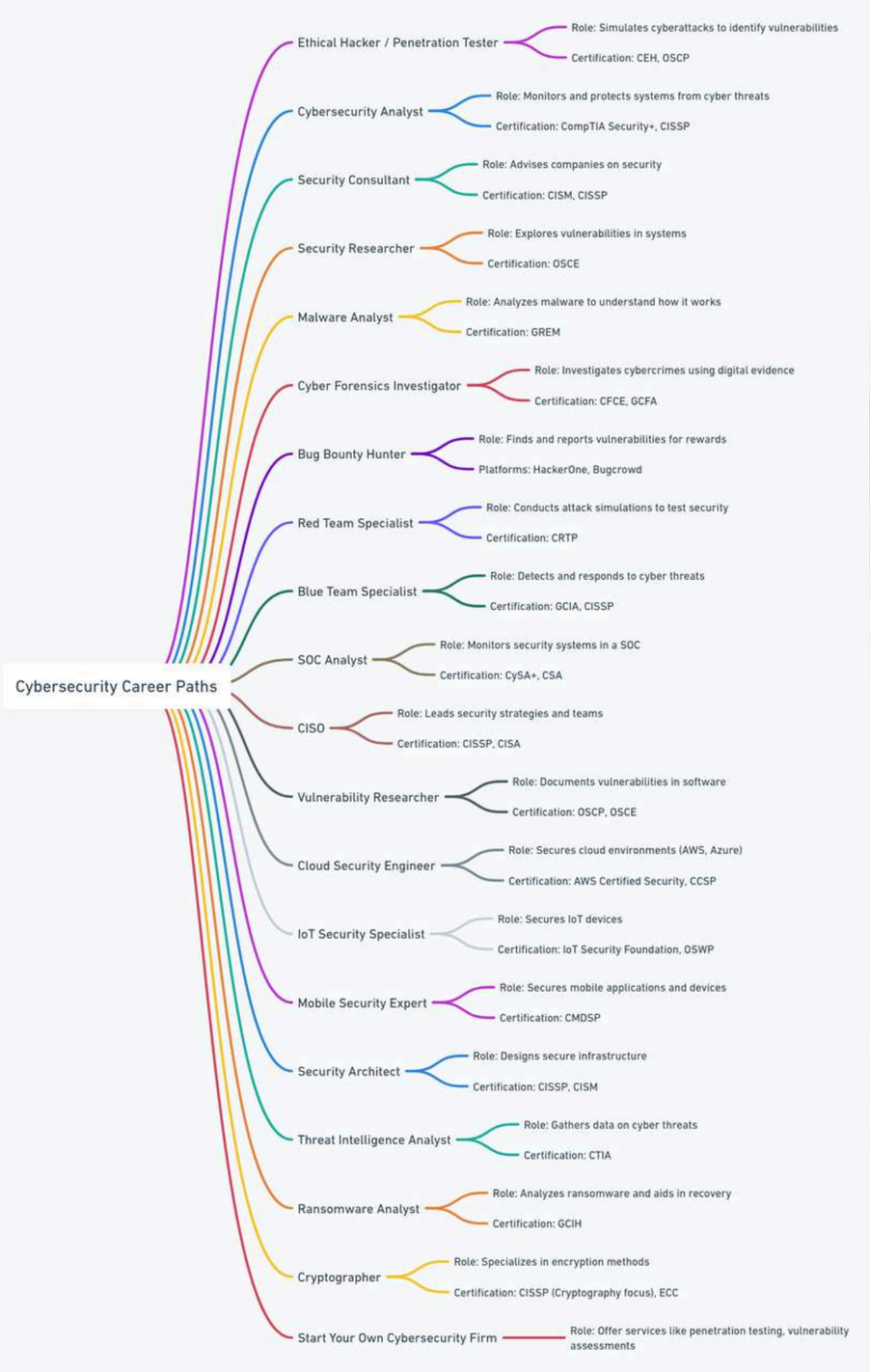
CYBER SECURITY PATHWAYS

MIND MAP


Cybersecurity Career Paths
Ethical Hacker / Penetration Tester
Role: Simulates cyberattacks to identify vulnerabilities
Certification: CEH, OSCP
Cybersecurity Analyst
Role: Monitors and protects systems from cyber threats
Certification: CompTIA Security+, CISSP
Security Consultant
Role: Advises companies on security
Certification: CISM, CISSP
Security Researcher
Role: Explores vulnerabilities in systems
Certification: OSCE
Malware Analyst
Role: Analyzes malware to understand how it works
Certification: GREM
Cyber Forensics Investigator
Role: Investigates cybercrimes using digital evidence
Certification: CFCE, GCFA
Bug Bounty Hunter
Role: Finds and reports vulnerabilities for rewards
Platforms: HackerOne, Bugcrowd
Red Team Specialist
Role: Conducts attack simulations to test security
Certification: CRTP
Blue Team Specialist
Role: Detects and responds to cyber threats
Certification: GCIA, CISSP
SOC Analyst
Role: Monitors security systems in a SOC
Certification: CySA+, CSA
CISO
Role: Leads security strategies and teams
Certification: CISSP, CISA
Vulnerability Researcher
Role: Documents vulnerabilities in software
Certification: OSCP, OSCE
Cloud Security Engineer
Role: Secures cloud environments (AWS, Azure)
Certification: AWS Certified Security, CCSP
IoT Security Specialist
Role: Secures IoT devices
Certification: IoT Security Foundation, OSWP
Mobile Security Expert
Role: Secures mobile applications and devices
Certification: CMDSP
Security Architect
Role: Designs secure infrastructure
Certification: CISSP, CISM
Threat Intelligence Analyst
Role: Gathers data on cyber threats
Certification: CTIA
