningful information to the regression model. For example, to cluster people in two groups based on their hair length, storing clustering ID as ordinal variable and cluster centroids as continuous variables will convey meaningful information.

58.What could be the possible reason(s) for producing two different dendrograms using agglomerative clustering algorithm for the same dataset?

A. Proximity function used

B. of data points used

C. of variables used

D. B and c only

E. All of the above

Solution: (E) Change in either of Proximity function, no. of data points or no. of variables will lead to different clustering results and hence different dendrograms.

59.In which of the following cases will K-Means clustering fail to give good results?

1. **Data points with outliers**
2. **Data points with different densities**
3. **Data points with round shapes**
4. **Data points with non-convex shapes**

Options:

A. 1 and 2

B. 2 and 3

C. 2 and 4

D. 1, 2 and 4

E. 1, 2, 3 and 4

Solution: (D)

K-Means clustering algorithm fails to give good results when the data contains outliers, the density spread of data points across the data space is different and the data points follow non-convex shapes.

60.Which of the following metrics, do we have for finding dissimilarity between two clusters in hierarchical clustering?

1. **Single-link**
2. **Complete-link**
3. **Average-link**

Options:

A. 1 and 2

B. 1 and 3

C. 2 and 3

D. 1, 2 and 3

Solution: (D)

All of the three methods i.e. single link, complete link and average link can be used for finding dissimilarity between two clusters in hierarchical clustering.

61.Which of the following are true?

1. **Clustering analysis is negatively affected by multicollinearity of features**
2. **Clustering analysis is negatively affected by heteroscedasticity**

Options:

A. 1 only

B. 2 only

C. 1 and 2

D. None of them

Solution: (A)

Clustering analysis is not negatively affected by heteroscedasticity but the results are negatively impacted by multicollinearity of features/ variables used in clustering as the correlated feature/ variable will carry extra weight on the distance calculation than desired.

62.Which of the following is/are valid iterative strategy for treating missing values before clustering analysis?

A. Imputation with mean

B. Nearest Neighbor assignment

C. Imputation with Expectation Maximization algorithm

D. All of the above

Solution: (C)

All of the mentioned techniques are valid for treating missing values before clustering analysis but only imputation with EM algorithm is iterative in its functioning.

63. K-Mean algorithm has some limitations. One of the limitation it has is, it makes hard assignments(A point either completely belongs to a cluster or not belongs at all) of points to clusters.

Note: Soft assignment can be consider as the probability of being assigned to each cluster: say K = 3 and for some point xn, p1 = 0.7, p2 = 0.2, p3 = 0.1)

Which of the following algorithm(s) allows soft assignments?

1. **Gaussian mixture models**
2. **Fuzzy K-means**

Options:

A. 1 only

B. 2 only

C. 1 and 2

D. None of these

Solution: (C)

Both, Gaussian mixture models and Fuzzy K-means allows soft assignments.

64. Assume, you want to cluster 7 observations into 3 clusters using K-Means clustering algorithm. After first iteration clusters, C1, C2, C3 has following observations:

C1: {(2,2), (4,4), (6,6)}

C2: {(0,4), (4,0)}

C3: {(5,5), (9,9)}

What will be the Manhattan distance for observation (9, 9) from cluster centroid C1. In second iteration.

A. 10

B. 5*sqrt(2)

C. 13*sqrt(2)

D. None of these

Solution: (A)

Manhattan distance between centroid C1 i.e. (4, 4) and (9, 9) = (9-4) + (9-4) = 10

65. If two variables V1 and V2, are used for clustering. Which of the following are true for K means clustering with k =3?

1. **If V1 and V2 has a correlation of 1, the cluster centroids will be in a straight line**
2. **If V1 and V2 has a correlation of 0, the cluster centroids will be in straight line**

Options:

A. 1 only

B. 2 only

C. 1 and 2

D. None of the above

Solution: (A)

If the correlation between the variables V1 and V2 is 1, then all the data points will be in a straight line. Hence, all the three cluster centroids will form a straight line as well.

66. Feature scaling is an important step before applying K-Mean algorithm. What is reason behind this?

A. In distance calculation it will give the same weights for all features

B. You always get the same clusters. If you use or don’t use feature scaling

C. In Manhattan distance it is an important step but in Euclidian it is not

D. None of these

Solution; (A)

Feature scaling ensures that all the features get same weight in the clustering analysis. Consider a scenario of clustering people based on their weights (in KG) with range 55-110 and height (in inches) with range 5.6 to 6.4. In this case, the clusters produced without scaling can be very misleading as the range of weight is much higher than that of height. Therefore, its necessary to bring them to same scale so that they have equal weightage on the clustering result.

