🔐Authentication & Authorization — Master Syllabus (LOCKED)

This document is **final and frozen**. It is designed for **deep understanding + real-world implementation** using **Node.js and Express**.

PHASE 0 — Cryptography Foundations (MANDATORY)

Topic 0.1 — Cryptography Terminologies

- Plaintext
- Ciphertext
- Encryption
- Decryption
- Key
- Hash
- Salt
- Signature

Topic 0.2 — Symmetric Cryptography

- Symmetric key
- Shared secret
- AES
- Key rotation
- Pros & cons of symmetric crypto

Topic 0.3 — Asymmetric Cryptography

- Public key
- Private key
- Key pair
- RSA vs Elliptic Curve (EC)
- Where public/private keys are used

Topic 0.4 — Digital Signatures

- Signing vs encryption
- Integrity
- Authenticity
- Non-repudiation
- Why JWTs are signed, not encrypted

Topic 0.5 — Hashing & Password Security

- Hash vs encryption
- bcrypt / argon2
- Password verification flow
- Rainbow tables
- Secure password storage

PHASE 1 — Authentication & Authorization Foundations

Topic 1 — Authentication vs Authorization

- Identity
- Principal
- Permission
- Policy
- AuthN vs AuthZ separation
- Express middleware responsibility

PHASE 2 — JWT (Token-Based Security)

Topic 2 — JWT Fundamentals

- Token
- Claim
- Header / Payload / Signature
- HS256 vs RS256
- Token lifecycle

Topic 3 — Secure Token Storage

- XSS
- CSRF
- HttpOnly cookies
- SameSite
- Why LocalStorage is dangerous

PHASE 3 — OAuth 2.0 (Authorization Framework)

Topic 4 — OAuth 2.0 Core Terminologies

- Resource Owner
- Client
- Authorization Server
- Resource Server

- Scope

Topic 5 — OAuth 2.0 Grant Types

- Authorization Code Grant
- Client Credentials Grant
- Refresh Token Grant
- Why Implicit Grant is deprecated

Topic 6 — OAuth 2.0 Authorization Code Flow

- Redirect-based flow
- Code exchange
- Token trust boundaries
- Attack scenarios

PHASE 4 — OpenID Connect (OIDC)

Topic 7 — OpenID Connect Basics

- ID Token
- Access Token
- UserInfo endpoint
- OAuth vs OIDC

Topic 8 — OIDC Flow & Token Validation

- iss, aud, sub, exp, nonce
- ID token validation rules
- Login vs API authorization

PHASE 5 — Express.js Real-World Implementation

Topic 9 — Express Authentication Architecture

- Middleware chaining
- Auth context propagation
- Error handling strategy

Topic 10 — Implementing JWT Auth in Express

- Login endpoint
- Token issuance

- Verification middleware
- Role-based authorization

Topic 11 — OAuth / OIDC Login in Express

- passport
- openid-client
- Google/Auth0-style login
- Session vs token-based auth

PHASE 6 — Security Hardening (Senior Level)

Topic 12 — Common Auth Vulnerabilities

- JWT misconfiguration
- Algorithm confusion attacks
- BOLA / IDOR
- Token leakage

Topic 13 — Authorization Models

- RBAC
- ABAC
- Policy-based authorization
- Why roles alone are insufficient

Topic 14 — Production Best Practices

- Token rotation
- Logout & revocation
- Auditing & logging
- Zero Trust principles

PHASE 7 — Platform & Network Security

Topic 15 — TLS / HTTPS Basics

- Certificates
- Public key usage in TLS
- Why OAuth requires HTTPS

Topic 16 — CSRF, CORS, Rate Limiting

- CSRF attacks & mitigations
- CORS misconceptions
- API abuse prevention

Topic 17 — Secrets & Key Management

- Environment variables
- Key rotation
- Why secrets must never be committed

🔗Learning Rules (Permanent)

- Every topic starts with **Terminologies**
- Follow order: Terminologies → Concept → Why → Technical → Implementation
- One topic at a time
- Move forward only after acknowledgment

🔒**This syllabus is locked unless explicitly changed by you.**