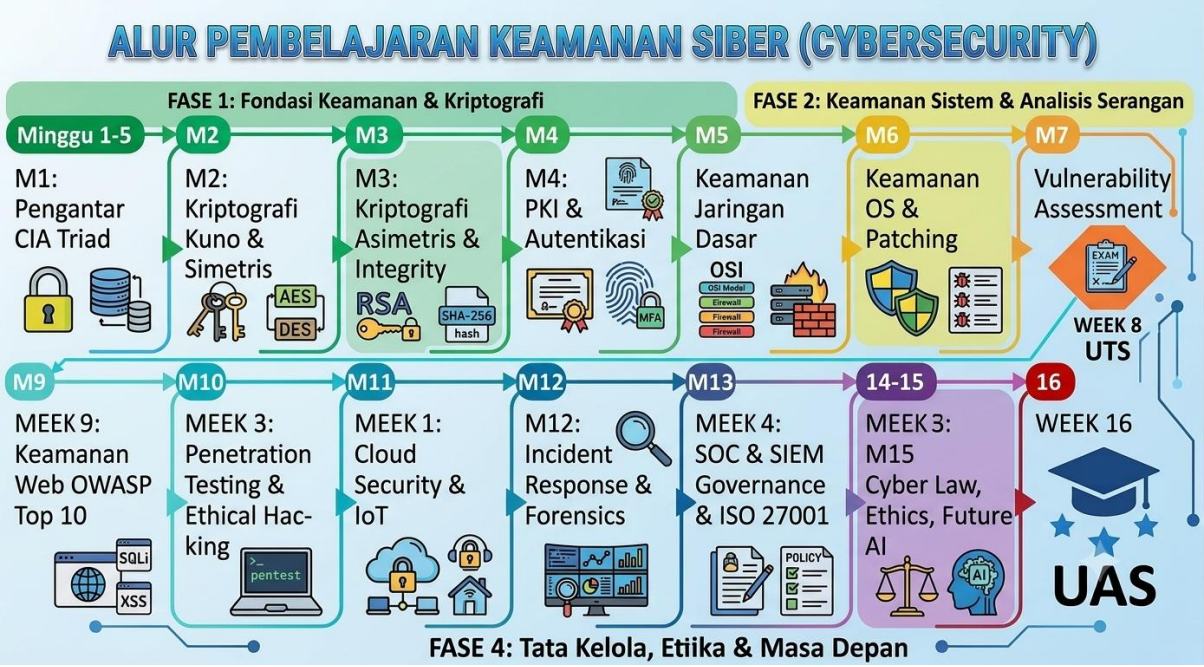

Berikut adalah rancangan alur pembelajaran mata kuliah **Keamanan Siber (Cybersecurity)** yang terstruktur secara sistematis selama 16 pertemuan, bergerak dari konsep dasar, aspek teknis pertahanan dan serangan, hingga manajemen kepatuhan.

- **Fase 1: Fondasi Keamanan & Kriptografi (Minggu 1 - 5)**

Fase ini membangun pemahaman dasar tentang lanskap ancaman dan prinsip matematika di balik pengamanan data.

- **Minggu 1: Pengantar Keamanan Siber & Lanskap Ancaman**
    - Definisi keamanan siber, triad CIA (*Confidentiality, Integrity, Availability*).
    - Pengenalan jenis-jenis ancaman (malware, phishing, ransomware, social engineering).
- **Minggu 2: Dasar-Dasar Kriptografi Kuno & Simetris**
    - Sejarah kriptografi dan konsep cipher teks.
    - Algoritma kunci simetris (DES, AES) dan manajemen kunci.
- **Minggu 3: Kriptografi Asimetris & Integritas Data**
    - Kriptografi kunci publik (RSA, ECC).
    - Fungsi Hash (MD5, SHA-256) dan Tanda Tangan Digital (*Digital Signature*).
- **Minggu 4: Infrastruktur Kunci Publik & Autentikasi**
    - *Public Key Infrastructure* (PKI) dan Sertifikat Digital (X.509).
    - Mekanisme autentikasi (MFA, Biometrik, OAuth).
- **Minggu 5: Keamanan Jaringan Dasar**
    - Arsitektur jaringan aman dan model OSI/TCP-IP dari perspektif keamanan.

    - Prinsip kerja Firewall, IDS (*Intrusion Detection System*), dan IPS (*Intrusion Prevention System*).

- **Fase 2: Keamanan Sistem & Analisis Serangan (Minggu 6 - 7)**

Fase untuk memahami celah keamanan pada infrastruktur komputer sebelum evaluasi tengah semester.

- **Minggu 6: Keamanan Sistem Operasi & Pengerasan (*Hardening*)**
    - Celah keamanan pada Windows dan Linux.
    - Teknik *OS hardening*, manajemen hak akses (*Least Privilege*), dan *patching*.
- **Minggu 7: *Vulnerability Assessment* & Pemindaian Celah**
    - Konsep siklus manajemen kerentanan.
    - Praktik pemindaian menggunakan perangkat lunak pemindai celah (*vulnerability scanner*).
- **Minggu 8: Ujian Tengah Semester (UTS)**
- **Fase 3: Keamanan Aplikasi, Operasi, & Defensif (Minggu 9 - 13)**

Fase yang berfokus pada implementasi keamanan di tingkat aplikasi, deteksi insiden aktif, dan taktik defensif.

- **Minggu 9: Keamanan Aplikasi Web & OWASP Top 10**
    - Analisis celah keamanan web terpopuler (SQL Injection, Cross-Site Scripting/XSS, Broken Authentication).
    - Praktik pengamanan kode (*Secure Coding*).
- **Minggu 10: *Penetration Testing* & Peretasan Etis (*Ethical Hacking*)**
    - Metodologi pengujian penetrasi (*Black, Grey, White box testing*).
    - Tahapan *reconnaissance*, *scanning*, *gaining access*, dan *maintaining access*.
- **Minggu 11: Keamanan Komputasi Awan (*Cloud Security*) & IoT**
    - Tantangan keamanan pada arsitektur Cloud (AWS, Azure, GCP) dan model *Shared Responsibility*.
    - Kerentanan pada perangkat IoT (*Internet of Things*).
- **Minggu 12: Manajemen Insiden & *Digital Forensics***
    - Langkah-langkah merespons insiden keamanan (*Incident Response Life Cycle*).
    - Dasar-dasar investigasi digital, akuisisi bukti (*imaging*), dan analisis artefak.
- **Minggu 13: *Security Operations Center* (SOC) & Analisis Log**
    - Peran SOC dalam perusahaan.
    - Pemanfaatan teknologi SIEM (*Security Information and Event Management*) untuk pemantauan ancaman *real-time*.
- **Fase 4: Tata Kelola, Etika, & Masa Depan (Minggu 14 - 15)**

Fase penutup untuk memahami aspek non-teknis, hukum, regulasi, dan tren masa depan keamanan siber.

- **Minggu 14: Tata Kelola Keamanan Informasi (*Cybersecurity Governance* & ISO 27001)**
    - Manajemen risiko TI dan penyusunan kebijakan keamanan korporasi.
    - Standar internasional keamanan informasi (ISO/IEC 27001, NIST Framework).
- **Minggu 15: Hukum Siber (*Cyber Law*), Etika, & Tren Masa Depan**
    - Regulasi perlindungan data (seperti UU PDP di Indonesia, GDPR di Eropa).
    - Tantangan keamanan baru: AI dalam serangan siber (*Adversarial AI*) dan *Quantum Computing vs Cryptography*.
- **Minggu 16: Ujian Akhir Semester (UAS)**