

RC5 is a block cipher and typically uses these modes of operation.

ECB (Electronic codebook)

CBC (cipher block chaining)

CFB (cipher feedback)

OFB (output feedback)

CTR (counter)

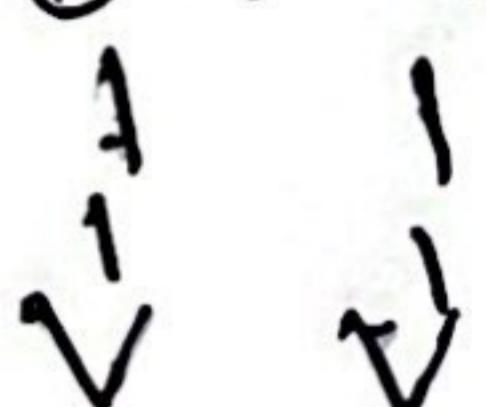
Language - Java

GUI : Java FX

Mode : ECB

PDF : SEE

64-bit plaintext block



$A + S[0]$

$B + S[1]$

[Rounds : $R = 12$]

$i \rightarrow$ for each round i :

$A = t[(A \oplus B) \lll B] + S[2^*i]$

$B = ((B \oplus A) \lll A) + S[2^*i + 1]$

4bit ciphertext block.

1. Permutation choice 1 (PC-1) and Final
Permutation (Invertible or PC-2):
PC-1: permutes a 64-bit key to remove
parity bits, leaving 56 bits.
PC-2: (final permutation choice): Reduces 56-bit
combined key shares to 48/48 bits among keys

3. Expansion Box: $48 \rightarrow 64$ bits
we simulate a method to expand 48 bits
to 64 by repeating some bits 0, 0, 1, 1
instruction 84

```
from typing import List, int, str, Table[int]
def permute(input_bits: str, table: Table[int]
→ str: """Permute 'input_bits' according
to the table. If 'i' is in 'table',
return ''.join([input_bits[i]] + j
for j in
range(len(input_bits) - 1, i, -1)] + table[i] + str[i + 1:]).
```

#1. permutation choice-1 (PC-1): from 64-bit key to 56-bit key via round robin mapping

PC1 - TABLE \equiv $\{i \mapsto j \mid i, j \in \{0, 1, \dots, 63\}\}$

57, 49, 41, 33, 25, 17, 9, 11, 13, 22, 5, 15, 31, 39, 47, 55, 63

1, 58, 50, 42, 34, 26, 18, 10, 2, 59, 51, 43, 35, 27

19, 11, 3, 60, 52, 44, 36, 17, 15, 13, 29, 5, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 26, 12, 4

16, 62, 54, 46, 38, 30, 22, 14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 26, 12, 4

14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 26, 12, 4

14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 26, 12, 4

14, 6, 61, 53, 45, 37, 29, 21, 13, 5, 28, 26, 12, 4

#2. comprehension Box: compression of 64 to 48 bits (custom example)

comprehension-Box \equiv $\{$

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63

#3. Expansion Box: Expanded 148' by 5' to 6' 4"

Custom examples); (1, 1, 1)

Expansion_BUXE_E - C / H8N / bcr0019.mrc

13, 14, 15, 16, 17, 18, 19, 20

21, 22, 23, 24, 25, 26, 27, 28, 29, 30

21, 22, 119, 243-07-7181, 311932, 11184.

1, 2, 3, 4, 5, 6, 7, 8

```
#Example 64 bits input (as binary string)
```

1000110011011101001011100110

1010" W. 115, 1000.

1. Apply PC^{-1}

key - 56 bit = permute Input - 64 bit, PC1 -
TABLE).

Print (f"56-bit) very (PUT) very-56bit)

#2. compress $64 \rightarrow 48$ bits = permutation input 64

bit, compression-box),

Print lf" compressed 1/MS7bit, output

#3, Expand 48 → 64 bits
Expanded-64 bit = permutation (compressed)

- 48bit, EXPANSION-BOX, 149, 240, 620, 110

Print Leaf" Expanded 64bit output. {
Print Leaf" Expanded 64bit output. {

"Expanded 64bity")

A close-up, high-angle view of a textured, light-colored surface, possibly a wall or ceiling, showing vertical streaks and discoloration. The surface has a mottled, weathered appearance with various shades of grey, brown, and white.

