הטכניון - מכון טכנולוגי לישראל
הפקולת לדינמי המחשב

מכון בקריפטולוגיה מופרדין - 2365056

سفנסטר מח' וQUIRE
מועלה לב, 2010

ena: מعناية: יניב ברקלי
מурсל: ידית אלכסנדרוביץ

מש' המכתב: שלוש שעות.
בצבת 4 שאולות, עד לע כבל.

מומר טלשטוש בכל תום זה או אחר (בפורמט אסרו בלוק סלולרי). (בפורמט אסרו בלוק סלולרי)
תקד ה-10 חקוקים והאשwrongת לקיראת כל השאלות והבתים.
עיגי חדשות וברורות לכל האפשר. נמק את כל השוניים.
וקצהマー.IPעיגיяемעדמיים במחבת לכל שאלות ועל שידי השאלות.
כותר בずっと מפורש ומקויה בצבע ברוור. תשובות לא ברורות לא נباشرיה.

בהצלחה!
1. An independent set (IS) of a graph $G = (V, E)$ is a subset $U \subseteq V$ such that $(u,v) \notin E$ for all $u,v \in U$. The graph $G$ is an independent set.

2. Given a graph $G = (V,E)$, the IS problem is to find a maximum independent set of $G$.

3. The maximum independent set problem is NP-complete.

4. The maximum independent set problem is a NP-complete problem.

5. The maximum independent set problem is a NP-complete problem.

6. The maximum independent set problem is a NP-complete problem.

7. The maximum independent set problem is a NP-complete problem.

8. The maximum independent set problem is a NP-complete problem.

9. The maximum independent set problem is a NP-complete problem.

10. The maximum independent set problem is a NP-complete problem.

11. The maximum independent set problem is a NP-complete problem.

12. The maximum independent set problem is a NP-complete problem.

13. The maximum independent set problem is a NP-complete problem.

14. The maximum independent set problem is a NP-complete problem.

15. The maximum independent set problem is a NP-complete problem.

16. The maximum independent set problem is a NP-complete problem.

17. The maximum independent set problem is a NP-complete problem.

18. The maximum independent set problem is a NP-complete problem.

19. The maximum independent set problem is a NP-complete problem.

20. The maximum independent set problem is a NP-complete problem.

21. The maximum independent set problem is a NP-complete problem.

22. The maximum independent set problem is a NP-complete problem.

23. The maximum independent set problem is a NP-complete problem.

24. The maximum independent set problem is a NP-complete problem.

25. The maximum independent set problem is a NP-complete problem.

26. The maximum independent set problem is a NP-complete problem.

27. The maximum independent set problem is a NP-complete problem.

28. The maximum independent set problem is a NP-complete problem.

29. The maximum independent set problem is a NP-complete problem.

30. The maximum independent set problem is a NP-complete problem.

31. The maximum independent set problem is a NP-complete problem.

32. The maximum independent set problem is a NP-complete problem.

33. The maximum independent set problem is a NP-complete problem.

34. The maximum independent set problem is a NP-complete problem.

35. The maximum independent set problem is a NP-complete problem.

36. The maximum independent set problem is a NP-complete problem.

37. The maximum independent set problem is a NP-complete problem.

38. The maximum independent set problem is a NP-complete problem.

39. The maximum independent set problem is a NP-complete problem.

40. The maximum independent set problem is a NP-complete problem.

41. The maximum independent set problem is a NP-complete problem.

42. The maximum independent set problem is a NP-complete problem.

43. The maximum independent set problem is a NP-complete problem.

44. The maximum independent set problem is a NP-complete problem.

45. The maximum independent set problem is a NP-complete problem.

46. The maximum independent set problem is a NP-complete problem.

47. The maximum independent set problem is a NP-complete problem.

48. The maximum independent set problem is a NP-complete problem.

49. The maximum independent set problem is a NP-complete problem.

50. The maximum independent set problem is a NP-complete problem.

51. The maximum independent set problem is a NP-complete problem.

52. The maximum independent set problem is a NP-complete problem.

53. The maximum independent set problem is a NP-complete problem.

54. The maximum independent set problem is a NP-complete problem.

55. The maximum independent set problem is a NP-complete problem.

56. The maximum independent set problem is a NP-complete problem.

57. The maximum independent set problem is a NP-complete problem.

58. The maximum independent set problem is a NP-complete problem.

59. The maximum independent set problem is a NP-complete problem.

60. The maximum independent set problem is a NP-complete problem.

61. The maximum independent set problem is a NP-complete problem.

62. The maximum independent set problem is a NP-complete problem.

63. The maximum independent set problem is a NP-complete problem.

64. The maximum independent set problem is a NP-complete problem.

65. The maximum independent set problem is a NP-complete problem.

66. The maximum independent set problem is a NP-complete problem.

67. The maximum independent set problem is a NP-complete problem.

68. The maximum independent set problem is a NP-complete problem.

69. The maximum independent set problem is a NP-complete problem.

70. The maximum independent set problem is a NP-complete problem.

71. The maximum independent set problem is a NP-complete problem.

72. The maximum independent set problem is a NP-complete problem.

73. The maximum independent set problem is a NP-complete problem.

74. The maximum independent set problem is a NP-complete problem.

75. The maximum independent set problem is a NP-complete problem.

76. The maximum independent set problem is a NP-complete problem.

77. The maximum independent set problem is a NP-complete problem.

78. The maximum independent set problem is a NP-complete problem.

79. The maximum independent set problem is a NP-complete problem.

80. The maximum independent set problem is a NP-complete problem.

81. The maximum independent set problem is a NP-complete problem.

82. The maximum independent set problem is a NP-complete problem.

83. The maximum independent set problem is a NP-complete problem.

84. The maximum independent set problem is a NP-complete problem.

85. The maximum independent set problem is a NP-complete problem.

86. The maximum independent set problem is a NP-complete problem.

87. The maximum independent set problem is a NP-complete problem.

88. The maximum independent set problem is a NP-complete problem.

89. The maximum independent set problem is a NP-complete problem.

90. The maximum independent set problem is a NP-complete problem.

91. The maximum independent set problem is a NP-complete problem.

92. The maximum independent set problem is a NP-complete problem.

93. The maximum independent set problem is a NP-complete problem.

94. The maximum independent set problem is a NP-complete problem.

95. The maximum independent set problem is a NP-complete problem.

96. The maximum independent set problem is a NP-complete problem.

97. The maximum independent set problem is a NP-complete problem.

98. The maximum independent set problem is a NP-complete problem.

99. The maximum independent set problem is a NP-complete problem.

100. The maximum independent set problem is a NP-complete problem.
 hvor $h_0 = IV \cdot h_i$.

Davies-Meyer (DM) SHA-1 generates a fixed-length output $h_i$:

$$h_i = E_M(h_{i-1}) + h_0$$

where $E_M$ is the compression function and $h_0$ is the initial vector. The output is:

$$h_i = E_M(h_{i-1}) + h_0$$

for $i = 1$ to $n$. The final output is $h_n$. This process ensures that the output is secure against collision attacks.

The diagram shows the process of generating the hash value $h_i$. The message is divided into blocks, and each block is processed using the compression function to generate the next hash value. The final output is the concatenation of the individual hash values.

The text also mentions the use of Davies-Meyer to generate a secure hash value. The initial vector $h_0$ is chosen to be a constant value, and the compression function $E_M$ is used to generate the next hash value. The final output is the concatenation of the individual hash values.