





$0 \leq i \leq N-1$   $N=3$   $\pi = (1 3 2)$   
 $Y = R_3 L_3$

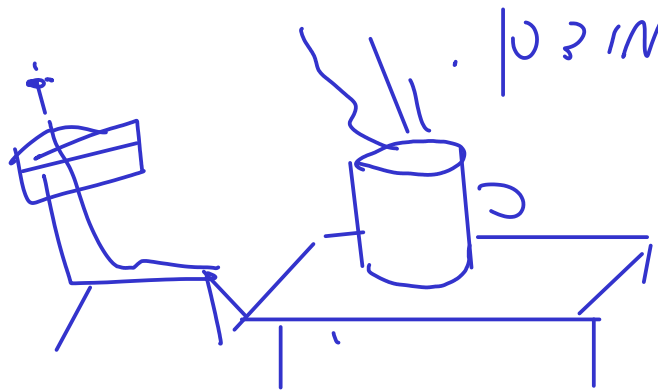
$X = 001011011$   $\pi = (1 3 2)$

$\pi = (1 3 2)$

$$f(X_1, X_2, X_3, X_4, X_5, \pi) = X_{\pi(1)} X_{\pi(2)} X_{\pi(3)} X_{\pi(4)} X_{\pi(5)}$$

$$\pi = (1 3 2)(4 5)$$

$$k_i = \pi^i$$



$\pi = (1 3 2)$

$\pi = (1 3 2)$

$N=3$

$$k_1 = \pi^1 = \pi$$

$$k_2 = \pi^2 = \pi \circ \pi \leftarrow \pi = (1 3 2)$$

$$2 \text{ de } i=3 \quad \pi^3 = \pi \circ \pi \circ \pi \leftarrow \text{מיון מלא} \quad \text{כל } i \in \{1, 2, 3, 4, 5\}$$

$$\pi = (135)(24) : \begin{array}{|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 \\ \hline \end{array}$$

מיון מלא - מיון מלא  $\pi$  מיון מלא

$i$	1	2	3	4	5
$\pi(i)$	3	4	5	2	<u>1</u>

"5"

$$(\#1) \rightarrow \begin{cases} \pi(1) = 3 \\ \pi(2) = 4 \\ \pi(3) = 5 \\ \pi(4) = 2 \\ \pi(5) = 1 \end{cases}$$

$$\underline{\pi^2(i) = \pi \circ \pi(i)} \quad i \in \{1, 2, 3, 4, 5\}$$

$$(\#2) \rightarrow \begin{cases} \pi^2(1) = \pi(\pi(1)) \stackrel{\#1}{=} \pi(3) = \underline{5} \\ \pi^2(2) = \pi(4) = 2 \\ \pi^2(3) = \pi(5) = \underline{1} \\ \pi^2(4) = \pi(2) = 4 \\ \pi^2(5) = \pi(1) = 3 \end{cases}$$

$$\pi^3(i) = \pi \circ \pi \circ \pi(i) \quad \text{if } \lambda \neq 1$$

$$\begin{array}{lclcl} \pi^3(1) = \pi(\pi^2(1)) \stackrel{\#2}{=} \pi(\underline{5}) \stackrel{\#1}{=} & 1 \\ \pi^3(2) = \pi(\pi^2(2)) \stackrel{\#2}{=} \pi(2) \stackrel{\#1}{=} & 4 \\ \pi^3(3) = \pi(\pi^2(3)) \stackrel{\#2}{=} \pi(1) \stackrel{\#1}{=} & 3 \\ \pi^3(4) = \pi(\pi^2(4)) \stackrel{\#2}{=} \pi(4) \stackrel{\#1}{=} & 2 \\ \pi^3(5) = \pi(\pi^2(5)) \stackrel{\#2}{=} \pi(3) \stackrel{\#1}{=} & 5 \end{array}$$

$i$	1	2	3	4	5
$\pi$	3	4	5	2	1
$\pi^2$	5	2	1	4	3
$\pi^3$	1	4	3	2	5

$$\kappa_1 = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} : / \circ \circ$$

$$| \tau_2 = \pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$k_3 = \tau_1^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