Ransomware Analyst
Role: Analyzes ransomware and aids in recovery
Certification: GCIH
Cryptographer
Role: Specializes in encryption methods
Certification: CISSP (Cryptography focus), ECC
Start Your Own Cybersecurity Firm
Role: Offer services like penetration testing, vulnerability assessments

CAREER PATHS

1. ETHICAL HACKER / PENETRATION TESTER

ROLE: SIMULATES CYBERATTACKS TO IDENTIFY VULNERABILITIES IN SYSTEMS BEFORE MALICIOUS HACKERS EXPLOIT THEM. ETHICAL HACKERS WORK TO STRENGTHEN SECURITY MEASURES BY FINDING WEAKNESSES.

CERTIFICATION: CERTIFIED ETHICAL HACKER (CEH), OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP).

2. CYBERSECURITY ANALYST

ROLE: MONITORS AND PROTECTS AN ORGANIZATION'S SYSTEMS AND NETWORKS FROM CYBER THREATS. ANALYSTS RESPOND TO SECURITY INCIDENTS AND IMPLEMENT PREVENTIVE MEASURES.

CERTIFICATION: COMPTIA SECURITY+, CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP).

3. SECURITY CONSULTANT

ROLE: ADVISES COMPANIES ON HOW TO PROTECT THEIR ASSETS AND INFORMATION SYSTEMS. SECURITY CONSULTANTS ASSESS RISKS, DESIGN SECURITY FRAMEWORKS, AND IMPLEMENT SOLUTIONS.

CERTIFICATION: CERTIFIED INFORMATION SECURITY MANAGER (CISM), CISSP.

4. SECURITY RESEARCHER

ROLE: EXPLORES VULNERABILITIES IN SOFTWARE, HARDWARE, AND SYSTEMS. SECURITY RESEARCHERS DISCOVER NEW ATTACK VECTORS, WRITE EXPLOITS, AND WORK TO DEVELOP SECURITY PATCHES.

CERTIFICATION: RESEARCH-FOCUSED CERTIFICATIONS LIKE OSCE (OFFENSIVE SECURITY CERTIFIED EXPERT).

5. MALWARE ANALYST

ROLE: ANALYZES MALWARE, VIRUSES, AND OTHER MALICIOUS SOFTWARE TO UNDERSTAND HOW THEY FUNCTION AND HOW TO PROTECT AGAINST THEM. THEY OFTEN WORK IN INCIDENT RESPONSE OR CYBERSECURITY FORENSICS.