1811. - *Surpris. sturmus*.

1. Permutation choice 1 (PC-1) and final permutation (inverse of PC-2): PC-1

PC-1: permutes a 64-bit key to remove parity bits, leaving 48 bits.

PC-2: (final permutation choice): Reduces 56-bit combined key halves to 48-bit round keys.

2. compression box: $64 \rightarrow 48$ bits

We'll simulate a design that selects 48-bits from a 64-bit input.

3. Expansion box: $48 \rightarrow 64$ bits

We simulate a method to expand 48 bits to 64 by repeating some bits if necessary.

```
from typing import List, int, str
def permute(input_bits: str, table: List[int]) -> str:
    permute, input_bits according
    to the table.
    for i in table:
        return join([input_bits[i]] for i in table).
```

#1. permutation choice of 1 (P₁) in lesson 64-
bit key to 56 bit key

PC1 - TABLE = Σ

57, 49, 41, 33, 25, 17, 9
1, 58, 50, 34, 2, 34, 26, 18
10, 2, 59, 51, 43, 35, 27
19, 11, 3, 60, 52, 44, 36
6, 63, 55, 47, 39, 31, 23, 15
7, 62, 54, 46, 38, 30, 22
14, 6, 61, 53, 45, 37, 29
21, 13, 5, 28, 20, 12, 4

#2. comprehension box: compress 64 to
48 bits (custom example)

