

1. Alice and Bob generate a session key using the Diffie-Hellman key establishment protocol. They agree on a finite cyclic group  $\mathbb{Z}_{23}^\times$  generated by 5. What is the order of  $\mathbb{Z}_{23}^\times$ ? Suppose that Alice's private exponent is 2, and Bob's private exponent is 3, what is the session key generated by Alice and Bob?

**Solution.** Alice computes  $5^2 = 25 \equiv 2 \pmod{23}$  and sends it to Bob. Bob computes  $5^3 = 125 \equiv 10 \pmod{23}$  and sends this value to Alice. To get the session key, Alice computes  $10^2 = 100 \equiv 8 \pmod{23}$  and Bob computes  $2^3 = 8 \pmod{23}$ .

2. Consider the following key agreement protocol between Alice (A) and Bob (B). Prior to starting any communication, Alice and Bob generate their secret keys  $\omega_A$  and  $\omega_B$ . Alice generates the session key  $K$ . To share  $K$  with Bob, the following sequence of messages is executed.

- (1) Alice  $\rightarrow$  Bob:  $\omega_A \oplus K$ .
- (2) Bob  $\rightarrow$  Alice:  $\omega_B \oplus \omega_A \oplus K$
- (3) Alice  $\rightarrow$  Bob:  $\omega_A \oplus \omega_B \oplus \omega_A \oplus K = \omega_B \oplus K$

After receiving the last message, Bob computes  $\omega_B \oplus \omega_B \oplus K = K$ . At this point Alice and Bob have the shared key  $K$  which they use to encrypt the communication. Can adversary Carol obtain the key  $K$  by eavesdropping on the communication channel?

**Solution.** Having obtained messages 1, 2 and 3, Carol can run an exclusive or operation on all three messages and reveal the shared secret  $K$ . Observe that

$$\begin{aligned} m_1 \oplus m_2 &= \omega_A \oplus K \oplus \omega_B \oplus \omega_A \oplus K = \omega_B, \\ (m_1 \oplus m_2) \oplus m_3 &= \omega_B \oplus \omega_B \oplus K = K. \end{aligned}$$

3. Provide prime factorization of the following integers:

- |         |         |
|---------|---------|
| (a) 64  | (b) 120 |
| (c) 375 | (d) 47  |

**Solution.**

- |                                       |                                 |
|---------------------------------------|---------------------------------|
| (a) $64 = 2^6$                        | (b) $120 = 2^3 \cdot 3 \cdot 5$ |
| (c) $375 = 15 \cdot 25 = 3 \cdot 5^3$ | (d) 47                          |

4. Given a list of functions in asymptotic notation, order them by growth rate (slowest to fastest).

- |                          |                   |                        |                            |                            |
|--------------------------|-------------------|------------------------|----------------------------|----------------------------|
| (a) $\Theta(n \log_2 n)$ | (b) $\Theta(n^2)$ | (c) $\Theta(n)$        | (d) $\Theta(1)$            | (e) $\Theta(2^n)$          |
| (f) $\Theta(n^3)$        | (g) $\Theta(n!)$  | (h) $\Theta(\log_2 n)$ | (i) $\Theta(n^2 \log_2 n)$ | (j) $\Theta(2^n \log^2 n)$ |

**Solution.** (a)  $\Theta(1)$   
 (b)  $\Theta(\log_2 n)$   
 (c)  $\Theta(n)$

- (d)  $\Theta(n \log_2 n)$
- (e)  $\Theta(n^2)$
- (f)  $\Theta(n^2 \log_2 n)$
- (g)  $\Theta(n^3)$
- (h)  $\Theta(2^n)$
- (i)  $\Theta(2^n \log^2 n)$
- (j)  $\Theta(n!)$

5. Check if the following conditions are true

- (a)  $\Theta(n + 30) = \Theta(3n - 1)$  ,
- (b)  $\Theta(n^2 + 2n - 10) = \Theta(n^2 + 3n)$  ,
- (c)  $\Theta(n^3 \cdot 3n) = \Theta(n^2 + 3n)$  .

**Solution.** (a) true (b) true (c) false

6. Write each of the following functions in  $O$  notation.

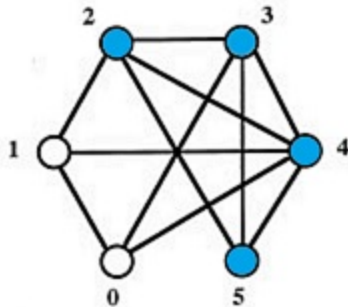
- (a)  $5 + 0.001n^3 + 0.025n$
- (b)  $500n + 100n^{1.5}$
- (c)  $0.3n + 5n^{1.5} + 2.5n^{1.75}$

**Solution.**

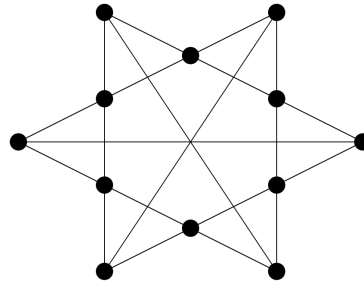
$O(n^3)$  ,

$O(n^{1.5})$  ,

$O(n^{1.75})$  .



(a) Maximal clique problem



(b) graph 3-coloring problem

7. Find the maximal clique in the graph shown in Fig. 1a. A subgraph  $H$  of a graph  $G$  is a maximal clique in  $G$  if there is an edge between every pair of vertices in  $H$ , and there is no vertex in  $G \setminus H$  connected to every vertex in  $H$ .

**Solution.** The vertices belonging to the maximal clique are marked in blue.

8. Provide a 3-coloring of the graph shown in Fig. 1b so that any two adjacent vertices do not share the same color.

**Solution.** To verify if the graph in Fig. 1b is 3-colorable, we reduce this problem to a 3-SAT instance, and run it through an SMT solver. The reduction of the 3-SAT to 3-colorability is pretty straightforward and can be easily inferred by reading the 3-SAT model. You can see the 3-SAT formulation of the task in file named "3sat". To verify uncolorability, copy-paste the model into Z3 solver the online version of which can be found here: <https://rise4fun.com/z3>.

The result is that this graph is **unsatisfiable**, which means that it is also not 3-colorable. The unsatisfiability core (the least set of edges, the vertices of which cannot be 3-colorable) is

```
(v1v2 v2v3 v3v4 v2v4 v4v5 v5v6 v4v6 v6v7 v7v8 v6v8 v8v9 v9v10  
v8v10 v10v11 v11v12 v10v12 v1v12 v2v12 v1v7 v5v11 v3v9)
```