11103111 de p. 2 de 11 n. 10 8321 2 de 2

$x = 0010111011$   
 $\begin{array}{|l} L_0 \\ R_0 \end{array}$   
 $L_0 = 00101$        $R_0 = 11011$

for  $3 \leq n$  and  $i \geq 1$

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, k_i) \end{aligned}$$

←  $11011$   $11011$   $11011$   $11011$

$R_{i-1}$  and  $k_i$  are non-zero  $f(R_{i-1}, k_i)$

$i=1$  case

$$L_1 = R_0 = 11011$$

$$R_1 = L_0 \oplus f(R_0, k_1)$$

$$\text{for } k_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \quad R_0 = 11011 \quad \text{for}$$

$$R_0 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 0 & 1 & 1 \end{matrix}$$

$$f(R_0, k_1) = \begin{matrix} 3 & 4 & 5 & 2 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{matrix}$$

$$R_1 = L_0 \oplus f(R_0, k_1) = (00101) \oplus (01111) = 01010$$

$$L_1 = 11011$$

$$R_1 = 01010$$

$i=2$  case

$$L_2 = R_1$$

$$R_2 = L_1 \oplus f(R_1, k_2)$$

$$L_2 = 01010$$

1 2 3 4 5

$$R_1 = 01010$$

$$k_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$f(R_1, k_2) = \begin{matrix} & 5 & 2 & 1 & 4 & 3 \\ 0 & 1 & 0 & 1 & 0 \end{matrix}$$

$$R_2 = L_1 \oplus f(R_1, k_2) = (1011) \oplus (01010) = 10001$$

$$L_2 = 01010$$

$$R_2 = 10001$$

$$L_3 = R_2 = 10001$$

$$R_3 = L_2 \oplus f(R_2, k_3)$$

i=3    2 10

$$k_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

$$R_2 = \begin{matrix} & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 0 & 0 & 1 \end{matrix}$$

$$f(R_2, k_3) = \begin{matrix} & 1 & 4 & 3 & 2 & 5 \\ 1 & 0 & 0 & 0 & 1 \end{matrix}$$

$$R_3 = L_2 \oplus f(R_2, k_3) = 01010 \oplus 10001$$

$$= 11011$$

$$L_3 = 10001$$

$$R_3 = 11011$$

$$\gamma = R_3 L_3 = 1101110001$$

$$: \Delta' 010 \quad 11210 \quad \Delta$$

$\gamma = 1101110001$

$\frac{10^3 \text{ m}}{60 \times 60} \text{ min} = \underline{11.1 \text{ s}}$

$$k_1 = \pi$$

$N \wedge N \vee N \quad / \quad N \wedge N \vee \quad / \quad N \vee$

$$k_2 = \tau_1^2$$

$$l_2 = \tau_1^3$$

$$\pi = (1\ 3\ 5)(2\ 4) \quad \kappa = (1\ 2) \quad \lambda = (1\ 2\ 3\ 4\ 5) \quad \mu = (1\ 2\ 3\ 4) \quad \nu = (1\ 2\ 3\ 4\ 5)$$

• '18d 60/10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844,

$\therefore \int 60'' \, d$      $\int 13 \, d$      $\int e \, d$      $\int 1158 \, d$      $\int e \, d$      $\int 1 \, d$      $\int 10 \, d$      $\int 1 \, d$      $\int 1 \, d$

$$\begin{aligned} R_i &= L_{i+1} \\ L_i &= R_{i+1} \oplus f(R_i, \kappa_{i+1}) \end{aligned}$$

$$\int \rho \cdot \vec{r} \, dV \quad N = \int \rho \, dV \quad \vec{r} \cdot \vec{r} = r^2 \quad N = \int \rho \, dV \quad \vec{r} \cdot \vec{r} = r^2$$