comprehension box = Σ

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199, 201, 203, 205, 207, 209, 211, 213, 215, 217, 219, 221, 223, 225, 227, 229, 231, 233, 235, 237, 239, 241, 243, 245, 247, 249, 251, 253, 255, 257, 259, 261, 263, 265, 267, 269, 271, 273, 275, 277, 279, 281, 283, 285, 287, 289, 291, 293, 295, 297, 299, 301, 303, 305, 307, 309, 311, 313, 315, 317, 319, 321, 323, 325, 327, 329, 331, 333, 335, 337, 339, 341, 343, 345, 347, 349, 351, 353, 355, 357, 359, 361, 363, 365, 367, 369, 371, 373, 375, 377, 379, 381, 383, 385, 387, 389, 391, 393, 395, 397, 399, 401, 403, 405, 407, 409, 411, 413, 415, 417, 419, 421, 423, 425, 427, 429, 431, 433, 435, 437, 439, 441, 443, 445, 447, 449, 451, 453, 455, 457, 459, 461, 463, 465, 467, 469, 471, 473, 475, 477, 479, 481, 483, 485, 487, 489, 491, 493, 495, 497, 499, 501, 503, 505, 507, 509, 511, 513, 515, 517, 519, 521, 523, 525, 527, 529, 531, 533, 535, 537, 539, 541, 543, 545, 547, 549, 551, 553, 555, 557, 559, 561, 563, 565, 567, 569, 571, 573, 575, 577, 579, 581, 583, 585, 587, 589, 591, 593, 595, 597, 599, 601, 603, 605, 607, 609, 611, 613, 615, 617, 619, 621, 623, 625, 627, 629, 631, 633, 635, 637, 639, 641, 643, 645, 647, 649, 651, 653, 655, 657, 659, 661, 663, 665, 667, 669, 671, 673, 675, 677, 679, 681, 683, 685, 687, 689, 691, 693, 695, 697, 699, 701, 703, 705, 707, 709, 711, 713, 715, 717, 719, 721, 723, 725, 727, 729, 731, 733, 735, 737, 739, 741, 743, 745, 747, 749, 751, 753, 755, 757, 759, 761, 763, 765, 767, 769, 771, 773, 775, 777, 779, 781, 783, 785, 787, 789, 791, 793, 795, 797, 799, 801, 803, 805, 807, 809, 811, 813, 815, 817, 819, 821, 823, 825, 827, 829, 831, 833, 835, 837, 839, 841, 843, 845, 847, 849, 851, 853, 855, 857, 859, 861, 863, 865, 867, 869, 871, 873, 875, 877, 879, 881, 883, 885, 887, 889, 891, 893, 895, 897, 899, 901, 903, 905, 907, 909, 911, 913, 915, 917, 919, 921, 923, 925, 927, 929, 931, 933, 935, 937, 939, 941, 943, 945, 947, 949, 951, 953, 955, 957, 959, 961, 963, 965, 967, 969, 971, 973, 975, 977, 979, 981, 983, 985, 987, 989, 991, 993, 995, 997, 999, 1001, 1003, 1005, 1007, 1009, 1011, 1013, 1015, 1017, 1019, 1021, 1023, 1025, 1027, 1029, 1031, 1033, 1035, 1037, 1039, 1041, 1043, 1045, 1047, 1049, 1051, 1053, 1055, 1057, 1059, 1061, 1063, 1065, 1067, 1069, 1071, 1073, 1075, 1077, 1079, 1081, 1083, 1085, 1087, 1089, 1091, 1093, 1095, 1097, 1099, 1101, 1103, 1105, 1107, 1109, 1111, 1113, 1115, 1117, 1119, 1121, 1123, 1125, 1127, 1129, 1131, 1133, 1135, 1137, 1139, 1141, 1143, 1145, 1147, 1149, 1151, 1153, 1155, 1157, 1159, 1161, 1163, 1165, 1167, 1169, 1171, 1173, 1175, 1177, 1179, 1181, 1183, 1185, 1187, 1189, 1191, 1193, 1195, 1197, 1199, 1201, 1203, 1205, 1207, 1209, 1211, 1213, 1215, 1217, 1219, 1221, 1223, 1225, 1227, 1229, 1231, 1233, 1235, 1237, 1239, 1241, 1243, 1245, 1247, 1249, 1251, 1253, 1255, 1257, 1259, 1261, 1263, 1265, 1267, 1269, 1271, 1273, 1275, 1277, 1279, 1281, 1283, 1285, 1287, 1289, 1291, 1293, 1295, 1297, 1299, 1301, 1303, 1305, 1307, 1309, 1311, 1313, 1315, 1317, 1319, 1321, 1323, 1325, 1327, 1329, 1331, 1333, 1335, 1337, 1339, 1341, 1343, 1345, 1347, 1349, 1351, 1353, 1355, 1357, 1359, 1361, 1363, 1365, 1367, 1369, 1371, 1373, 1375, 1377, 1379, 1381, 1383, 1385, 1387, 1389, 1391, 1393, 1395, 1397, 1399, 1401, 1403, 1405, 1407, 1409, 1411, 1413, 1415, 1417, 1419, 1421, 1423, 1425, 1427, 1429, 1431, 1433, 1435, 1437, 1439, 1441, 1443, 1445, 1447, 1449, 1451, 