| | Universitas Negeri Surabaya<br>Fakultas Teknik<br>Program Studi S2 Informatika | Kode Dokumen |
|---|---|---|

# RENCANA PEMBELAJARAN SEMESTER

| MATA KULIAH (MK) | KODE | Rumpun MK | BOBOT (sks) | | | SEMESTER | Tgl Penyusunan |
|---|---|---|---|---|---|---|---|
| Keamanan Jaringan dan Kriptografi | 5510003013 | Mata Kuliah Wajib Program Studi | T=3 | P=0 | ECTS=6.72 | 2 | 16 Januari 2025 |

| OTORISASI | Pengembang RPS | Koordinator RMK | Koordinator Program Studi |
|---|---|---|---|
| | Ibnu Febry Kurniawan, S.Kom., M.Sc., Ph.D. | Dr. Ir. Ricky Eka Putra, S.Kom., M.Kom. | RICKY EKA PUTRA |

| | | |
|---|---|---|
| **Model Pembelajaran** | **Project Based Learning** | |
| **Capaian Pembelajaran (CP)** | **CPL-PRODI yang dibebankan pada MK** | |
| | **CPL-3** | Mengembangkan pemikiran logis, kritis, sistematis, dan kreatif dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan |
| | **CPL-5** | Menguasai dan mengaplikasikan teori-teori, konsep, prinsip, dan teknologi terkini dalam bidang Teknik Informatika, termasuk Data Sains, Kecerdasan Artifisial, Jaringan Cerdas, Rekayasa Perangkat Lunak, serta Sistem dan Teknologi Informasi untuk mengembangkan ilmu pengetahuan dan teknologi melalalui riset dan penciptaan karya inovatif. |
| | **CPL-7** | Menganalisis kebutuhan dan menyelesaikan masalah yang kompleks dalam berbagai bidang Teknik Informatika, menggunakan metode analitis dan pendekatan ilmiah. |
| | **CPL-8** | Mengevaluasi kinerja sistem dan teknologi informasi serta mengimplementasikan perbaikan berkelanjutan berdasarkan data dan analisis. |
| | **CPL-9** | Mengembangkan solusi inovatif untuk meningkatkan efisiensi dan efektivitas organisasi dengan memanfaatkan teknologi informasi terbaru. |
| | **Capaian Pembelajaran Mata Kuliah (CPMK)** | |
| | **CPMK - 1** | Menerapkan prinsip-prinsip keamanan jaringan dan kriptografi dalam pengembangan dan pengelolaan jaringan yang aman (C3) |
| | **CPMK - 2** | Menganalisis dan mengevaluasi protokol keamanan untuk menentukan kekuatan dan kelemahan dalam konteks keamanan sistem informasi (C4) |
| | **CPMK - 3** | Mengembangkan solusi kriptografi yang inovatif untuk meningkatkan keamanan data dan transaksi dalam jaringan (C6) |
| | **CPMK - 4** | Mengevaluasi implementasi keamanan jaringan dalam studi kasus nyata untuk mengidentifikasi area perbaikan dan penerapan strategi keamanan yang lebih efektif (C5) |
| | **CPMK - 5** | Menerapkan teknik kriptografi modern dalam pengembangan aplikasi yang aman dan memenuhi standar keamanan yang ditetapkan (C3) |
| | **CPMK - 6** | Menganalisis kebutuhan keamanan informasi organisasi dan merancang arsitektur jaringan yang sesuai untuk memenuhi kebutuhan tersebut (C4) |
| | **CPMK - 7** | Menciptakan metode baru dalam deteksi dan pencegahan intrusi menggunakan teknologi terkini (C6) |
| | **CPMK - 8** | Mengevaluasi efektivitas berbagai algoritma kriptografi dalam konteks kebutuhan spesifik organisasi dan membuat rekomendasi berdasarkan analisis tersebut (C5) |
| | **CPMK - 9** | Menerapkan dan mengintegrasikan solusi keamanan berlapis untuk melindungi infrastruktur TI dari serangan siber (C3) |
| | **CPMK - 10** | Menganalisis dan merespon secara efektif terhadap insiden keamanan dengan menggunakan prinsip forensik digital (C4) |
| | **Matrik CPL - CPMK** | |

| CPMK | CPL-3 | CPL-5 | CPL-7 | CPL-8 | CPL-9 |
|---|---|---|---|---|---|
| CPMK-1 | ✔ | ✔ | | | |
| CPMK-2 | | | ✔ | ✔ | |
| CPMK-3 | | ✔ | | | ✔ |
| CPMK-4 | | | ✔ | ✔ | |
| CPMK-5 | ✔ | ✔ | | | |
| CPMK-6 | | | ✔ | | ✔ |
| CPMK-7 | | ✔ | | | ✔ |
| CPMK-8 | | | ✔ | ✔ | |
| CPMK-9 | ✔ | | | | ✔ |
| CPMK-10 | | | ✔ | ✔ | |

**Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)**

| CPMK | Minggu Ke | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| CPMK-1 | ✔ | ✔ | | | | | | | | | | | | | | |
| CPMK-2 | | | ✔ | | | | | | | | | | | | | |
| CPMK-3 | | | | | | | | | | | | ✔ | | | | |
| CPMK-4 | | | | | | | | | | | | | ✔ | ✔ | ✔ | |
| CPMK-5 | | | | ✔ | | | | | | ✔ | | | | | | |
| CPMK-6 | | | | | ✔ | | | | | | | | | | | |
| CPMK-7 | | | | | | | ✔ | | | | | | | | | |
| CPMK-8 | | | | | | ✔ | | | | | | | | | | |
| CPMK-9 | | | | | | | | | ✔ | | | | | | | |
| CPMK-10 | | | | | | | | ✔ | | | ✔ | | | | | |

| | |
|---|---|
| **Deskripsi Singkat MK** | Matakuliah Keamanan Jaringan dan Kriptografi pada jenjang S2 program studi Informatika bertujuan untuk memberikan pemahaman mendalam dan terintegrasi tentang konsep, teknik, dan implementasi keamanan jaringan serta kriptografi. Mahasiswa akan mempelajari teknik-teknik perlindungan jaringan komputer, analisis risiko, protokol keamanan, serta implementasi enkripsi dan dekripsi untuk melindungi informasi dalam sistem komputer. Selain itu, mata kuliah ini juga mencakup pembahasan tentang pengembangan strategi keamanan berbasis teknologi terbaru dan penerapan kriptografi dalam berbagai konteks industri dan penelitian. Dengan memadukan teori dan praktik, mata kuliah ini mendukung pengembangan kemampuan analitis dan inovatif mahasiswa dalam menyelesaikan tantangan keamanan di era transformasi digital. |
| **Pustaka** | **Utama :** |
| | 1. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.<br>2. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley. |
| | **Pendukung :** |
| **Dosen Pengampu** | Dr. Ir. Ricky Eka Putra, S.Kom., M.Kom. |

