LAPORAN HASIL ENKRIPSI & DEKRIPSI

Nama: M Juan Yafi Zaim Wibisono

NIM: 202410370110258

Kelas: Informatika F

PROSES ENKRIPSI EL GAMAL:

Blok 1 - ASCII: 77 (k = 16)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^16 mod 2579 = 622

949^16 × 77 mod 2579

= 47894 mod 2579

= 1472

Hasil Enkripsi Blok 1: ASCII (M) = 77, = 1061, = 1472

Blok 2 - ASCII: 32 (k = 14)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

Menghitung hasil akhir 2^14 mod 2579:

2^14 mod 2579 = [2^8 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] mod 2579

= (256 × 16 × 4) mod 2579

= 16384 mod 2579

= 910

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

Menghitung hasil akhir 949^14 mod 2579:

949^14 mod 2579 = [949^8 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] mod 2579

= (678 × 2368 × 530) mod 2579

= 850917120 mod 2579

= 1860

949^14 mod 2579 = 1860

949^14 × 32 mod 2579

= 59520 mod 2579

= 203

Hasil Enkripsi Blok 2: ASCII (M) = 32, = 910, = 203

Blok 3 - ASCII: 74 (k = 9)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

Menghitung hasil akhir 2^9 mod 2579:

2^9 mod 2579 = [2^8 mod 2579] × [2^1 mod 2579] mod 2579

= (256 × 2) mod 2579

= 512 mod 2579

= 512

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

Menghitung hasil akhir 949^9 mod 2579:

949^9 mod 2579 = [949^8 mod 2579] × [949^1 mod 2579] mod 2579

= (678 × 949) mod 2579

= 643422 mod 2579

= 1251

949^9 mod 2579 = 1251

949^9 × 74 mod 2579

= 92574 mod 2579

= 2309

Hasil Enkripsi Blok 3: ASCII (M) = 74, = 512, = 2309

Blok 4 - ASCII: 117 (k = 16)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^16 mod 2579 = 622

949^16 × 117 mod 2579

= 72774 mod 2579

= 562

Hasil Enkripsi Blok 4: ASCII (M) = 117, = 1061, = 562

Blok 5 - ASCII: 97 (k = 45)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^45 mod 2579:

2^45 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 256 × 16 × 2) mod 2579

= 10461184 mod 2579

= 760

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^45 mod 2579:

949^45 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] × [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 678 × 2368 × 949) mod 2579

= 51803192064 mod 2579

= 246

949^45 mod 2579 = 246

949^45 × 97 mod 2579

= 23862 mod 2579

= 651

Hasil Enkripsi Blok 5: ASCII (M) = 97, = 760, = 651

Blok 6 - ASCII: 110 (k = 41)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^41 mod 2579:

2^41 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 256 × 2) mod 2579

= 653824 mod 2579

= 1337

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^41 mod 2579:

949^41 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 678 × 949) mod 2579

= 21876348 mod 2579

= 1270

949^41 mod 2579 = 1270

949^41 × 110 mod 2579

= 139700 mod 2579

= 434

Hasil Enkripsi Blok 6: ASCII (M) = 110, = 1337, = 434

Blok 7 - ASCII: 32 (k = 5)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

Menghitung hasil akhir 2^5 mod 2579:

2^5 mod 2579 = [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (16 × 2) mod 2579

= 32 mod 2579

= 32

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

Menghitung hasil akhir 949^5 mod 2579:

949^5 mod 2579 = [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (2368 × 949) mod 2579

= 2247232 mod 2579

= 923

949^5 mod 2579 = 923

949^5 × 32 mod 2579

= 29536 mod 2579

= 1167

Hasil Enkripsi Blok 7: ASCII (M) = 32, = 32, = 1167

Blok 8 - ASCII: 89 (k = 5)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

Menghitung hasil akhir 2^5 mod 2579:

2^5 mod 2579 = [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (16 × 2) mod 2579

= 32 mod 2579

= 32

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

Menghitung hasil akhir 949^5 mod 2579:

949^5 mod 2579 = [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (2368 × 949) mod 2579