1453, 1455, 1457, 1459, 1461, 1463, 1465, 1467, 1469, 1471, 1473, 1475, 1477, 1479, 1481, 1483, 1485, 1487, 1489, 1491, 1493, 1495, 1497, 1499, 1501, 1503, 1505, 1507, 1509, 1511, 1513, 1515, 1517, 1519, 1521, 1523, 1525, 1527, 1529, 1531, 1533, 1535, 1537, 1539, 1541, 1543, 1545, 1547, 1549, 1551, 1553, 1555, 1557, 1559, 1561, 1563, 1565, 1567, 1569, 1571, 1573, 1575, 1577, 1579, 1581, 1583, 1585, 1587, 1589, 1591, 1593, 1595, 1597, 1599, 1601, 1603, 1605, 1607, 1609, 1611, 1613, 1615, 1617, 1619, 1621, 1623, 1625, 1627, 1629, 1631, 1633, 1635, 1637, 1639, 1641, 1643, 1645, 1647, 1649, 1651, 1653, 1655, 1657, 1659, 1661, 1663, 1665, 1667, 1669, 1671, 1673, 1675, 1677, 1679, 1681, 1683, 1685, 1687, 1689, 1691, 1693, 1695, 1697, 1699, 1701, 1703, 1705, 1707, 1709, 1711, 1713, 1715, 1717, 1719, 1721, 1723, 1725, 1727, 1729, 1731, 1733, 1735, 1737, 1739, 1741, 1743, 1745, 1747, 1749, 1751, 1753, 1755, 1757, 1759, 1761, 1763, 1765, 1767, 1769, 1771, 1773, 1775, 1777, 1779, 1781, 1783, 1785, 1787, 1789, 1791, 1793, 1795, 1797, 1799, 1801, 1803, 1805, 1807, 1809, 1811, 1813, 1815, 1817, 1819, 1821, 1823, 1825, 1827, 1829, 1831, 1833, 1835, 1837, 1839, 1841, 1843, 1845, 1847, 1849, 1851, 1853, 1855, 1857, 1859, 1861, 1863, 1865, 1867, 1869, 1871, 1873, 1875, 1877, 1879, 1881, 1883, 1885, 1887, 1889, 1891, 1893, 1895, 1897, 1899, 1901, 1903, 1905, 1907, 1909, 1911, 1913, 1915, 1917, 1919, 1921, 1923, 1925, 1927, 1929, 1931, 1933, 1935, 1937, 1939, 1941, 1943, 1945, 1947, 1949, 1951, 1953, 1955, 1957, 1959, 1961, 1963, 1965, 1967, 1969, 1971, 1973, 1975, 1977, 1979, 1981, 1983, 1985, 1987, 1989, 1991, 1993, 1995, 1997, 1999, 2001, 2003, 2005, 2007, 2009, 2011, 2013, 2015, 2017, 2019, 2021, 2023, 2025, 2027, 2029, 2031, 2033, 2035, 2037, 2039, 2041, 2043, 2045, 2047, 2049, 2051, 2053, 2055, 2057, 2059, 2061, 2063, 2065, 2067, 2069, 2071, 2073, 2075, 2077, 2079, 2081, 2083, 2085, 2087, 2089, 2091, 2093, 2095, 2097, 2099, 2101, 2103, 2105, 2107, 2109, 2111, 2113, 2115, 2117, 2119, 2121, 2123, 2125, 2127, 2129, 2131, 2133, 2135, 2137, 2139, 2141, 2143, 2145, 2147, 2149, 2151, 2153, 2155, 2157, 2159, 2161, 2163, 2165, 2167, 2169, 2171, 2173, 2175, 2177, 2179, 2181, 2183, 2185, 2187, 2189, 2191, 2193, 2195, 2197, 2199, 2201, 2203, 2205, 2207, 2209, 2211, 2213, 2215, 2217, 2219, 2221, 2223, 2225, 2227, 2229, 2231, 2233, 2235, 2237, 2239, 2241, 2243, 2245, 2247, 2249, 2251, 2253, 2255, 2257, 2259, 2261, 2263, 2265, 2267, 2269, 2271, 2273, 2275, 2277, 2279, 2281, 2283, 2285, 2287, 2289, 2291, 2293, 2295, 2297, 2299, 2301, 2303, 2305, 2307, 2309, 2311, 2313, 2315, 2317, 2319, 2321, 2323, 2325, 2327, 2329, 2331, 2333, 2335, 2337, 2339, 2341, 2343, 2345, 2347, 2349, 2351, 2353, 2355, 2357, 2359, 2361, 2363, 2365, 2367, 2369, 2371, 2373, 2375, 2377, 2379, 2381, 2383, 2385, 2387, 2389, 2391, 2393, 2395, 2397, 2399, 2401, 2403, 2405, 2407, 2409, 2411, 2413, 2415, 2417, 2419, 2421, 2423, 2425, 2427, 2429, 2431, 2433, 2435, 2437, 2439, 2441, 2443, 2445, 2447, 2449, 2451, 2453, 2455, 2457, 2459, 2461, 2463, 2465, 2467, 2469, 2471, 2473, 2475, 2477, 2479, 2481, 2483, 2485, 2487, 2489, 2491, 2493, 2495, 2497, 2499, 2501, 2503, 2505, 2507, 2509, 2511, 2513, 2515, 2517, 2519, 2521, 2523, 2525, 2527, 2529, 2531, 2533, 2535, 2537, 2539, 2541, 2543, 2545, 2547, 2549, 2551, 2553, 2555, 2557, 2559, 2561, 2563, 2565, 2567, 2569, 2571, 2573, 2575, 2577, 2579, 2581, 2583, 2585, 2587, 2589, 2591, 2593, 2595, 2597,