| Mg Ke- | Kemampuan akhir tiap tahapan belajar (Sub-CPMK) | Penilaian | | Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [ Estimasi Waktu] | | Materi Pembelajaran [ Pustaka ] | Bobot Penilaian (%) |
|---|---|---|---|---|---|---|---|
| | | Indikator | Kriteria & Bentuk | Luring (*offline*) | Daring (*online*) | | |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
| 1 | Mahasiswa mampu menjelaskan konsep dasar keamanan jaringan dan kriptografi | 1.Ketepatan menjelaskan konsep dasar keamanan jaringan<br>2.Penerapan kriptografi dalam jaringan<br>3.Kemampuan menjelaskan prinsip keamanan dalam pengelolaan jaringan | **Kriteria:** Kejelasan dan kelengkapan penjelasan<br><br>**Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk | Pembelajaran aktif melalui diskusi kelompok dan proyek<br>2 x 50 | Diskusi daring tentang penerapan kriptografi dalam keamanan jaringan<br>1 x 50 | **Materi:** Pengenalan Keamanan Jaringan, Prinsip-prinsip Kriptografi, Penerapan Keamanan dalam Jaringan<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Pengantar Keamanan Jaringan<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.*<br><br>**Materi:** Dasar-dasar Kriptografi<br>**Pustaka:** *Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **2** | Mahasiswa mampu mengidentifikasi ancaman dan risiko keamanan pada jaringan komputer | 1. konsep dasar keamanan jaringan dipahami<br>2. teknik kriptografi diterapkan dengan benar<br>3. implementasi keamanan jaringan dilakukan secara tepat<br>4. Ketepatan identifikasi ancaman dan risiko. | **Kriteria:**<br>Kemampuan menghubungkan ancaman dengan potensi dampaknya.<br><br>**Bentuk Penilaian** :<br>Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk | Pembelajaran aktif melalui diskusi dan proyek<br>2 x 50 | Penugasan online memungkinkan, Tugas online: Implementasikan teknik kriptografi pada sebuah simulasi jaringan yang diberikan. Laporkan hasil analisis keamanan yang Anda lakukan.<br>1 x 50 | **Materi:** Konsep dasar keamanan jaringan, Teknik kriptografi, Implementasi keamanan jaringan<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Ancaman dan Serangan Jaringan<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **3** | Mahasiswa mampu mengevaluasi protokol keamanan jaringan untuk menentukan kelemahan dan kekuatannya | 1. Ketepatan analisis protokol keamanan dilakukan dengan mendalam<br>2. Mampu mengidentifikasi kekuatan dan kelemahan protokol<br>3. Rekomendasi perbaikan disusun secara jelas | **Kriteria:**<br>Kelengkapan evaluasi kelemahan dan kekuatan<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran aktif melalui diskusi kelompok dan proyek<br>2 x 50 | Diskusi dan presentasi daring tentang analisis protokol keamanan dengan proyek tertentu<br>1 x 50 | **Materi:** Pengenalan protokol keamanan, Metode analisis protokol keamanan, Teknik evaluasi kekuatan dan kelemahan<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Protokol Keamanan Jaringan<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **4** | Mahasiswa mampu menerapkan teknik enkripsi dasar dalam simulasi jaringan sederhana | 1. Kemampuan merancang solusi kriptografi inovatif<br>2. Kemampuan mengimplementasikan teknik kriptografi dengan baik<br>3. Ketepatan implementasi teknik enkripsi | **Kriteria:**<br>Kepatuhan terhadap prosedur enkripsi<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran berbasis proyek<br>2 x 50 | Pengembangan solusi kriptografi inovatif untuk proyek tertentu<br>1 x 50 | **Materi:** Konsep kriptografi modern, Algoritma kriptografi terkini, Implementasi kriptografi dalam jaringan<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Teknik Enkripsi<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **5** | Mahasiswa mampu merancang arsitektur jaringan yang aman berdasarkan analisis kebutuhan keamanan informasi | 1. Analisis implementasi keamanan jaringan<br>2. Identifikasi area perbaikan<br>3. Ketepatan perancangan strategi keamanan efektif<br>4. Ketepatan rancangan arsitektur jaringan. | **Kriteria:**<br>Relevansi rancangan dengan kebutuhan keamanan<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran Berbasis Proyek<br>2 x 50 | Diskusi daring tentang implementasi keamanan jaringan dalam kehidupan nyata<br>1 x 50 | **Materi:** Studi Kasus Implementasi Keamanan Jaringan, Evaluasi Keamanan Jaringan, Perancangan Strategi Keamanan<br>**Pustaka:**<br>*Handbook Perkuliahan*<br><br>**Materi:**<br>Arsitektur Keamanan Jaringan<br>**Pustaka:**<br>*Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **6** | Mahasiswa mampu mengevaluasi algoritma kriptografi modern untuk aplikasi tertentu | 1. Penerapan teknik kriptografi modern dalam pengembangan aplikasi<br>2. Kemampuan memilih teknik kriptografi yang sesuai dengan standar keamanan<br>3. Kemampuan mengimplementasikan teknik kriptografi dalam aplikasi<br>4. Kelengkapan evaluasi algoritma kriptografi | **Kriteria:**<br>Ketepatan analisis relevansi algoritma dengan aplikasinya<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran berbasis proyek<br>2 x 50 | Penugasan proyek pengembangan aplikasi dengan menerapkan teknik kriptografi modern<br>1 x 50 | **Materi:**<br>Konsep dasar kriptografi modern, Algoritma kriptografi simetris dan asimetris, Implementasi kriptografi dalam aplikasi<br>**Pustaka:**<br>*Handbook Perkuliahan*<br><br>**Materi:**<br>Algoritma Kriptografi Modern<br>**Pustaka:**<br>*Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **7** | Mahasiswa mampu mengembangkan teknologi deteksi intrusi dengan menggunakan perangkat lunak terkini | 1. Penerapan teknik kriptografi modern dalam pengembangan aplikasi<br>2. Kemampuan memilih teknik kriptografi yang sesuai<br>3. Kemampuan mengimplementasikan standar keamanan<br>4. Ketepatan implementasi teknologi deteksi intrusi | **Kriteria:**<br>Efektivitas solusi deteksi intrusi yang diusulkan<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran berbasis proyek<br>2 x 50 | Pengembangan aplikasi keamanan dengan teknik kriptografi<br>1 x 50 | **Materi:**<br>Konsep dasar kriptografi modern, Algoritma kriptografi simetris dan asimetris, Implementasi kriptografi pada aplikasi, Standar keamanan dalam pengembangan aplikasi<br>**Pustaka:**<br>*Handbook Perkuliahan*<br><br>**Materi:** Sistem Deteksi Intrusi<br>**Pustaka:**<br>*Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **8** | Mampu menjelaskan dengan lebih baik materi-materi dari minggu ke-1 s.d. ke-7 | 1. Menerapkan konsep yang telah dipelajari<br>2. Mengalisis dan memecahkan masalah<br>3. Menjawab soal esai dan studi kasus | **Kriteria:**<br>1. Kedalaman jawaban<br>2. Kejelasan analisis<br>3. Ketepatan solusi<br><br>**Bentuk Penilaian** :<br>Tes | Menyelesaikan soal ujian Sub-Sumatif<br>3 x 50 | | **Materi:** Materi-materi dari minggu ke-1 s.d. ke-7<br>**Pustaka:**<br>*Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.