67. Which of the following method is used for finding optimal of cluster in K-Mean algorithm?

A. Elbow method

B. Manhattan method

C. Ecludian mehthod

D. All of the above

E. None of these

Solution: (A)

Out of the given options, only elbow method is used for finding the optimal number of clusters. The elbow method looks at the percentage of variance explained as a function of the number of clusters: One should choose a number of clusters so that adding another cluster doesn't give much better modeling of the data.

68. What is true about K-Mean Clustering?

1. **K-means is extremely sensitive to cluster center initializations**
2. **Bad initialization can lead to Poor convergence speed**
3. **Bad initialization can lead to bad overall clustering**

Options:

A. 1 and 3

B. 1 and 2

C. 2 and 3

D. 1, 2 and 3

Solution: (D)

All three of the given statements are true. K-means is extremely sensitive to cluster center initialization. Also, bad initialization can lead to Poor convergence speed as well as bad overall clustering.

69. Which of the following can be applied to get good results for K-means algorithm corresponding to global minima?

1. **Try to run algorithm for different centroid initialization**
2. **Adjust number of iterations**
3. **Find out the optimal number of clusters**

Options:

A. 2 and 3

B. 1 and 3

C. 1 and 2

D. All of above

Solution: (D)

All of these are standard practices that are used in order to obtain good clustering results.

70.Which of the following sequences is correct for a K-Means algorithm using Forgy method of initialization?

1. **Specify the number of clusters**
2. **Assign cluster centroids randomly**
3. **Assign each data point to the nearest cluster centroid**
4. **Re-assign each point to nearest cluster centroids**
5. **Re-compute cluster centroids**

Options:

A. 1, 2, 3, 5, 4

B. 1, 3, 2, 4, 5

C. 2, 1, 3, 4, 5

D. None of these

Solution: (A)

The methods used for initialization in K means are Forgy and Random Partition. The Forgy method randomly chooses k observations from the data set and uses these as the initial means. The Random Partition method first randomly assigns a cluster to each observation and then proceeds to the update step, thus computing the initial mean to be the centroid of the cluster's randomly assigned points.

71. If you are using Multinomial mixture models with the expectation-maximization algorithm for clustering a set of data points into two clusters, which of the assumptions are important:

A. All the data points follow two Gaussian distribution

B. All the data points follow n Gaussian distribution (n >2)

C. All the data points follow two multinomial distribution

D. All the data points follow n multinomial distribution (n >2)

Solution: (C)

In EM algorithm for clustering its essential to choose the same no. of clusters to classify the data points into as the no. of different distributions they are expected to be generated from and also the distributions must be of the same type.

72. Which of the following is/are not true about Centroid based K-Means clustering algorithm and Distribution based expectation-maximization clustering algorithm:

1. **Both starts with random initializations**
2. **Both are iterative algorithms**
3. **Both have strong assumptions that the data points must fulfill**
4. **Both are sensitive to outliers**
5. **Expectation maximization algorithm is a special case of K-Means**
6. **Both requires prior knowledge of the no. of desired clusters**
7. **The results produced by both are non-reproducible.**

Options:

A. 1 only

B. 5 only

C. 1 and 3

D. 6 and 7

E. 4, 6 and 7

F. None of the above

Solution: (B)

All of the above statements are true except the 5th as instead K-Means is a special case of EM algorithm in which only the centroids of the cluster distributions are calculated at each iteration.

Information and Cyber Security

1. **What is the size of the key in the SDES algorithm?**
   a)24bits
   b)16bits
   c)20bits
   d) 10 bits

   Answer:d
   Explanation: The size of the key in the SDES algorithm is 10 bits.

2. **Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K1?**
   a)10100100
   b)01011011
   c)01101000
   d) 10100111

   Answer:a
   Explanation: The permuted key P10 = 1000001100. Input to P8: 0000111000 and K1 is 10100100.

3. **Assume input 10-bit key, K: 1010000010 for the SDES algorithm. What is K2?**
   a)10100111
   b)01000011
   c)00100100
   d) 01011010

Answer:b
Explanation: Input to P8: 0010000011 and K2 is 01000011.

4. **The Ciphertext for the Plaintext 01110010, given that the keys K1 is 10100100 and K2 is 01000011 is**
a)01110111
b)10010110
c)01010110
d) 01000101

Answer:a
Explanation: Perform the SDES algorithm and compute the cipher text.

5. **DES follows**
a) Hash Algorithm
b) Caesars Cipher
c) Feistel Cipher Structure
d) SP Networks

Answer: c
Explanation: DES follows Feistel Cipher Structure.