1) 10, 2) 11, 3) 12, 4) 13, 5) 14, 6) 15, 7) 16, 8) 17, 9) 18, 10) 19, 11) 20, 12) 21, 13) 22, 14) 23, 15) 24, 16) 25, 17) 26, 18) 27, 19) 28, 20) 29, 21) 30, 22) 31, 23) 32, 24) 33, 25) 34, 26) 35, 27) 36, 28) 37, 29) 38, 30) 39, 31) 40, 32) 41, 33) 42, 34) 43, 35) 44, 36) 45, 37) 46, 38) 47, 39) 48, 40) 49, 41) 50, 42) 51, 43) 52, 44) 53, 45) 54, 46) 55, 47) 56, 48) 57, 49) 58, 50) 59, 51) 60, 52) 61, 53) 62, 54) 63, 55) 64, 56) 65, 57) 66, 58) 67, 59) 68, 60) 69, 61) 70, 62) 71, 63) 72, 64) 73, 65) 74, 66) 75, 67) 76, 68) 77, 69) 78, 70) 79, 71) 80, 72) 81, 73) 82, 74) 83, 75) 84, 76) 85, 77) 86, 78) 87, 79) 88, 80) 89, 81) 90, 82) 91, 83) 92, 84) 93, 85) 94, 86) 95, 87) 96, 88) 97, 89) 98, 90) 99, 91) 100, 92) 101, 93) 102, 94) 103, 95) 104, 96) 105, 97) 106, 98) 107, 99) 108, 100) 109, 101) 110, 102) 111, 103) 112, 104) 113, 105) 114, 106) 115, 107) 116, 108) 117, 109) 118, 110) 119, 111) 120, 112) 121, 113) 122, 114) 123, 115) 124, 116) 125, 117) 126, 118) 127, 119) 128, 120) 129, 121) 130, 122) 131, 123) 132, 124) 133, 125) 134, 126) 135, 127) 136, 128) 137, 129) 138, 130) 139, 131) 140, 132) 141, 133) 142, 134) 143, 135) 144, 136) 145, 137) 146, 138) 147, 139) 148, 140) 149, 141) 150, 142) 151, 143) 152, 144) 153, 145) 154, 146) 155, 147) 156, 148) 157, 149) 158, 150) 159, 151) 160, 152) 161, 153) 162, 154) 163, 155) 164, 156) 165, 157) 166, 158) 167, 159) 168, 160) 169, 161) 170, 162) 171, 163) 172, 164) 173, 165) 174, 166) 175, 167) 176, 168) 177, 169) 178, 170) 179, 171) 180, 172) 181, 173) 182, 174) 183, 175) 184, 176) 185, 177) 186, 178) 187, 179) 188, 180) 189, 181) 190, 182) 191, 183) 192, 184) 193, 185) 194, 186) 195, 187) 196, 188) 197, 189) 198, 190) 199, 191) 200, 192) 201, 193) 202, 194) 203, 195) 204, 196) 205, 197) 206, 198) 207, 199) 208, 200) 209, 201) 210, 202) 211, 203) 212, 204) 213, 205) 214, 206) 215, 207) 216, 208) 217, 209) 218, 210) 219, 211) 220, 212) 221, 213) 222, 214) 223, 215) 224, 216) 225, 217) 226, 218) 227, 219) 228, 220) 229, 221) 230, 222) 231, 223) 232, 224) 233, 225) 234, 226) 235, 227) 236, 228) 237, 229) 238, 230) 239, 231) 240, 232) 241, 233) 242, 234) 243, 235) 244, 236) 245, 237) 246, 238) 247, 239) 248, 240) 249, 241) 250, 242) 251, 243) 252, 244) 253, 245) 254, 246) 255, 247) 256, 248) 257, 249) 258, 250) 259, 251) 260, 252) 261, 253) 262, 254) 263, 255) 264, 256) 265, 257) 266, 258) 267, 259) 268, 260) 269, 261) 270, 262) 271, 263) 272, 264) 273, 265) 274, 266) 275, 267) 276, 268) 277, 269) 278, 270) 279, 271) 280, 272) 281, 273) 282, 274) 283, 275) 284, 276) 285, 277) 286, 278) 287, 279) 288, 280) 289, 281) 290, 282) 291, 283) 292, 284) 293, 285) 294, 286) 295, 287) 296, 288) 297, 289) 298, 290) 299, 291) 300, 292) 301, 293) 302, 294) 303, 295) 304, 296) 305, 297) 306, 298) 307, 299) 308, 300) 309, 301) 310, 302) 311, 303) 312, 304) 313, 305) 314, 306) 315, 307) 316, 308) 317, 309) 318, 310) 319, 311) 320, 312) 321, 313) 322, 314) 323, 315) 324, 316) 325, 317) 326, 318) 327, 319) 328, 320) 329, 321) 330, 322) 331, 323) 332, 324) 333, 325) 334, 326) 335, 327) 336, 328) 337, 329) 338, 330) 339, 331) 340, 332) 341, 333) 342, 334) 343, 335) 344, 336) 345, 337) 346, 338) 347, 339) 348, 340) 349, 341) 350, 342) 351, 343) 352, 344) 353, 345) 354, 346) 355, 347) 356, 348) 357, 349) 358, 350) 359, 351) 360, 352) 361, 353) 362, 354) 363, 355) 364, 356) 365, 357) 366, 358) 367, 359) 368, 360) 369, 361) 370, 362) 371, 363) 372, 364) 373, 365) 374, 366) 375, 367) 376, 368) 377, 369) 378, 370) 379, 371) 380, 372) 381, 373) 382, 374) 383, 375) 384, 376) 385, 377) 386, 378) 387, 379) 388, 380) 389, 381) 390, 382) 391, 383) 392, 384) 393, 385) 394, 386) 395, 387) 396, 388) 397, 389) 398, 390) 399, 391) 400, 392) 401, 393) 402, 394) 403, 395) 404, 396) 405, 397) 406, 398) 407, 399) 408, 400) 409, 401) 410, 402) 411, 403) 412, 404) 413, 405) 414, 406) 415, 407) 416, 408) 417, 409) 418, 410) 419, 411) 420, 412) 421, 413) 422, 414) 423, 415) 424, 416) 425, 417) 426, 418) 427, 419) 428, 420) 429, 421) 430, 422) 431, 423) 432, 424) 433, 425) 434, 426) 435, 427) 436, 428) 437, 429) 438, 43

