Karta pracy — „Szyfrowanie i sortowanie”

Imię i nazwisko: _____ klasa_____

Data: _____

Instrukcja dla ucznia

- Pracuj samodzielnie — staraj się wyjaśniać własnymi słowami.
- Przy zadaniach praktycznych dokładnie pokaż kroki (np. zmiany po każdym kroku).
- W części analitycznej argumentuj swoje odpowiedzi.
- Sprawdź dwukrotnie, czy w zadaniach szyfrowania/odszyfrowania nie popełniłaś/popełniłeś błędu w przesunięciu lub kolejności.

Grupa 1: Pytania teoretyczne

1. Zdefiniuj pojęcie **szyfr**.
2. Co to jest **tekst jawny**, a co to jest **szyfrogram**?
3. Wyjaśnij, czym jest **kryptografia**.
4. Wyjaśnij, czym zajmuje się **kryptoanaliza**.
5. Co oznacza pojęcie **kryptologia** i jakie dziedziny obejmuje?
6. W wymownym skrócie — czym różni się szyfrowanie **symetryczne** od **asymetrycznego**?
7. Podaj przynajmniej dwa przykłady zastosowań szyfrowania danych w praktyce.
8. Co oznacza, że algorytm jest „sortowaniem” i dlaczego algorytmy sortowania są ważne w informatyce?

Grupa 2: Zadania praktyczne z szyfrowania i deszyfrowania

9. Zaszyfruj słowo **DOM** szyfrem Szyfr Cezara z przesunięciem o +4.
10. Odszyfruj szyfrogram **TRHY** zakładając, że został zaszyfrowany szyfrem Cezara z przesunięciem o +5.
11. Zaszyfruj słowo **KOTKA** szyfrem Cezara z kluczem +2.
12. Utwórz szyfr **przestawieniowy** dla zdania „ALA MA KOTA” przy założeniu 3 kolumn — zapisz wynik.
13. Utwórz **anagram** ze zdania „MY LUBIMY INFORMATYKĘ” (może być dowolny układ liter, zachowujący wszystkie litery).
14. Odszyfruj (lub spróbuj) szyfrogram przestawieniowy zapisany jako „TMA AUR” wiedząc, że tekst oryginalny miał długość 6 znaków i zapisano go w wierszach po 3 znaki, kolumny odczytano w kolejności 3-1-2.
15. Zaszyfruj zdanie „ENIGMA RZĄDZI” szyfrem Cezara z przesunięciem +3.

Grupa 3: Zadania analityczne

16. Porównaj szyfrowanie symetryczne i asymetryczne — wypisz co najmniej trzy różnice.
17. W jakich sytuacjach algorytm asymetryczny (np. RSA) jest korzystniejszy niż symetryczny i dlaczego?
18. Omów, jakie zagrożenia może stwarzać słabe szyfrowanie lub jego brak w przypadku danych wrażliwych (np. bankowych).
19. Wyjaśnij, jak algorytm szyfrowania może być złamany przez kryptoanalizę — podaj przykład.
20. Wskaż, jakie cechy powinien mieć dobry algorytm sortowania oraz dlaczego te cechy są istotne w praktycznych zastosowaniach.

Grupa 4: Zadania z sortowania (Sortowanie bąbelkowe i Sortowanie przez wstawianie)

21. Posortuj liczby [7, 2, 9, 4, 1] metodą sortowania bąbelkowego — pokaż każdy pełny przebieg (po każdym przejściu listy).
22. Posortuj liczby [3, 6, 1, 8, 5] metodą sortowania przez wstawianie — pokaż, jak zmienia się część posortowana po każdym wstawieniu.
23. Dla listy [4, 2, 5, 3, 1] zaprezentuj w jednej tabeli dwa pierwsze przejścia dla obu algorytmów: bąbelkowego i przez wstawianie.
24. Wyjaśnij, w jakim przypadku (jakie ułożenie danych początkowych) sortowanie przez wstawianie może być wyraźnie szybsze niż sortowanie bąbelkowe — uzasadnij.