Q. 1: Prove Fermat's Little Theorem:

If p is a prime number and a is an integer such that $a \not\equiv 0 \pmod{p}$, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof using modular arithmetic:

$$S = \{1, 2, 3, \dots, p-1\}$$

multiply each element in S by a , where $a \not\equiv 0 \pmod{p}$.

$$S' = \{a \cdot 1, a \cdot 2, a \cdot 3, \dots, a \cdot (p-1)\} \pmod{p}$$

thus, $a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

since $(p-1)! \not\equiv 0 \pmod{p}$

$$a^{p-1} \equiv 1 \pmod{p}$$

∴ Fermat's Little Theorem is proved.

Given, $a \equiv 26 \pmod{21}$, $5 \cdot 21 \equiv 105 \equiv 1 \pmod{21}$

$$a^5 \equiv 26^5 \pmod{21}$$

$$\text{D1: } P = 13$$

13 is prime and $7 \not\equiv 1 \pmod{13}$

so $7^{12} \equiv 1 \pmod{13}$

so, $7^{12} \pmod{13} = 1$

1. Efficient modular Exponentiation.

$a \equiv m \pmod{n}$ and $m \equiv c^d \pmod{n}$

2. key insights for Euler's theorem.

$a^{\phi(n)} \equiv 1 \pmod{n}$

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

3. Primality testing.

$a^{p-1} \not\equiv 1 \pmod{p}$

$(a^{p-1})^{(p-1)} \equiv 1 \pmod{p}$

Q.2: Euler's theorem statement.

compute $\phi(n)$ for $n = 35, 45, 100$
given n factored into distinct primes

as $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right)$$

$$\phi(35)$$

$$35 = 5 \cdot 7$$

$$\phi(35) = 35 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$$

$$\phi(45)$$

$$45 = 3^2 \cdot 5$$

$$\phi(45) = 45 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 45 \cdot \frac{2}{3} \cdot \frac{4}{5} = 24$$

$$\phi(100)$$

$$100 = 2^2 \cdot 5^2$$

$$\phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$\text{If } a \cdot \phi(n) \equiv 1 \pmod{n}$$

this is known as Euler's theorem.

Proof:

$$\bullet a \in \mathbb{Z}$$

$$\bullet \gcd(a, n) = 1$$

$$\bullet R = \{r_1, r_2, \dots, r, \phi(n)\}$$

1. permutes the elements of R.

$$r_1 r_2 \cdots r_{\phi(n)} \equiv (ar_1)(ar_2) \cdots (ar_{\phi(n)}) \pmod{n}$$

$$r_1 r_2 \cdots r_{\phi(n)} \equiv a^{\phi(n)} \cdot r_1 r_2 \cdots r_{\phi(n)} \pmod{n}$$

With the help of the above, we can write $0.02 = \frac{2}{99} = \text{W}$.

$$K = \sqrt{11}, \sqrt{11} - 1, \sqrt{11} + 1, \frac{11u}{N} = N$$

$$u \in \mathcal{C}^1([0, 1], \mathbb{R}^N) \cap \mathcal{C}^0([0, 1], \mathbb{R}^N)$$

09 = ω_{ultra}

and is now on . ENRICO M. TRUCCO

1990. 7. 1. 10:00 a.m. $u = 1.2$ m/s

11-02

$$i_0(100) = 100 \left(1 - \frac{1}{100}\right) = 99$$

$$1000 \times 100 = 100000$$

$$h(x) = \sqrt{1-x^2} \quad \text{and} \quad \int_0^1 h(x) dx = \pi/4$$

Get power. $\tau \equiv \lambda$

162/162

11/13/2010 10:00 AM. 248 P.M. 2010

the 11th of Sept. 1858. I. G. C.

0 2 Mt. Brown. west.

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.

$$(N; m_i) \equiv 1 \pmod{n_i-1}$$

Step-2

$$N_1 = 20 \pmod{3}$$

$$m_1 = 2$$

$$20 \cdot 2 = 40 \equiv 1 \pmod{3}$$

$$m_1 = 2$$

$$N_2 = 15 \pmod{4}$$

$$15 \cdot m_2 \equiv 1 \pmod{4}$$

$$m_2 = 3$$

$$15 \cdot 3 = 45 \equiv 1 \pmod{4}$$

$$m_2 = 3$$

$$N_3 = 12 \pmod{5}$$

$$12 \cdot m_3 \equiv 1 \pmod{5}$$

$$m_3 = 3$$

$$12 \cdot 3 = 36 \equiv 1 \pmod{5}$$

$$m_3 = 3$$

Step-3:

$$x \equiv a_1 N_1 m_1 + a_2 N_2 m_2 + a_3 N_3 m_3 \pmod{N}$$