$$; \wedge \nu, \rho, \tau, \dots$$

Λιλιαν ν / ιν ζ η

$i$	1	2	3	4	5
$\pi$	3	4	5	2	1
$\pi^2$	5	2	1	4	3
$\pi^3$	1	4	3	2	5

$$K_1 = \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \quad \therefore \text{10 J}$$

$$K_2^{-2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$K_3 = \pi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$



$(i=3 \geq J_e) : \text{||}\wedge\text{||}$

~~$$Y = 1101110001,$$

$$L_3 = 11011 \quad R_3 = 10001$$~~

$$Y = 1101110001,$$

$$R_3 = 11011 \quad L_3 = 10001$$

||>||

$$R_2 = L_3 = 10001$$

$$L_2 = R_3 \oplus f(R_2, k_3)$$

$$k_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

$$R_2 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 4 & 3 & 2 & 5 \end{matrix}$$

$$f(R_2, k_3) = 10001$$

$$L_2 = R_3 \oplus f(R_2, k_3) = 10011 \oplus 10001 = 01010$$

$$L_2 = 01010 \quad R_2 = 10001$$

$i=1 \geq J_e$

$$R_1 = L_2 = 01010$$

$$L_1 = R_2 \oplus f(R_1, k_2)$$

$$R_1 = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 0 & 1 & 0 \\ 5 & 2 & 1 & 4 & 3 \end{matrix}$$

$$k_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$$

$$f(R_1, k_2) = 01010$$

$$L_1 = R_2 \oplus f(R_1, k_2) = 10001 \oplus 01010 = 11011$$

$$R_0 = L_1 = 1 \ 1 \ 0 \ 1 \ 1$$

$$L_0 = R_1 \oplus f(R_0, k_1)$$

$$R_0 = \begin{matrix} & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{matrix}$$

