Skedul Rencana Kuliah IF4020 Kriptografi
Semester 1 Tahun 2021/2022

Dosen: Rinaldi Munir

Minggu ke-	Materi	Waktu	Keterangan
1	Pengantar kriptografi a)Landasan matematika untuk kriptografi b)Kriptografi klasik	23 Agustus 2021 25 Agustus 2021	
2	Kriptografi klasik (lanjutan) a)One-time pad b)Serangan pada kriptografi	30 Agustus 2021 1 September 2021	Tugas program 1
3	Kriptanalisis sederhana Kriptanalisis sederhana (lanjutan)	6 September 2021 8 September 2021	 Tugas 2 (kriptanalisis)
4	Steganografi a)Steganografi (lanjutan) b)Watermarking	13 September 2021 15 September 2021	Tugas program 3
5	Kriptografi modern – stream cipher dan block cipher a)Kriptografi modern – lanjutan block cipher b)Review beberapa algoritma kriptografi kunci-simetri (DES dan GOST)	20 September 2021 22 September 2021	
6	Review beberapa algoritma kriptografi kunci-simetri (Triple DES, RC5) a)Review beberapa algoritma kriptografi kunci-simetri (RC4, A5) b)Advanced Encryption Standard (AES)	27 September 2021 29 September 2021	

7	Kriptografi kunci nir-simetri / kriptografi kunci-publik Review beberapa algoritma kriptografi kunci-publik (RSA, Diffie-Hellman)	4 Oktober 2021 6 Oktober 2021	
8	**UTS**	**11 – 15 Oktober 2021**	
9	Review beberapa algoritma kriptografi kunci-publik (ElGamal, knapsack) Elliptic Curve Cryptography (ECC)	18 Oktober 2021 20 Oktober 2021	Tugas program 4
10	Fungsi hash Review beberapa fungsi hash (MD5, SHA-1)	25 Oktober 2021 27 Oktober 2021	
11	SHA-3 a)MAC b)Tanda-tangan digital c) DSA	1 November 2021 3 November 2021	Tugas program 5
12	Pembangkit bilangan acak Protokol kriptografi	8 November 2021 10 November 2021	
13	Sertifikat digital Public Key Infrastructure (PKI)	15 November 2021 17 November 2021	
14	Enkripsi homomorfik Manajemen kunci	22 November 2021 24 November 2021	
15	Kriptogafi visual	29 November 2021	

	Kripografi visual	1 Desember 2021	
16	UAS	6 – 21 Desember 2021	Tugas makalah penggani UAS