Tutorial

Day-4

Solve the following problems:

1. Define RSA digital signature and compare it to the RSA scheme
2. Using RSA scheme, let p=809, q=751 and d=23, calculate the public key e, then

   a. Sign and verify a message with $m_1 = 100$, call the signature s_1

   b. Show that if $M = m_1 * m_2 = 5000$, then $s = s_1 * s_2$

3. Why can't deffie hellman be used for signing?

4. Identify which of the following statements are propositions-

1.France is a country.

2. 2020 will be a leap year.

3. Sun rises in the west.

4. P(x) : x + 6 = 7

5. P(5) : 5 + 6 = 2

6. Apples are oranges.

7. Grapes are black.

8. Two and two makes 4.

9. $x > 10$

10. Open the door.

11. Are you tired?

12. What a bright sunny day!

13. Mumbai is in India.

14. I always tell truth.

15. I always tell lie.

16. Do not go there.

17. This sentence is true.

18. This sentence is false.

19. It will rain tomorrow.

20. Fan is rotating.

5. Let's consider a propositional language, where

A ="Angelo comes to the party" B ="Bruno comes to the party" C ="Carlo comes to the party" D ="Davide comes to the party".

Formalize the following sentences:

i. "If Davide comes to the party then Bruno and Carlo come too"

ii. "Carlo comes to the party only if Angelo and Bruno do not come"

iii. "Davide comes to the party if and only if Carlo comes and Angelo doesn't come"

iv. "If Davide comes to the party, then, if Carlo doesn't come then Angelo comes"

v. "Carlo comes to the party provided that Davide doesn't come, but, if Davide comes, then Bruno doesn't come"

vi. "A necessary condition for Angelo coming to the party, is that, if Bruno and Carlo aren't coming, Davide comes"

vii. "Angelo, Bruno and Carlo come to the party if and only if Davide doesn't come, but, if neither Angelo nor Bruno come, then Davide comes only if Carlo comes"

6. Let g_k , r_k, and o_k be the propositions

g_k : traffic light is green at instant r_k : traffic light is red at instant o_k : traffic light is orange at instant

Write these propositions using g_k , r_k, and o_k and logical connectives (including negations).

Expresses the following facts:

i. the traffic light is either green, or red or orange;

ii. 2. the traffic light switches from green to orange, from orange to red, and from red to green;

iii. 3. it can keep the same color over at most 3 successive states.

7. We are given the following statement: If today is Sunday, then the weather is sunny.

(i) Write the inverse and converse of this statement.
(ii) Identify which of these statements you have made is not logical and explain why.

8. (i) Write down the contrapositive statement for

"If you are human, then you have DNA."

(ii) Write down the two if-then statements for

"A polygon is a quadrilateral if and only if the polygon has 4 sides."

9. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a series of logical equivalences.

10. Check wheather the compound preposition given below is a tautology, contradiction or a contingency

$$\neg(p \wedge q)) \leftrightarrow \neg p \vee \neg q$$

11.The statement $\neg p \rightarrow \neg q$ is logically equivalent to

i. $p \rightarrow q$

ii. $q \rightarrow p$

iii. $\neg q \vee p$

iv. $\neg p \vee q$

12. Which of the following is not a tautology:

i. $((a \rightarrow b) \wedge (b \rightarrow c)) \rightarrow (a \rightarrow c)$

ii. $(a \leftrightarrow c) \rightarrow (\neg b \rightarrow (a \wedge c))$

iii. $(a \wedge b \wedge c) \rightarrow (c \vee a)$

iv. $a \rightarrow (b \rightarrow a)$