

Skedul Rencana Kuliah IF4020 Kriptografi Semester II Tahun 2022/2023

Dosen: Rinaldi Munir

Minggu ke-	Materi	Waktu	Keterangan
1	a) Perkenalan kuliah b) Pengantar kriptografi	16 Januari 2023	
	c) Ragam cipher klasik	18 Januari 2023	
2	a) Ragam cipher klasik (lanjutan) b) One-time pad c) Serangan pada kriptografi	23 Januari 2023	Tugas 1
	d) Kriptanalisis sederhana	25 Januari 2023	
3	a) Steganografi b) Steganalisis	30 Januari 2023	
	c) (No-stega) Noiseless-steganography	1 Februari 2023	
4	a) Digital watermarking b) Kriptografi modern: stream cipher c) Beberapa algoritma stream cipher	6 Februari 2023	Tugas 2
	a) Block cipher b) Beberapa algoritma block cipher	8 Februari 2023	
5	a) Beberapa algoritma block cipher (lanjutan)	13 Februari 2023	
	b) Beberapa algoritma block cipher (lanjutan)	15 Februari 2023	
6	a) Kriptografi nirsimetri (kriptografi kunci-publik)	20 Februari 2023	
	b) Beberapa algoritma kriptografi kunci-publik (lanjutan)	22 Februari 2023	

7	a) Beberapa algoritma kriptografi kunci-publik b) Review sebelum UTS	27 Februari 2023 1 Maret 2023	Tugas 3
8	UTS	6 – 10 Maret 2023	
9	a) Elliptic curve cryptography (ECC) b) Beberapa algoritma ECC	13 Maret 2023 15 Maret 2023	
10	a) Enkripsi homomorfik b) Fungsi hash	20 Maret 2023 22 Maret 2023	
11	a) Beberapa fungsi hash b) MAC	27 Maret 2023 29 Maret 2023	Tugas 4
12	a) Tanda-tangan digital b) DSA c) Protokol kriptografi	3 April 2023 5 April 2023	
13	a) Protokol kriptografi (lanjutan) b) Pembangkit bilangan acak c) Sertifikat digital	10 April 2023 12 April 2023	Tugas 5
14	a) Public Key Infrastructure (PKI) b) Skema pembagian secret	17 April 2023 19 April 2023	
15	Kriptografi visual	3 Mei 2023	Tugas Makalah
16	UAS	6 – 21 Desember 2021	