CERTIFICATION: GIAC REVERSE ENGINEERING MALWARE (GREM).

6. CYBER FORENSICS INVESTIGATOR

ROLE: INVESTIGATES CYBERCRIMES BY GATHERING AND ANALYZING DIGITAL EVIDENCE. CYBER FORENSICS PROFESSIONALS WORK IN LAW ENFORCEMENT, PRIVATE FIRMS, OR GOVERNMENT AGENCIES TO TRACK HACKERS AND GATHER EVIDENCE FOR LEGAL PROCEEDINGS.

CERTIFICATION: CERTIFIED FORENSIC COMPUTER EXAMINER (CFCE), GIAC CERTIFIED FORENSIC ANALYST (GCFA).

7. BUG BOUNTY HUNTER

ROLE: PARTICIPATES IN BUG BOUNTY PROGRAMS OFFERED BY COMPANIES, FINDING AND REPORTING VULNERABILITIES IN EXCHANGE FOR MONETARY REWARDS. MANY BUG BOUNTY HUNTERS WORK INDEPENDENTLY.

PLATFORMS: HACKERONE, BUGCROWD.

8. RED TEAM SPECIALIST

ROLE: WORKS WITHIN AN ORGANIZATION TO CONDUCT FULL-SCOPE ATTACK SIMULATIONS. RED TEAMS MIMIC ADVANCED PERSISTENT THREAT (APT) ACTORS TO TEST THE SECURITY POSTURE OF A COMPANY.

CERTIFICATION: CERTIFIED RED TEAM PROFESSIONAL (CRTP).

9. BLUE TEAM SPECIALIST

ROLE: WORKS ON THE DEFENSE SIDE, PROTECTING SYSTEMS FROM ATTACKS. BLUE TEAMS ARE RESPONSIBLE FOR DETECTING AND RESPONDING TO CYBER THREATS IN REAL-TIME.

CERTIFICATION: GIAC CERTIFIED INTRUSION ANALYST (GCIA), CISSP.

10. SECURITY OPERATIONS CENTER (SOC) ANALYST

ROLE: MONITORS AND MANAGES SECURITY SYSTEMS WITHIN A SOC. THEY RESPOND TO SECURITY INCIDENTS, ANALYZE THREAT DATA, AND ENSURE THAT SECURITY MEASURES ARE FUNCTIONING PROPERLY.

CERTIFICATION: COMPTIA CYBERSECURITY ANALYST (CYSA+), CERTIFIED SOC ANALYST (CSA).

11. CHIEF INFORMATION SECURITY OFFICER (CISO)
ROLE: HEADS THE INFORMATION SECURITY DEPARTMENT IN A COMPANY, RESPONSIBLE FOR MANAGING SECURITY STRATEGIES AND POLICIES. A CISO LEADS TEAMS TO PROTECT THE ORGANIZATION'S ASSETS AND ENSURES COMPLIANCE WITH REGULATIONS.
CERTIFICATION: CISSP, CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA).
12. VULNERABILITY RESEARCHER
ROLE: FOCUSES ON FINDING AND DOCUMENTING VULNERABILITIES IN SOFTWARE OR HARDWARE, OFTEN CONTRIBUTING TO OPEN-SOURCE COMMUNITIES OR WORKING FOR LARGE TECH COMPANIES.
CERTIFICATION: OSCP, OSCE.
13. CLOUD SECURITY ENGINEER
ROLE: ENSURES THAT CLOUD ENVIRONMENTS (E.G., AWS, AZURE, GOOGLE CLOUD) ARE SECURE FROM CYBER THREATS. THEY CONFIGURE CLOUD SECURITY SERVICES, MONITOR ACCESS CONTROLS, AND SECURE DATA STORED IN THE CLOUD.
CERTIFICATION: AWS CERTIFIED SECURITY – SPECIALTY, CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP).
14. IOT SECURITY SPECIALIST
ROLE: FOCUSES ON SECURING INTERNET OF THINGS (IOT) DEVICES, WHICH HAVE BECOME A GROWING TARGET FOR HACKERS. SPECIALISTS PROTECT CONNECTED DEVICES, SENSORS, AND NETWORKS FROM CYBERATTACKS.
CERTIFICATION: IOT SECURITY FOUNDATION CERTIFICATIONS, OFFENSIVE SECURITY WIRELESS PROFESSIONAL (OSWP).
15. MOBILE SECURITY EXPERT
ROLE: SECURES MOBILE APPLICATIONS AND DEVICES AGAINST THREATS LIKE MOBILE MALWARE, UNAUTHORIZED ACCESS, AND DATA BREACHES. MOBILE SECURITY EXPERTS WORK WITH ANDROID, IOS, AND OTHER MOBILE PLATFORMS.
CERTIFICATION: CERTIFIED MOBILE DEVICE SECURITY PROFESSIONAL (CMDSP).

