|  |
| --- |
| logo UEU kecil |
| **RENCANA PEMBELAJARAN SEMESTER GANJIL 2017/2018** |
| **PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS ILMU KOMPUTER** |
| **UNIVERSITAS ESA UNGGUL** |
|  |
| **Mata Kuliah** | **:** | Cryptography | **Kode MK** | **:** |  |
| **Mata Kuliah Prasyarat** | **:** | - | **Bobot MK** | **:** | 3 sks |
| **Dosen Pengampu** | **:** | Agung Mulyo Widodo, ST,MSc,; Drs. Holder Simorangkir,MT. | **Kode Dosen** | **:** | 6592 |
| **Alokasi Waktu** | **:** | Tatap muka 14 x 100 menit, praktik 14 x 100 menit, ada online |
| **Capaian Pembelajaran** | **:** | 1. Mahasiswa mampu memahami dan mengerti konsep dasar crytogrpahy
2. Mahasiswa mampu memahami dan mengerti konsep DES dan AES
3. Mahasiswa mampu memahami dan mengerti konsep public-key cryptography
4. Mahasiswa mampu memahami dan mengerti konsep primality testing
5. Mahasiswa mampu memahami dan mengerti konsep electronic mail dan internet security
 |
|  |  |  |
| **SESI** | **KEMAMPUAN****AKHIR** | **MATERI** **PEMBELAJARAN** | **BENTUK PEMBELAJARAN** | **SUMBER** **PEMBELAJARAN** | **INDIKATOR****PENILAIAN** |
| 1 | Mahasiswa mampu menguasai konsep dasar cryptography  | Pengantar :Kontrak pembelajaran, masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik, Algoritma Blok Cipher dan Stream Cipher  | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguasai dan menguraikan pengertian masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik dengan benar dan mampu menyelesaikan soal-soal yang terkait dengannya. |
| 2 | Mahasiswa mampu menguasai konsep enkripsi dan dekripsi | Terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptography yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan  | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguraikan Terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptograhy yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan dengan benar dan mampu menyelesaikan soal-soal yang terkait dengannya |
| 3 | Mahasiswa mampu menguasai konsep algoritma cryptography modern | Pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguraikan pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik dengan benar dan mampu menyelesaikan soal-soal yang terkait dengannya. |
| 4 | Mahasiswa mampu menguasai konsep data encryption standard (DES) | Pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR)  | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR) dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya |
| 5 | Mahasiswa mampu menguasai konsep advanced encryption standard (AES) | Pengertian dan konsep AES , cara kerja AES | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan pengertian dan konsep AES , cara kerja AES dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 6 | Mahasiswa mampu menguasai konsep dan pengertian algoritma RSA | Pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan daan keamana RSA  | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Menguraikan Pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan daan keamana RSA dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 7 | Mahasiswa mampu menguasai review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA | QUIZ 1 | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Latihan soal-soal
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan menguasai review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya |
| 8 | Mahasiswa mampu menguasai pengertian dan konsep algoritmaMessage digest 5 (MD5) | Pengertian dan konsep algoritma MD5 | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan pengertian dan konsep algoritma MD5dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 9 | Mahasiswa mampu menguasai konsep Double DES dan Triple DES | DES Overview, konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryption | 1. Metoda *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryptiondengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 10 | Mahasiswa mampu menguasai konsep fungsi hash dalam cryptography | Pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah. | 1. Metoda : *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mengerti dan mampu menguraikan Pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah.dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 11 | Mahasiswa mampu menguasai konsep digital signature | Pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing | 1. Metoda : *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C. Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguasai dan menguraikan , pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya. |
| 12 | Mahasiswa mampu menguasai konsep algoritma Number Theory  | Pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testing | 1. Metoda : *contextual instruction*
2. Media : : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C.Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguasai dan menguraikan , Pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testing dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya.menyelesaikan soal-soal yang berkaitan dengannya |
| 13 | Mahasiswa mampu menguasai konsep electronic mail dan keamanan | Pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites  | 1. Metoda : *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Pratikum
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C.Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”, 2009
 | Mampu menguasai dan menguraikan , pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya |
| 14 | Mahasiswa mampu menguasai konsep algoritma Message digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan | QUIZ 2 | 1. Metoda : *contextual instruction*
2. Media : kelas, komputer, *LCD, whiteboard.*
3. Latihan soal-soal
 | 1. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, 1996.
2. HCA van tilborg, “ Fundamentals of cryptography”, Kluwer academic publisher.
3. C.Paar,J.Pelzl,”Understanding Cryptography-Textbook for Student and Practitioners”,
 | Mampu menguasai menguraikan , konsep cryptography melalui review konsep algoritmaMessage digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan dengan benar dan mampu menyelesaikan soal-soal yang berkaitan dengannya.menyelesaikan soal-soal yang berkaitan dengannya |

