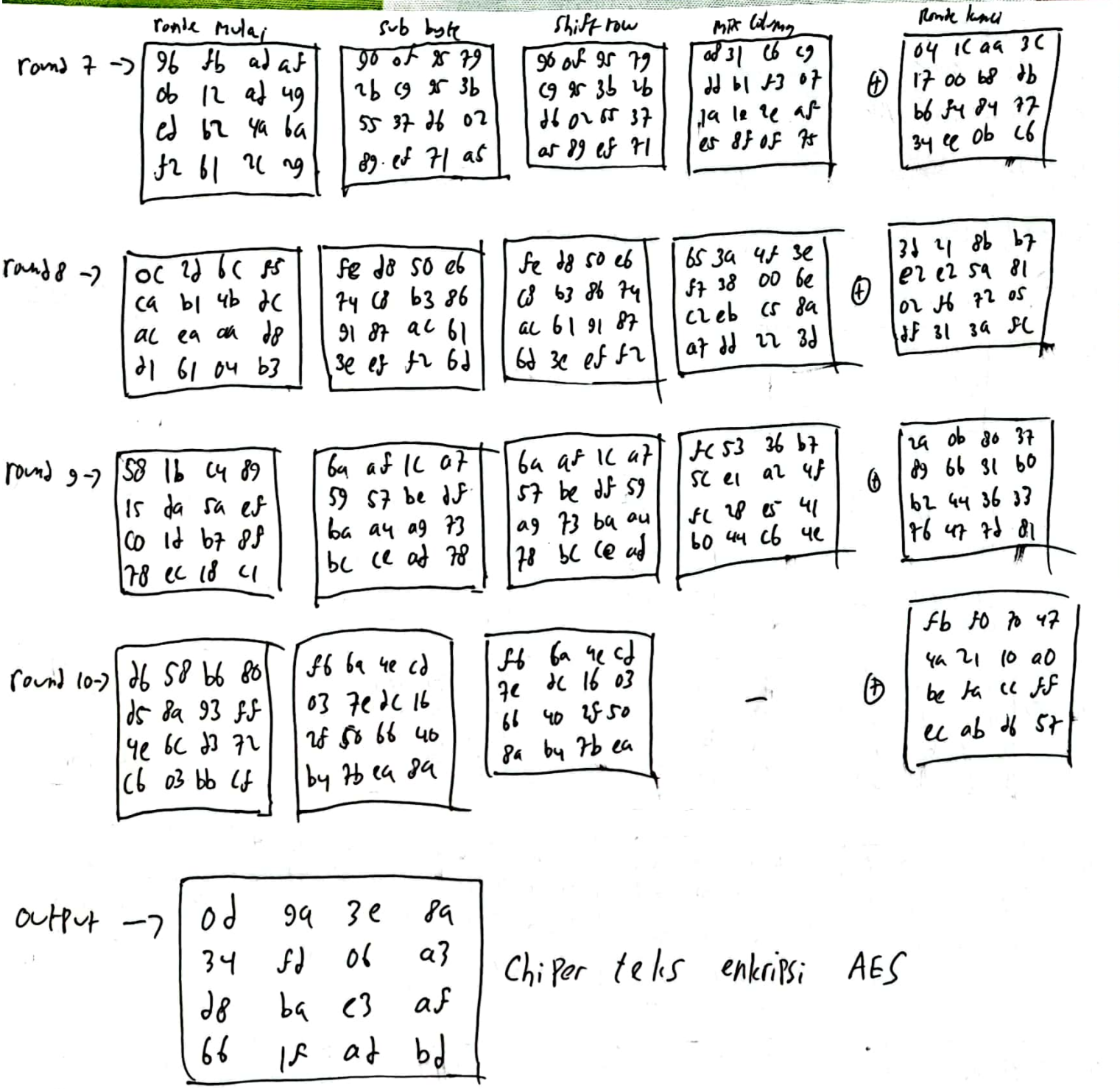
alan luthfi
0721 184000 0063
Tugas kriptografi AES

Plain teks = NIM => 000721 184000 0063

Key => kebalikan plain teks => 3600 000481127000

mulai

	ronde mulai	sub bytes	shift row	mix column	ronde key
input →	00 20 40 00 00 10 00 00 00 10 00 60 70 80 00 30	—	—	—	⊕ 30 00 80 70 60 00 10 00 00 00 10 00 00 40 20 00
round 1 →	30 20 C0 70 60 10 10 00 00 10 10 60 70 C0 20 30	04 b7 ba 51 d0 ca ca 63 63 ca ca d0 51 ba b7 04	04 b7 ba 51 ca ca 63 d0 ca d0 63 ca 04 51 ba b7	83 b1 13 b4 ca 02 63 10 4d 35 ca cc 04 7a ba 9c	⊕ 52 52 d2 a2 03 03 13 13 63 63 73 73 51 11 31 31
round 2 →	d1 e3 c1 16 c9 01 70 0b 2e 56 69 bf 55 66 86 ad	3e 11 78 47 dd 7c 51 2b 31 b1 56 08 fc 75 3d 95	3e 11 78 47 7c 51 2b dd 56 08 31 b1 95 fc 75 3d	3b 25 c3 7e a9 57 02 13 4a 4f b0 a4 59 89 6c 8f	⊕ 8d 7f ad 0f 8c 8f 9c 8f a4 c7 b4 c7 66 7a 46 7a
round 3 →	1b 5a 6e 71 25 d8 9e 9c ec 88 04 63 32 f3 27 a5	47 be 9f a3 3f 61 0b de 28 c4 f2 fb 23 0d cc 06	47 be 9f a3 61 0b de 3f f2 fb 28 c4 06 23 0d cc	d9 a2 79 14 8e 9d 4d 46 d3 3d 06 40 56 6f 56 86	⊕ 5a 25 88 87 4a c5 59 76 7e 69 0d ca 1d 67 2c 56
round 4 →	83 87 f1 93 c4 58 14 90 ad 84 0b 8a 46 08 7a d0	ec 17 a1 dc 1c ba fa 60 95 5f 26 7e b3 30 da 70	ec 17 a1 dc ba fa 60 1c 26 7e 95 5f 70 b3 30 da	26 f6 5c 02 35 c9 ff df 40 df a0 0b 8e c0 6d 93	⊕ a4 81 69 8e 3e fb a2 74 cf 76 7b b1 0a 6d 4 17
round 5 →	82 77 55 8c 0b 32 57 ab 8f a9 db ba 84 ad 2c 84	13 f5 fc 64 2b 23 5b 62 73 d3 b9 f4 5f 95 71 5f	13 f5 fc 64 23 5b 62 2b b9 f4 73 d3 5f 5f 95 71	a5 b7 a3 17 da 1b 38 2f b8 bc dc b1 11 15 3f b6	⊕ 26 a7 ae 20 f8 0d af db 3f 49 32 83 13 7e 3f 28
round 6 →	83 10 0d 37 2c 1b 97 f6 87 f5 ee e2 02 6b 00 9e	ec ca d7 9a 71 47 88 42 17 eb 28 98 77 7f 63 0b	ec ca d7 9a 47 88 42 71 28 98 17 eb 0b 77 7f 63	29 e3 1b 39 11 05 15 2a eb f0 3a 99 56 bb c9 e4	⊕ bf 18 b6 96 1a 17 b8 63 0b 42 70 f3 a4 da e5 cd



Chiper teks enkripsi AES