

## Skedul Materi Kuliah IF4020 Kriptografi Semester 2 Tahun 2023/2024

Dosen: Rinaldi Munir

Minggu ke-	Materi	Waktu	Keterangan
1	a) Pengantar kriptografi (1 jam) b) Ragam cipher klasik (1 jam)  <b>• Libur Isra' Mi'raj Nabi Muhammad SAW</b>	Selasa, 6 Februari 2024  <b>Kamis 8 Februari 2024</b>	<b>Tidak ada kuliah</b>
2	a) Ragam cipher klasik (lanjutan) b) One-time pad c) Serangan pada kriptografi  d) Kriptanalisis sederhana	Selasa, 13 Februari 2024  Kamis, 15 Februari 2024	Tugas 1
3	a) Steganografi (2 jam) b) Steganalisis c) No-stega  d) Digital watermarking	Selasa, 20 Februari 2023  Kamis, 22 Februari 2023	
4	a) Kriptografi modern: stream cipher b) Beberapa algoritma stream cipher  c) Block cipher d) Beberapa algoritma block cipher	Selasa, 27 Februari 2024  Kamis, 29 Februari 2024	
5	a) Beberapa algoritma block cipher (lanjutan)  b) Kriptografi nirsimetri (kriptografi kunci-publik)	Selasa, 5 Maret 2024  Kamis, 7 Maret 2024	
6	<b>a) Cuti bersama tahun baru Saka</b>	<b>Selasa, 12 Maret 2024</b>	<b>Tidak ada kuliah (Tucil 2 dirilis online via</b>

	a) Beberapa algoritma kriptografi kunci-publik (lanjutan)	Kamis, 14 Maret 2024	<b>WA/Teams/email dll. Tugil 2: divide &amp; conquer/decrease and conquer</b>
7	a) Elliptic curve cryptography (ECC) b) Beberapa algoritma ECC	Selasa, 19 Maret 2024 Kamis, 21 Maret 2024	
<b>8</b>	<b>UTS</b>	<b>25 Maret – 1 April 2024</b>	
9	a) Enkripsi homomorfik b) Fungsi hash	Selasa, 2 April 2024 Kamis, 4 April 2024	
10	a) Beberapa fungsi hash b) MAC	Selasa, 16 April 2024 Kamis, 18 April 2024	
11	a) Tanda-tangan digital b) DSA c) Protokol kriptografi	Selasa, 23 April 2024 Kamis, 25 April 2024	
12	a) Protokol kriptografi (lanjutan) b) Pembangkit bilangan acak c) Sertifikat digital dan PKI	Selasa, 30 April 2024 Kamis, 2 Mei 2024	
13	a) Skema pembagian secret	Selasa, 7 Mei 2024	

	<b>b) Libur</b>	<b>Kamis, 9 Mei 2024</b>	<b>Tidak ada kuliah</b>
14	a) Enkripsi homomorfik b) Kriptografi visual	Selasa, 14 Mei 2024 Kamis, 16 Mei 2024	
15	Kuliah tamu (tentatif)	Selasa 21 Mei 2024 <b>Kamis 23 Mei 2024</b>	Tidak ada kuliah
<b>16</b>	<b>UAS</b>	<b>8 – 23 Mei 2023</b>	