6. **The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key**
a) 12
b) 18
c) 9
d) 16

Answer: d
Explanation: The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

7. **The DES algorithm has a key length of**
a) 128 Bits
b) 32 Bits
c) 64 Bits
d) 16 Bits

Answer: c
Explanation: DES encrypts blocks of 64 bits using a 64 bit key.

8. **In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.**

a) True
b) False

Answer: b
Explanation: 56 bits are used, the rest 8 bits are parity bits.

9. **In the DES algorithm the round key is __________ bit and the Round Input is ____________bits.**
a) 48, 32
b) 64,32
c) 56, 24
d) 32, 32

Answer: a
Explanation: The round key is 48 bits. The input is 32 bits.

10. **In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via ____________**
a) Scaling of the existing bits
b) Duplication of the existing bits
c) Addition of zeros
d) Addition of ones

Answer: a
Explanation: The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

11. **The Initial Permutation table/matrix is of size**
a) 16×8
b) 12×8
c) 8×8
d) 4×8

Answer: c
Explanation: There are 64 bits to permute and this requires a 8×8 matrix.

12. **The number of unique substitution boxes in DES after the 48 bit XOR operation are**
a) 8
b) 4
c) 6
d) 12

Answer: a
Explanation: The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

13. **In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.**
a) True
b) False

Answer: b
Explanation: Every 8th bit is ignored to shorten the key length.

14. **During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.**
a) True
b) False

Answer: a
Explanation: IP-1 is the first step and the last step is IP during decryption.

15. **A preferable cryptographic algorithm should have a good avalanche effect**.
a) True
b) False

Answer: a
Explanation: Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher text. This is referred to as the avalanche effect.

16. **The number of tests required to break the DES algorithm are**
a) 2.8×10^{14}
b) 4.2×10^{9}
c) 1.84×10^{19}
d) 7.2×10^{16}

Answer: d
Explanation: There are 2^{56} keys $=7.2\times10^{16}$.

17. **The number of tests required to break the Double DES algorithm are**
a) 2112
b) 2111
c) 2128
d) 2119

Answer: b
Explanation: For Double DES key is 2112 bits, should require 2111 tests to break.

18. **How many keys does the Triple DES algorithm use?**
a) 2
b) 3

c) 2 or 3
d) 3 or 4

Answer: c
Explanation: For Triple DES we can either have 2 or 3 keys.
Using two keys: c = Ek1(Dk2(Ek1(m)))
Using three keys: c = Ek3(Ek2(Ek1(m))).

19. **In triple DES, the key size is ___ and meet in the middle attack takes ___ tests to break the key.**
a) 2192 ,2112
b) 2184,2111
c) 2168,2111
d) 2168,2112

Answer: d
Explanation: The key size is 2168 and meet in the middle attack takes 2112 tests to break.

20. **Using Linear Crypt-analysis, the minimum computations required to decipher the DES algorithm is**
a) 2^{48}
b) 2^{43}
c) 2^{56}
d) 2^{64}

Answer: b
Explanation: Linear Crypt-analysis requires only 2^{43} computations to decipher the DES algorithm.

21. **Which is the key exchange algorithm used in CipherSuite parameter?**
a) RSA
b) Fixed Diffie-Hellman
c) Ephemeral Diffie-Hellman
d) Any of the mentioned

Answer: d
Explanation: We can use either of the following for the CipherSuite key exchange-
i) RSA
ii) Fixed Diffie-Hellman
iii) Ephemeral Diffie-Hellman
iv) Anonymous Diffie-Hellman
v) Fortezza.

22. **The certificate message is required for any agreed-on key exchange method except _______________**

a) Ephemeral Diffie-Hellman
b) Anonymous Diffie-Hellman
c) Fixed Diffie-Hellman
d) RSA

Answer: b
Explanation: The certificate message is required for any agreed-on key exchange method except Anonymous Diffie-Hellman.

23. **The RSA signature uses which hash algorithm?**

a) MD5
b) SHA-1
c) MD5 and SHA-1
d) None of the mentioned.

Answer: c
Explanation: The MD5 and SHA-1 hash is concatenated together and the then encrypted with the server’s private key.

24. **What is the size of the RSA signature hash after the MD5 and SHA-1 processing?**

a) 42 bytes
b) 32 bytes
c) 36 bytes
d) 48 bytes

Answer: c
Explanation: The size is 36 bytes after MD5 and SHA-1 processing.

25. **For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where PT message=88 and thus find the CT.**

a) 23
b) 64
c) 11
d) 54

Answer: c
Explanation: n = pq = 11 × 19 = 187.
$C=M^e \bmod n$; $C=88^7 \bmod 187$; $C = 11 \bmod 187$