RSA and Course Summary

Ali Akbari

June 2025

RSA Example

- **Problem**: Encrypt message 9 with primes $p = 3$, $q = 11$, $e = 7$, $d = 3$.
- **Step-by-Step**:
  1. $n = p \times q = 33$, $\phi(n) = 20$.
  2. Encrypt: $9^7 \mod 33 = 27$.
  3. Decrypt: $27^3 \mod 33 = 9$.

RSA

- Uses modular exponentiation with public/private keys.
- Security relies on factoring large numbers.
- **Time Complexity**: $O(\log k)$ for exponentiation.
- **Space Complexity**: $O(1)$.

Course Summary

- Covered sorting, searching, graphs, DP, cryptography.
- Introduced time complexity (O, Ω, Θ).
- Future: Machine learning (e.g., optimization like gradient descent).