Zagadnienia do egzaminu z przedmiotu „Kodowanie, Kompresja, Kryptografia”

1. Zdefiniuj entropię H(X) zmiennej losowej X i omów jej podstawowe własności.
2. Co to jest entropia łączna H(X,Y) i jakie są jej własności?
3. Zdefiniuj entropię warunkową H(X|Y) i podaj jej własności.
4. Sformułuj nierówność Krafta. Wyjaśnij jak można ją uzasadnić.
5. Co to jest kod bezprefiksowy?
6. Co to jest kod Shannona-Fano?
7. Podaj twierdzenie Shannona o kodowaniu dla kanałów bez szumu.
8. Podaj przykłady kodu optymalnego i nieoptymalnego spełniających nierówność w tw. Shannona.
9. Opisz kod Huffmana i metodę jego konstrukcji.
10. Jak można poprawić stopień kompresji w stosunku do podstawowej metody kodowania Huffmana?
11. Zdefiniuj stacjonarny bezpamięciowy kanał informacyjny.
12. Podaj przykład kanału symetrycznego i opisz jego postać macierzową.
13. Co można powiedzieć o entropiach zmiennych losowych X i Y, jeśli $Y = \Phi(X)$ dla pewnego kanału informacyjnego Φ?
14. Zdefiniuj informację wzajemną I(X,Y).
15. Co to jest pojemność informacyjna kanału?
16. Jaka jest pojemność informacyjna binarnego kanału symetrycznego?
17. Podaj nierówność Fano i jej interpretację
18. Co to jest tempo transmisji (binarnej) przez kanał informacyjny?
19. W jaki sposób pojemność kanału wpływa na tempo transmisji?
20. Podaj twierdzenie Shannona o kodowaniu dla kanałów z szumem.
21. Co to jest odległość Hamminga i jaki jest jej związek z konstrukcją samokorygujących kodów?
22. Opisz kod Hamminga (7,4).
23. Ile bitów mniej więcej musiałby mieć kod typu Hamminga korygujący 2 błędy, jeśli chcemy zakodować w nim 265 znaków?
24. Ile mniej więcej bitów można przeznaczyć na kodowanie użytkowej informacji w 64-bitowym kodzie korygującym max do 3 błędów?
25. Kody linowe — definicja i przykład.
26. Postać macierzy kodowej i macierzy syndromu dla kodu liniowego.
27. Omówić schemat dekodowania z korektą dla kodu liniowego.
28. Kody cykliczne — definicja i przykład.
29. Postać ogólna generatora cyklicznego kodu liniowego w F_2^N
30. Jak znaleźć macierz kodową i macierz syndromu dla kodu cyklicznego w F_2^N ?
31. Jak sensownie wyznaczyć cykliczny kod 17-bitowy?
32. Co to są kody BCH? Czym wyróżniają się wśród kodów cyklicznych?
33. Opisz metodę korekty błędów dla kodów BCH.
34. Co to jest szyfr Vigenère’a?
35. Omów 3 poziomy bezpieczeństwa kodów kryptograficznych.
36. Na czym polegają metody statystycznej analizy frekwencyjnej przy łamaniu szyfrów?
37. Co to jest wieloznaczność kodu kryptograficznego?
38. Opisz kod o doskonałej prywatności.
39. Co to jest jednoznaczność dla kodu kryptograficznego?
40. Na czym polega schemat kryptografii z publicznym kluczem?
41. Opisz schemat podpisu elektronicznego
42. Opisz algorytm kryptograficzny RSA.
43. Na czym polega bezpieczeństwo metody RSA?
44. Opisz kod Rabina.
45. Co to jest dyskretny logarytm? Jaka jest złożoność wyznaczania go?
46. Opisz protokół Diffiego-Hellmana wymiany tajnego klucza.
47. Opisz kod Shamira.
48. Opisz kod ElGamala.