$$\begin{matrix} 3 & 4 & 5 & 2 & 1 \end{matrix}$$

$$f(R_0, k_1) = 0 \ 1 \ 1 \ 1 \ 1$$

$$\begin{matrix} i=0 & 2 & 4 & 6 \end{matrix}$$

$$k_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$L_0 = R_1 \oplus f(R_0, k_1) = 0 \ 1 \ 0 \ 1 \ 0 \oplus 0 \ 1 \ 1 \ 1 \ 1 = 0 \ 0 \ 1 \ 0 \ 1$$

$$X = L_0 R_0 = 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 1$$

10.3.1 : פונקציה

הפונקציה  $\phi$  היא פונקציה מ- $\mathbb{N}$  ל- $\mathbb{N}$  המוגדרת על ידי:

$$\phi(p^n) = \begin{cases} (p-1)\phi(n) & p \nmid n \\ p\phi(n) & p \mid n \end{cases}$$

למשל:  $\phi(12) = 4$  כי  $12 = 2^2 \cdot 3$  ולכן  $\phi(12) = \phi(2^2) \cdot \phi(3) = 2 \cdot 2 = 4$

הפונקציה  $\phi$  היא פונקציה מ- $\mathbb{N}$  ל- $\mathbb{N}$  המוגדרת על ידי:

הפונקציה  $\phi$  היא פונקציה מ- $\mathbb{N}$  ל- $\mathbb{N}$  המוגדרת על ידי:

אם  $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$  אז:

$$\phi(a) = (p_1^{e_1} - p_1^{e_1-1}) \cdot (p_2^{e_2} - p_2^{e_2-1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k-1})$$

למשל:  $\phi(12) = 4$  כי  $12 = 2^2 \cdot 3$  ולכן  $\phi(12) = (2^2 - 2^{2-1}) \cdot (3^1 - 3^{1-1}) = 2 \cdot 2 = 4$

$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k} \Rightarrow \phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k-1})$

למשל:  $\phi(12) = 4$  כי  $12 = 2^2 \cdot 3$  ולכן  $\phi(12) = (2^2 - 2^{2-1}) \cdot (3^1 - 3^{1-1}) = 2 \cdot 2 = 4$

$p^n = p \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$

$= p^1 \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k} \Rightarrow \phi(p^n) = (p^1 - p^{1-1}) \cdot (p_1^{e_1} - p_1^{e_1-1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k-1})$

$$\Rightarrow \phi(p\alpha) = (p-1)\phi(\alpha)$$

.  $\alpha$   $\in$   $\mathbb{Z}$   $\Rightarrow$   $\alpha = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$   $\Rightarrow \phi(\alpha) = (p_1^{e_1} - p_1^{e_1-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$  : 2  $\alpha \in \mathbb{N}$

$$\alpha = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k} \Rightarrow \phi(\alpha) = (p_1^{e_1} - p_1^{e_1-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$$

$$\phi(\alpha) = (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1})$$

$$\Rightarrow p \cdot \alpha = p \cdot p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

.  $\alpha$   $\in$   $\mathbb{Z}$   $\Rightarrow$   $p_i = p$   $\Rightarrow$   $\phi(p\alpha) = (p-1)\phi(\alpha)$  : 2  $\alpha \in \mathbb{N}$

$$p_i = p \Rightarrow \alpha = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

$$p \cdot \alpha = p_1^{e_1+1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

$$\begin{aligned} \phi(p\alpha) &= (p_1^{e_1+1} - p_1^{e_1}) (p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1}) \\ &= p_1 (p_1^{e_1} - p_1^{e_1-1}) (p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1}) \end{aligned}$$

$$= p_1 \phi(\alpha)$$

$$= p \phi(\alpha)$$

$$\phi(p^n) = (p^1 - p^0) \underbrace{(p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})}_{\phi(n)} \quad \text{c/d}$$

$$= (p-1) \phi(n)$$