16. SECURITY ARCHITECT

ROLE: DESIGNS, BUILDS, AND OVERSEES THE IMPLEMENTATION OF COMPLEX SECURITY SYSTEMS. SECURITY ARCHITECTS CREATE BLUEPRINTS FOR SECURE INFRASTRUCTURE AND NETWORKS.

CERTIFICATION: CISSP, CISM.

17. THREAT INTELLIGENCE ANALYST

ROLE: GATHERS AND ANALYZES DATA ON CYBER THREATS TO PROVIDE ACTIONABLE INSIGHTS. THREAT INTELLIGENCE ANALYSTS WORK TO PREDICT AND MITIGATE FUTURE ATTACKS BY UNDERSTANDING ADVERSARY TACTICS.

CERTIFICATION: CERTIFIED THREAT INTELLIGENCE ANALYST (CTIA).

18. RANSOMWARE ANALYST / SPECIALIST

ROLE: DEALS WITH THE AFTERMATH OF RANSOMWARE ATTACKS BY ANALYZING THE RANSOMWARE, ASSISTING IN NEGOTIATIONS, AND HELPING ORGANIZATIONS RECOVER THEIR ENCRYPTED DATA.

CERTIFICATION: INCIDENT RESPONSE-FOCUSED CERTIFICATIONS LIKE GIAC CERTIFIED INCIDENT HANDLER (GCIH).

19. CRYPTOGRAPHER

ROLE: SPECIALIZES IN SECURING COMMUNICATIONS THROUGH ENCRYPTION METHODS. CRYPTOGRAPHERS DEVELOP ENCRYPTION ALGORITHMS AND PROTOCOLS TO PROTECT SENSITIVE DATA.

CERTIFICATION: CISSP WITH CRYPTOGRAPHY FOCUS, ECC (ELLIPTIC CURVE CRYPTOGRAPHY) CERTIFICATION.

20. START YOUR OWN CYBERSECURITY FIRM

ROLE: IF YOU HAVE A BROAD SET OF SKILLS AND EXPERIENCE, YOU COULD START YOUR OWN CYBERSECURITY CONSULTING BUSINESS, OFFERING SERVICES LIKE PENETRATION TESTING, VULNERABILITY ASSESSMENTS, AND INCIDENT RESPONSE TO CLIENTS.

CERTIFICATIONS

1. Ethical Hacker / Penetration Tester

Certified Ethical Hacker (CEH)

Offensive Security Certified Professional (OSCP)

GIAC Penetration Tester (GPEN)

2. Cybersecurity Analyst

CompTIA Security+

Certified Information Systems Security Professional (CISSP)

Certified Cybersecurity Analyst (CySA+)

3. Security Consultant

Certified Information Systems Security Professional (CISSP)

Certified Information Security Manager (CISM)

Certified Information Systems Auditor (CISA)

4. Security Researcher

Offensive Security Certified Expert (OSCE)

Offensive Security Web Expert (OSWE)

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

5. Malware Analyst

GIAC Reverse Engineering Malware (GREM)

Certified Incident Handler (GCIH)

Offensive Security Certified Expert (OSCE)