**EVALUASI PEMBELAJARAN**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SESI** | **PROSE-DUR** | **BENTUK** | **SEKOR > 77** **( A / A-)** | **SEKOR > 65****(B- / B / B+ )** | **SEKOR > 60****(C / C+ )** | **SEKOR > 45****( D )** | **SEKOR < 45****( E )** | **BOBOT** |
| 1 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik, Algoritma Blok Cipher dan Stream Cipher dengan cara dan jawaban yang benar.  | Mampu menyelesaikan soal-soal yang berkaitan dengan masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik, Algoritma Blok Cipher dan Stream Cipher dengan caranya yang benar akan tetapi jawaban yang salah  | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik, Algoritma Blok Cipher dan Stream Cipher | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan masalah ancaman dan aspek keamanan , konsep cryptography, crytoanalysis dan cryptologi, fakta sejarah cryptography, pengertian algoritm simetrik dan asimetrik, Algoritma Blok Cipher dan Stream Cipher yang di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 2 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptography yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptography yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan pengertian terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptography yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan yang di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian Terminologi enkripsi, proses enkripsi, algoritma cryptography klasik, teknik dasar cryptography yakni subtitusi, blocking,permutasi, ekspansi dan pemampatan yang di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 3 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan Pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian algoritma cryptography modern, penggunaan kunci, algoritma simetrik dan algoritma asimetrik yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 4 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR) dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR) dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR) yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan Pengertian DES, cara kerja DES, mode DES : Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter Mode (CTR)  yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 5 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian dan konsep AES , cara kerja AES dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian dan konsep AES , cara kerja AES dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian dan konsep AES , cara kerja AES yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian dan konsep AES , cara kerja AES yang telah di berikan | Tidak mengerjakan soal yang diberikan | 0 %5 % |
| 6 | *Post test* | 1. Tes tulisan (UTS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan Pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan daan keamanan RSA dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan Pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan daan keamanan RSA dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan dan keamanan RSA yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian dan konsep RSA, cara kerja algoritma RSA, Kekuatan daan keamanan RSA yang telah di berikan | Tidak mengerjakan soal yang diberikan | 0 %5 % |
| 7 | *Post test* | 1. QUIZ 1
2. Tes tulisan (UTS)
 | Mampu menyelesaikan soal-soal yang berkaitan dengan review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan review konsep cryptography, enkripsi dan dekripsi, algoritm cryptography moder, DES, AES dan RSA yang telah di berikan | Tidak mengerjakan soal yang diberikan | 10 %35 % |
| 8 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian dan konsep algoritma MD5 dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan Pengertian dan konsep algoritma MD5dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian dan konsep algoritma MD5 yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian dan konsep algoritma MD5 yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 9 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan DES Overview, konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryptiondengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan DES Overview, konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryptiondengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan DES Overview, konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryptionyang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan DES Overview, konsep Double DES, Triple DES with 2-key encryption, Triple DES with 3-key encryptionyang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 10 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah.dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah. dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah. yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian, fungsi hash, kegunaan, penguji keutuhan pesan, fungsi hash satu arah, dan aplikasi fungsi hash satu arah. yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 11 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan konsep Pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian digital signature, mekanisme digital signature, prosedur iging, verifikasi signing yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 12 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testing dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testingdengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testingyang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian GCD, Multiplicative Inverse,Fermat & Euler’s Theorems, Public Key Cryptographic Systems,Primality Testingyang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 13 | *Post test* | 1. Tes tulisan (UAS)
2. Pratikum
 | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan pengertian, dan konsep Pretty Good Privacy, S/MIME, Recommended web sites yang telah di berikan | Tidak mengerjakan soal yang diberikan | 5 % |
| 14 | *Post test* | 1. QUIZ 2
2. Tes tulisan (UAS)
 | Mampu menyelesaikan soal-soal yang berkaitan dengan review konsep algoritma Message digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan dengan cara dan jawaban yang benar | Mampu menyelesaikan soal-soal yang berkaitan dengan review konsep algoritma Message digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan dengan caranya yang benar akan tetapi jawaban yang salah | Hanya mampu menyelesaikan soal yang di berikan dengan cara yang salah, akan tetapi masih berhubungan dengan review konsep algoritma Message digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan yang telah di berikan | Mampu menyelesakan soal yang diberikan dengan cara yang salah, dan tidak berhubungan dengan review konsep algoritma Message digest 5 (MD5), doble DES dan Triple DES, Fungsi Hash, digital signature, algoritma Number Theory dan electronic mail dan keamanan yang telah di berikan | Tidak mengerjakan soal yang diberikan | 10 %35 % |

**Komponen penilaian :**

1. Kehadiran = 10 %
2. QUIZ = 20 %
3. UTS = 35%
4. UAS = 35 %

**Jakarta, 3 Juli 2017**

**Mengetahui,**

**Ketua Program Studi, Dosen Pengampu,**

**Bambang Irawan,SKom,MKom Agung Mulyo Widodo,ST,MSc. Drs. Holder Simorangkir, MT.**