*<br><br>**Materi:** Materi-materi dari minggu ke-1 s.d. ke-7<br>**Pustaka:**<br>*Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 15% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **9** | Mahasiswa mampu menyusun strategi keamanan jaringan berbasis proyek tertentu | 1. Analisis kebutuhan keamanan informasi organisasi<br>2. Rancangan arsitektur jaringan yang sesuai<br>3. Ketepatan strategi yang disusun | **Kriteria:**<br>Relevansi strategi dengan permasalahan di proyek<br><br>**Bentuk Penilaian** :<br>Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk | Pembelajaran berbasis proyek<br>2 x 50 | Penugasan proyek online<br>1 x 50 | **Materi:**<br>Konsep keamanan informasi, Kebutuhan keamanan organisasi, Arsitektur jaringan yang sesuai<br>**Pustaka:**<br>*Handbook Perkuliahan*<br><br>**Materi:**<br>Strategi Keamanan Jaringan<br>**Pustaka:**<br>*Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |
| **10** | Mahasiswa mampu menerapkan teknik enkripsi lanjutan untuk aplikasi tertentu | 1. Kemampuan mengidentifikasi celah keamanan<br>2. Kemampuan mengembangkan solusi deteksi intrusi<br>3. Kemampuan menguji keefektifan solusi<br>4. Ketepatan menerapkan teknik enkripsi | **Kriteria:**<br>Relevansi teknik enkripsi dengan kebutuhan aplikasi<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran Berbasis Proyek<br>2. x 50 | Diskusi daring tentang solusi deteksi intrusi yang diusulkan<br>1 x 50 | **Materi:**<br>Pengenalan Teknologi Terkini dalam Keamanan Jaringan, Metode Deteksi Intrusi yang Umum Digunakan, Penerapan Teknologi Terkini dalam Pencegahan Intrusi<br>**Pustaka:**<br>*Handbook Perkuliahan*<br><br>**Materi:** Teknik Enkripsi Lanjutan<br>**Pustaka:**<br>*Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **11** | Mahasiswa mampu menganalisis dan merespon insiden keamanan menggunakan prinsip forensik digital | 1. Kemampuan menciptakan metode baru dalam deteksi dan pencegahan intrusi<br>2. Penerapan teknologi terkini dalam keamanan jaringan<br>3. Ketepatan analisis insiden | **Kriteria:**<br>Kelengkapan respons terhadap insiden keamanan<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio | Pembelajaran Berbasis Proyek<br>2 x 50 | Forum diskusi dan Penugasan Proyek<br>1 x 50 | **Materi:** Pengenalan Teknologi Terkini dalam Keamanan Jaringan, Metode Deteksi Intrusi, Strategi Pencegahan Intrusi<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Forensik Digital dalam Keamanan Jaringan<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **12** | Mahasiswa mampu mengembangkan solusi kriptografi inovatif untuk meningkatkan keamanan data dalam jaringan | 1. Kemampuan menganalisis kebutuhan organisasi<br>2. Kemampuan mengevaluasi efektivitas algoritma kriptografi<br>3. Kemampuan memberikan rekomendasi berdasarkan analisis<br>4. Kreativitas solusi yang dikembangkan | **Kriteria:**<br>Relevansi solusi terhadap kebutuhan keamanan data<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio | Pembelajaran berbasis proyek<br>2 x 50 | Forum diiskusi dan penugasan penilaian hasil proyek<br>1 x 50 | **Materi:** Pengenalan algoritma kriptografi, Analisis kebutuhan organisasi, Metode evaluasi algoritma kriptografi, Pembuatan rekomendasi berdasarkan analisis<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Solusi Kriptografi untuk Keamanan Data<br>**Pustaka:** *Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **13** | Mahasiswa mampu membuat laporan evaluasi keamanan jaringan yang terstruktur dan informatif | 1. Integrasi lapisan keamanan<br>2. Pemahaman solusi keamanan berlapis<br>3. Kemampuan menerapkan solusi keamanan<br>4. Kelengkapan laporan evaluasi | **Kriteria:**<br>Kejelasan penyajian data dan rekomendasi<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran Berbasis Proyek<br>2 x 50 | Diskusi daring tentang implementasi solusi keamanan berlapis, Analisis kasus keamanan berlapis, dan Tugas daring<br>1 x 50 | **Materi:** Konsep keamanan berlapis, Teknik integrasi solusi keamanan, Studi kasus implementasi<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Laporan Evaluasi Keamanan Jaringan<br>**Pustaka:** *Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |
| **14** | Mahasiswa mampu merevisi rancangan keamanan berdasarkan umpan balik | 1. Pemahaman konsep keamanan berlapis<br>2. Kemampuan mengidentifikasi potensi serangan siber<br>3. Kemampuan merancang solusi keamanan yang efektif<br>4. Ketepatan revisi rancangan | **Kriteria:**<br>Perbaikan yang relevan dengan umpan balik<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk | Pembelajaran Berbasis Proyek<br>2 x 50 | Forum Diskusi dan Penugasan Proyek Online<br>1 x 50 | **Materi:** Konsep keamanan berlapis, Teknik identifikasi serangan siber, Desain solusi keamanan berlapis<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Revisi Sistem Keamanan<br>**Pustaka:** *Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.* | 5% |
| **15** | Mahasiswa mampu menyusun laporan akhir proyek keamanan jaringan dan kriptografi | 1. Mampu mengidentifikasi jejak digital yang relevan<br>2. Mampu menerapkan prinsip forensik digital dalam analisis insiden keamanan<br>3. Mampu menyusun laporan forensik digital yang komprehensif<br>4. Kelengkapan laporan akhir | **Kriteria:**<br>Kesesuaian dengan standar penulisan akademik<br><br>**Bentuk Penilaian** :<br>Penilaian Hasil Project / Penilaian Produk, Penilaian Portofolio | Pembelajaran berbasis proyek<br>2 x 50 | Penugasan Analisis Kasus Forensik Digital<br>1 x 50 | **Materi:** Pengenalan Forensik Digital, Proses Analisis Forensik Digital, Penyusunan Laporan Forensik Digital<br>**Pustaka:** *Handbook Perkuliahan*<br><br>**Materi:** Penyusunan Laporan Proyek Keamanan Jaringan<br>**Pustaka:** *Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **16** | Mampu menjelaskan dengan lebih baik materi-materi dari minggu ke-9 s.d. ke-15 | Mengintegrasikan seluruh materi Keamanan Jaringan dan Kriptografi yang telah dipelajari dalam mata kuliah | **Kriteria:**<br>Kemampuan menyelesaikan soal terkait semua CPMK<br><br>**Bentuk Penilaian** :<br>Tes | Menyelesaikan soal Ujian Sumatif<br>3 x 50 | | **Materi:** Materi-materi dari minggu ke-9 s.d. ke-15<br>**Pustaka:**<br>*Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.*<br><br>**Materi:** Materi-materi dari minggu ke-9 s.d. ke-15<br>**Pustaka:**<br>*Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.* | 15% |