6. Cyber Forensics Investigator
Certified Forensic Computer Examiner (CFCE)
GIAC Certified Forensic Analyst (GCFA)
GIAC Certified Forensic Examiner (GCFE)
7. Bug Bounty Hunter
Offensive Security Certified Professional (OSCP)
Certified Ethical Hacker (CEH)
8. Red Team Specialist
Certified Red Team Professional (CRTP)
Offensive Security Certified Professional (OSCP)
GIAC Penetration Tester (GPEN)
9. Blue Team Specialist
GIAC Certified Intrusion Analyst (GCIA)
GIAC Certified Enterprise Defender (GCED)
Certified Information Systems Security Professional (CISSP)
10. Security Operations Center (SOC) Analyst
CompTIA Cybersecurity Analyst (CySA+)
Certified SOC Analyst (CSA)
GIAC Certified Incident Handler (GCIH)

11. Chief Information Security Officer (CISO)
Certified Information Systems Security Professional (CISSP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
12. Vulnerability Researcher
Offensive Security Certified Professional (OSCP)
Offensive Security Certified Expert (OSCE)
GIAC Web Application Penetration Tester (GWAPT)
13. Cloud Security Engineer
AWS Certified Security – Specialty
Certified Cloud Security Professional (CCSP)
Google Professional Cloud Security Engineer
14. IoT Security Specialist
Offensive Security Wireless Professional (OSWP)
IoT Security Foundation Certifications
Certified Internet of Things Security Practitioner (CIoTSP)
15. Mobile Security Expert
Certified Mobile Device Security Professional (CMDSP)
Offensive Security Certified Professional (OSCP)

16. Security Architect

Certified Information Systems Security Professional (CISSP)

Certified Information Security Manager (CISM)

Certified Information Systems Auditor (CISA)

17. Threat Intelligence Analyst

Certified Threat Intelligence Analyst (CTIA)

GIAC Cyber Threat Intelligence (GCTI)

Certified Information Systems Security Professional (CISSP)

18. Ransomware Analyst

GIAC Certified Incident Handler (GCIH)

Certified Ethical Hacker (CEH)

