Zestaw pytań do egzaminu: Ochrona Danych

1. Podstawowe zadania (aspekty) ochrony danych. Różne metody ochrony.
2. Definicja kryptografii oraz kryptoanalizy.
3. Podstawowe techniki kryptoanalizy. Metody łamania szyfrów.
4. Definicja systemu kryptograficznego: algorytm kryptograficzny, klucz kryptograficzny.
5. Zasada działania i zastosowanie algorytmów kryptografii symetrycznej.
6. Zasada działania i zastosowanie algorytmów kryptografii asymetrycznej (z kluczem publicznym).
7. Definicja systemu algebraicznego – grupa.
8. Definicja systemu algebraicznego – ciało.
9. Definicja systemu algebraicznego – pierścień.
10. Podstawowe własności kongruencji i arytmetyki modularnej.
11. Stosując zasady arytmetyki modularnej obliczyć $y^z \mod q$ (y,z – podane), np. $2^{16} \mod 17$.
12. Twierdzenie Fermata o kongruencjach. Podać przykład potwierdzający prawdziwość.
13. Definicja funkcji Eulera. Wyznaczyć wartość funkcji dla podanego n.
14. Twierdzenie Eulera o kongruencjach. Podać przykład potwierdzający prawdziwość.
15. Ciała skończone (Galois), ciała proste – definicje przykłady.
16. Wyznaczyć tabelki dodawania i mnożenia w ciele prostym GF(p) dla podanego p.
17. Wyznaczyć elementy przeciwne i odwrotne w ciele prostym GF(p) dla podanego p.
18. Definicja rzędu multyplikatywnego elementu ciała. Własności elementów pierwotnych.
19. Definicja wielomianu nad ciałem skończonym GF(p). Wielomian unormowany. Zapis wielomianu w postaci ciągu współczynników.
20. Zastosowanie wielomianów do generowania sekwencji okresowych nad ciałami skończonymi. Dany jest wielomian f(x) = ... o współczynnikach z ciała GF(p). Wyznaczyć sekwencję okresową stowarzyszoną z wielomianem f(x). Podać okres sekwencji. Na podstawie długości okresu sekwencji określić czy wielomian f(x) jest wielomianem pierwotnym.
21. Schemat kanału transmisyjnego z systemem korekcji błędów.
22. Rodzaje zakłóceń oraz błędów występujących w kanałach transmisji danych.
23. Definicja detekcyjno/korekcyjnego kodu blokowego o parametrach (n,k), kodu liniowego, kodu cyklicznego. Struktury algebraiczne wykorzystywane do konstrukcji kodów.
24. Definicja odległości Hamminga oraz minimalnej odległości Hamminga między dwoma wektorami kodu liniowego. Definicja wagi Hamminga wektora kodowego. Definicja zdolności detekcyjnej kodu oraz zdolności korekcyjnej.
25. Zasada działania kodu blokowego (n,k) utworzonego w oparciu o wielomian generujący g(x).
26. Metoda obliczania kodu cyklicznego dualnego (n,n-k) do kodu cyklicznego (n,k).
27. Definicja cyklicznego kodu Hamminga.
28. Dla kodu cyklicznego o danych (n,k) oraz wielomianie generującym g(x) = ... zrealizować kolejne kroki kodowania wektora wiadomości m(x) = ... Podać postać wektora kodowego c(x) dla podanego kodu.
29. Dany jest wektor z błędem cb(x) = ... kodu cyklicznego o parametrach (n,k), wielomianie generującym g(x) = ... oraz zdolności korekcyjnej t = ... Zrealizować kolejne kroki ogólnej procedury dekodowania. Podać postać wektora wiadomości m(x).
30. Systemy kryptograficzne symetryczne: struktura, zasada działania, metody zapewniania poufności i autentyczności (integralności).
31. Systemy kryptograficzne asymetryczne: struktura, zasada działania, metody zapewniania poufności i autentyczności (integralności).
32. Proste szyfry podstawieniowe, np. szyfr Cezara, szyfr iloczynowy.
33. Szyfry podstawieniowe homofoniczne.
34. Szyfry podstawieniowe wieloalfabetowe, np. szyfr Vigenere'a, Vernama.
35. Szyfry podstawieniowe poligramowe – szyfr Playfaira.
36. Szyfry przestawieniowe (permutacyjne) oparte o figury geometryczne.
37. Standard szyfrowania z kluczem tajnym DES – zasada działania.
38. Standard szyfrowania z kluczem publicznym RSA – zasada działania.