**Rekap Persentase Evaluasi : Project Based Learning**

| No | Evaluasi | Persentase |
|---|---|---|
| 1. | Aktifitas Partisipasif | 7.5% |
| 2. | Penilaian Hasil Project / Penilaian Produk | 55% |
| 3. | Penilaian Portofolio | 7.5% |
| 4. | Tes | 30% |
| | | 100% |

**Catatan**

1. **Capaian Pembelajaran Lulusan Prodi (CPL - Prodi)** adalah kemampuan yang dimiliki oleh setiap lulusan prodi yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. **CPL yang dibebankan pada mata kuliah** adalah beberapa capaian pembelajaran lulusan program studi (CPL-Prodi) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. **CP Mata kuliah (CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. **Sub-CPMK Mata kuliah (Sub-CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. **Indikator penilaian** kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. **Kreteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. **Bentuk penilaian:** tes dan non-tes.
8. **Bentuk pembelajaran:** Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
9. **Metode Pembelajaran:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
10. **Materi Pembelajaran** adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. **Bobot penilaian** adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
12. TM=Tatap Muka, PT=Penugasan terstruktur, BM=Belajar mandiri.

RPS ini telah divalidasi pada tanggal 3 Februari 2025

Koordinator Program Studi S2
Informatika

RICKY EKA PUTRA
NIDN 0716018704

**UPM** Program Studi S2
Informatika

NIDN 0024118405

File PDF ini digenerate pada tanggal 8 Desember 2025 Jam 13:33 menggunakan aplikasi RPS-OBE SiDia Unesa