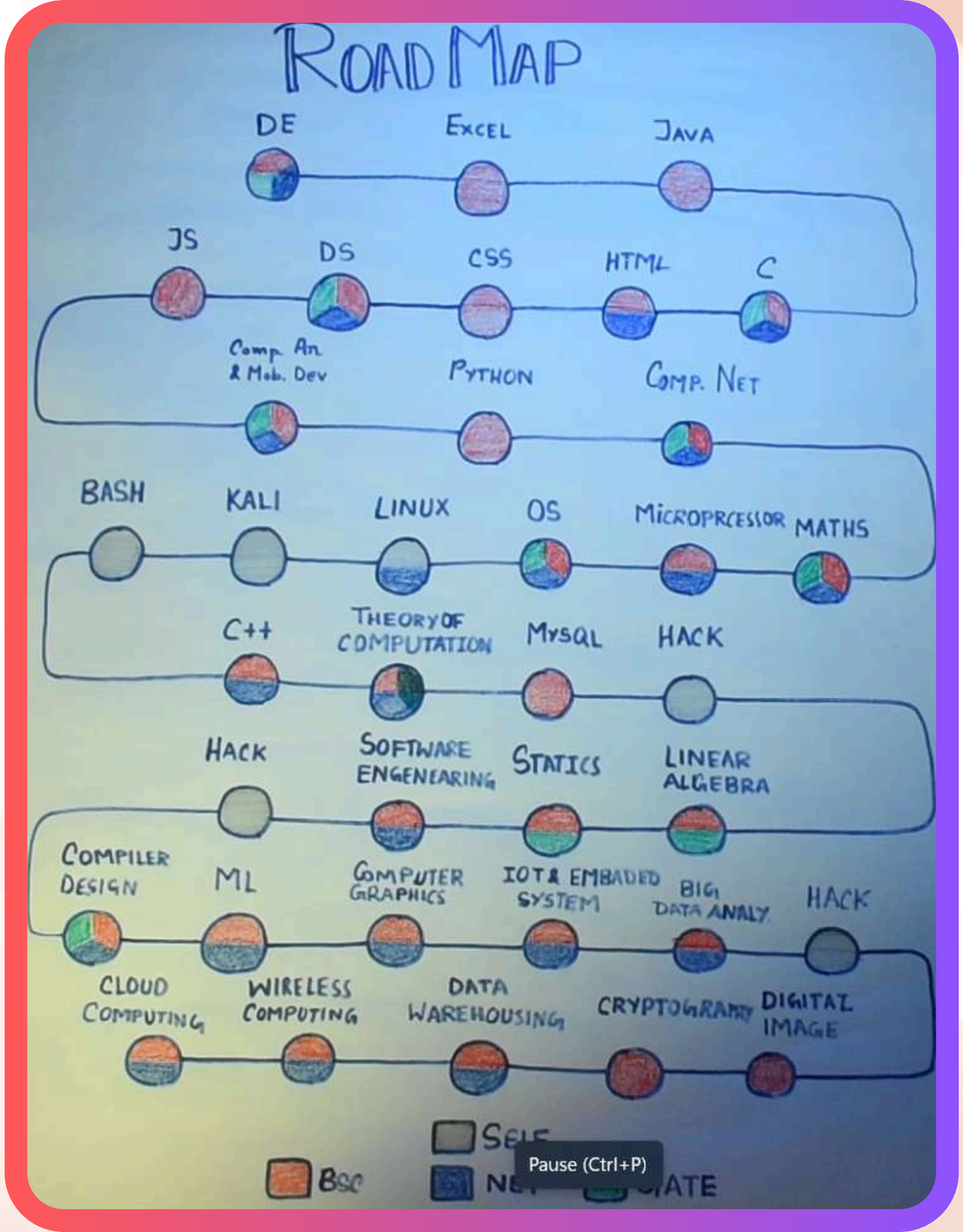
19. Cryptographer

Certified Information Systems Security Professional (CISSP) – Cryptography focus

ECC (Elliptic Curve Cryptography) certification

20. Start Your Own Cybersecurity Firm

Depending on the services offered, certifications like CISSP, CISM, OSCP, and CEH will be valuable for credibility and technical expertise.


ROAD MAP
DE
EXCEL
JAVA
JS
DS
CSS
HTML
C
COMP. AN & MOB. DEV
PYTHON
COMP. NET
BASH
KALI
LINUX
OS
MICROPRCESSOR
MATHS
C++
THEORY OF COMPUTATION
MYSQL
HACK
HACK
SOFTWARE ENGENEARING
STATICS
LINEAR ALGEBRA
COMPILER DESIGN
ML
COMPUTER GRAPHICS
IOT & EMBADED SYSTEM
BIG DATA ANALY
HACK
CLOUD COMPUTING
WIRELESS COMPUTING
DATA WAREHOUSING
CRYPTOGRAPHY
DIGITAL IMAGE
BSC
SELF
NET
GATE

