Programování a vývoj aplikací

1. Algoritmizace, Césarova šifra. Třída Program a význam statické metody Main() v C#. Numerické literály.
2. Konvence, klíčová slova, datové a výčtové typy, proměnná, konstanta, přetypování a konverze datových typů. Referenční a hodnotové datové typy. Třídění.
3. Druhy operátorů, snižování a zvyšování hodnoty proměnných, složené přiřazení. Vigenèrova šifra.
4. Řízení toku programu, definice prvočísla. Algoritmus pro určení prvočísla.
5. Náhodná čísla a náhodná čísla bez opakování, kryptografická kvalita náhodných čísel.
Metoda Monte Carlo.
6. Jednorozměrné, dvourozměrné pole, Eratostenovo síto. Využití jednorozměrných a vícerozměrných polí.
7. Kolekce (List, Dictionary), frekvenční analýza a její význam pro dešifrování
8. Správa chyb a výjimek, přetečení, hierarchie výjimek, vyhazování výjimek, použití v metodách. Nejběžnější používané výjimky.
9. Datum a čas, šifrování operací XOR a opakovaným klíčem, kvalita šifrování
10. Řetězcové funkce, specifika typu string. Operace v zásobníku a na haldě.
11. Regulární výrazy, použití pro validaci polí a pro vyhledávání informací v rozsáhlých nestrukturovaných datech
12. Práce s textovými soubory, zpracování velkých textových souborů
13. Metody (předávání argumentů odkazem a hodnotou), rozsah platnosti proměnných v metodách. Specifikátory dostupnosti.
14. Třídy, konstruktor, dědičnost, implementace interface. Polymorfismus. Vlastnosti a jejich použití.
15. Abstraktní třídy, interface, implementace interface, porovnání abstraktní třídy a interface. Operátor IS a AS
16. Delegát, multicasting. Události a jejich použití
17. Symetrické šifrování, jeho výhody a nevýhody. Použití kryptovacích knihoven.
18. Asymetrické šifrování, princip předávání klíčů, jeho výhody a nevýhody. Použití kryptovacích knihoven
19. Smysl autentikace, hashování, použití hashování při autentikaci. Použití kryptovacích knihoven.
20. Steganografie a ukrývání informací. Příklady užití. Ukládání citlivých informací.