BSc SYLLABUS

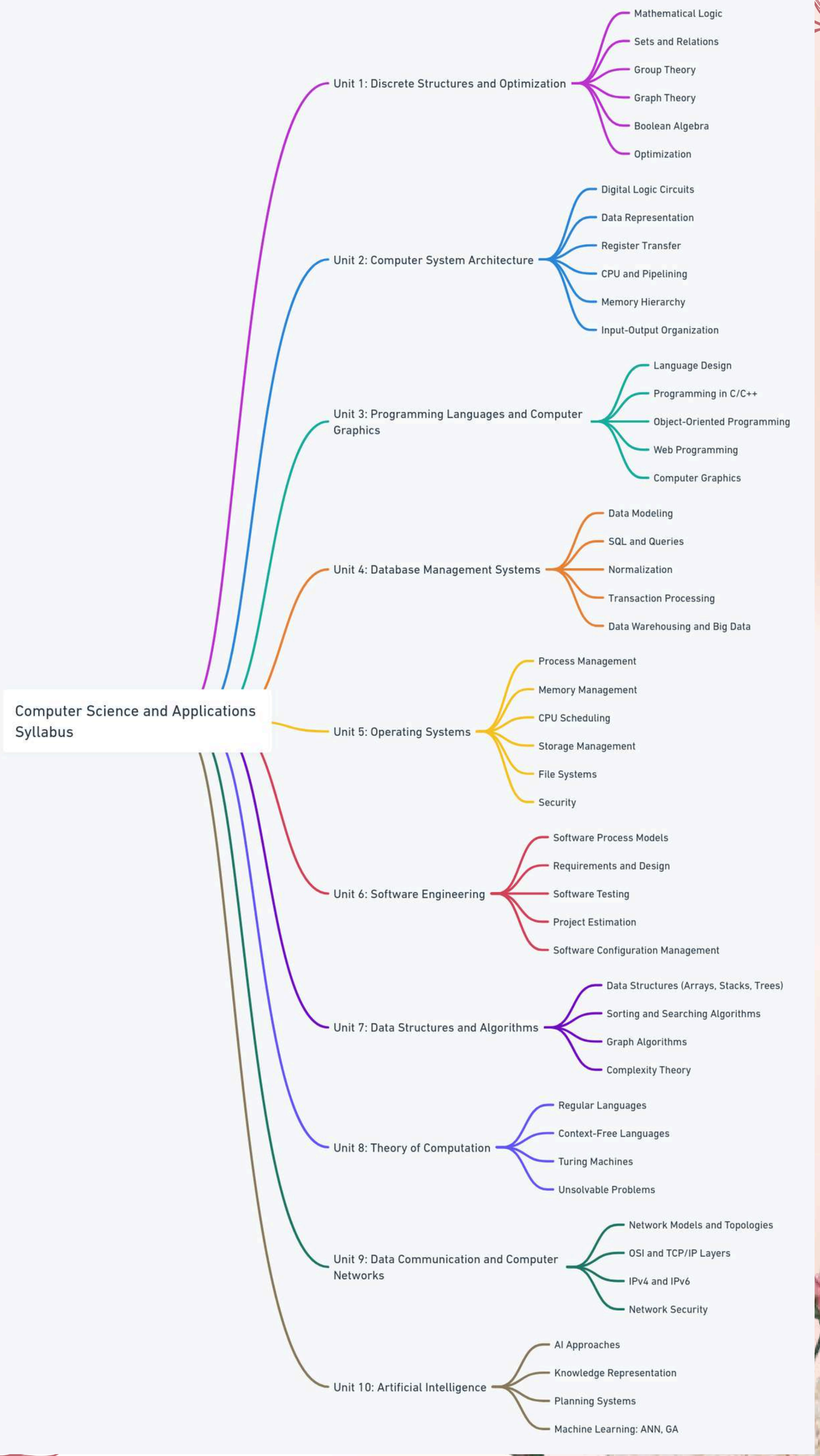
Topics in Core Subjects (Excluding Programming Languages)

- Logic Design
  - Computer Fundamentals & Digital Logic
  - Computer Architecture & Organization
- Microprocessor — 8085 MPU Programming
- Shell Programming — Operating System
- Database Management — Database Management System (DBMS)
- Data Communication & Networking
  - Data Communication & Networking
  - Mobile & Wireless Computing
- Digital Image Processing — Python with OpenCV
- Compiler Design — Related to theory
- IoT & Embedded Systems — IoT & Embedded Systems
- Big Data Analytics — Hadoop, MongoDB, JavaSpark
- Cloud Computing — Cloud Simulator Learning, Virtualization, Cloud Services
- Statistical Methods & Linear Algebra — Using Python
- Graph Algorithms — Algorithms using C++
- System Analysis & Design — System Analysis & Design Lab
- Data Warehousing

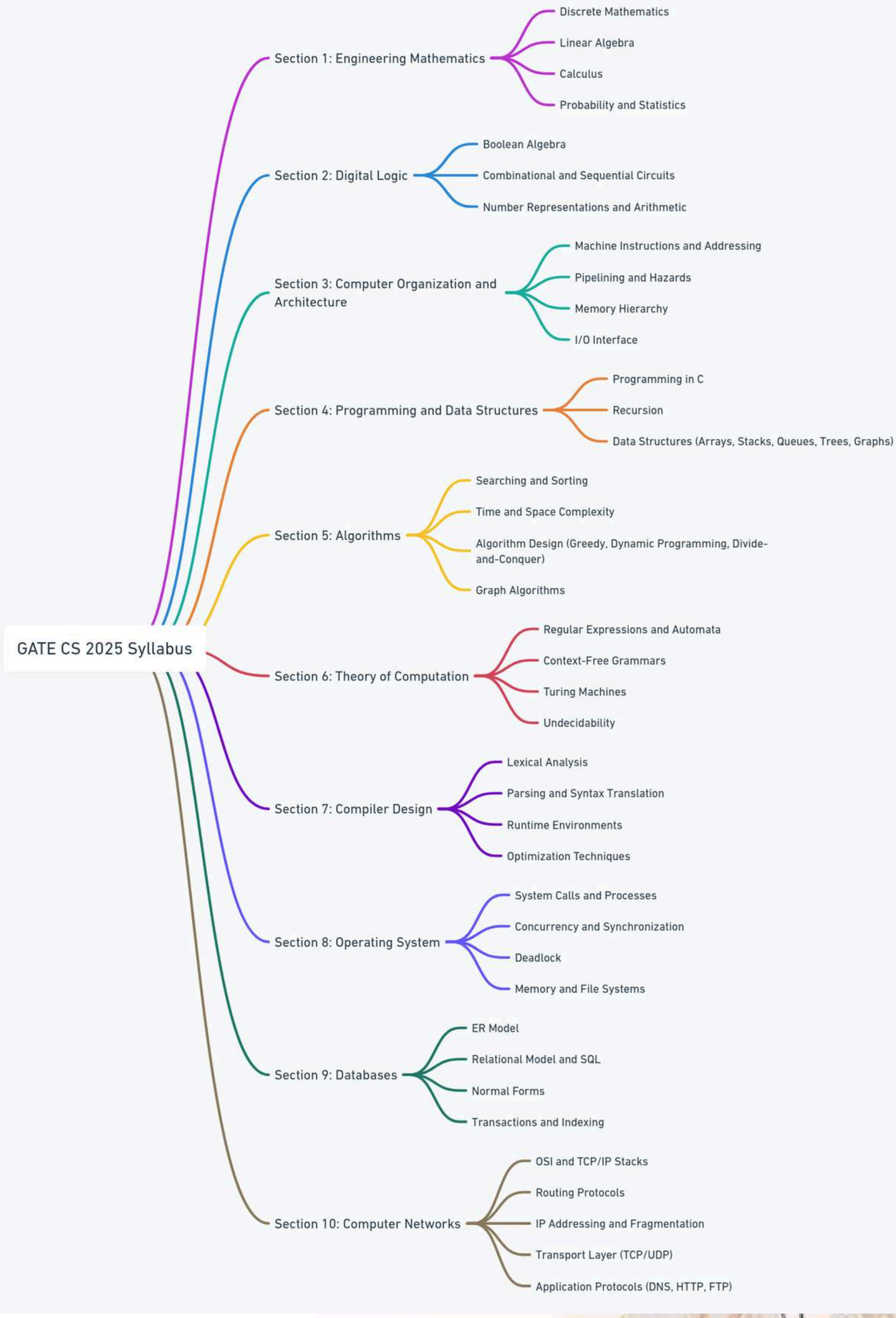
Programming Languages in Core Subjects

- C
  - Problem Solving using C
  - Algorithms using C++
- C++ — Graph Algorithms
- Java — Object-Oriented Programming
- Python
  - Programming in Python
  - Machine Learning
  - Linear Algebra & Statistical Methods
  - Compiler Design
  - Data Warehousing
- Shell Programming — Operating System
- JavaScript (JS) — Database Management Systems

NET SYLLABUS



GATE SYLLABUS



Thank You