= 2247232 mod 2579

= 923

949^5 mod 2579 = 923

949^5 × 89 mod 2579

= 82147 mod 2579

= 2198

Hasil Enkripsi Blok 8: ASCII (M) = 89, = 32, = 2198

Blok 9 - ASCII: 97 (k = 37)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^37 mod 2579:

2^37 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 16 × 2) mod 2579

= 40864 mod 2579

= 2179

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^37 mod 2579:

949^37 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 2368 × 949) mod 2579

= 76405888 mod 2579

= 434

949^37 mod 2579 = 434

949^37 × 97 mod 2579

= 42098 mod 2579

= 834

Hasil Enkripsi Blok 9: ASCII (M) = 97, = 2179, = 834

Blok 10 - ASCII: 102 (k = 22)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

Menghitung hasil akhir 2^22 mod 2579:

2^22 mod 2579 = [2^16 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] mod 2579

= (1061 × 16 × 4) mod 2579

= 67904 mod 2579

= 850

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

Menghitung hasil akhir 949^22 mod 2579:

949^22 mod 2579 = [949^16 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] mod 2579

= (622 × 2368 × 530) mod 2579

= 780634880 mod 2579

= 2528

949^22 mod 2579 = 2528

949^22 × 102 mod 2579

= 257856 mod 2579

= 2535

Hasil Enkripsi Blok 10: ASCII (M) = 102, = 850, = 2535

Blok 11 - ASCII: 105 (k = 1)

2^1 mod 2579 = 2

949^1 mod 2579 = 949

949^1 mod 2579 = 949

949^1 × 105 mod 2579

= 99645 mod 2579

= 1643

Hasil Enkripsi Blok 11: ASCII (M) = 105, = 2, = 1643

Blok 12 - ASCII: 32 (k = 27)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

Menghitung hasil akhir 2^27 mod 2579:

2^27 mod 2579 = [2^16 mod 2579] × [2^8 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (1061 × 256 × 4 × 2) mod 2579

= 2172928 mod 2579

= 1410

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

Menghitung hasil akhir 949^27 mod 2579:

949^27 mod 2579 = [949^16 mod 2579] × [949^8 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (622 × 678 × 530 × 949) mod 2579

= 212110496520 mod 2579

= 1928

949^27 mod 2579 = 1928

949^27 × 32 mod 2579

= 61696 mod 2579

= 2379

Hasil Enkripsi Blok 12: ASCII (M) = 32, = 1410, = 2379

Blok 13 - ASCII: 90 (k = 3)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

Menghitung hasil akhir 2^3 mod 2579:

2^3 mod 2579 = [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (4 × 2) mod 2579

= 8 mod 2579

= 8

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

Menghitung hasil akhir 949^3 mod 2579:

949^3 mod 2579 = [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (530 × 949) mod 2579

= 502970 mod 2579

= 65

949^3 mod 2579 = 65

949^3 × 90 mod 2579

= 5850 mod 2579

= 692

Hasil Enkripsi Blok 13: ASCII (M) = 90, = 8, = 692

Blok 14 - ASCII: 97 (k = 5)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

Menghitung hasil akhir 2^5 mod 2579:

2^5 mod 2579 = [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (16 × 2) mod 2579

= 32 mod 2579

= 32

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

Menghitung hasil akhir 949^5 mod 2579:

949^5 mod 2579 = [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (2368 × 949) mod 2579

= 2247232 mod 2579

= 923

949^5 mod 2579 = 923

949^5 × 97 mod 2579

= 89531 mod 2579

= 1845

Hasil Enkripsi Blok 14: ASCII (M) = 97, = 32, = 1845

Blok 15 - ASCII: 105 (k = 17)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

Menghitung hasil akhir 2^17 mod 2579:

2^17 mod 2579 = [2^16 mod 2579] × [2^1 mod 2579] mod 2579

= (1061 × 2) mod 2579

= 2122 mod 2579

= 2122

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

Menghitung hasil akhir 949^17 mod 2579:

949^17 mod 2579 = [949^16 mod 2579] × [949^1 mod 2579] mod 2579

= (622 × 949) mod 2579

= 590278 mod 2579

= 2266

949^17 mod 2579 = 2266

949^17 × 105 mod 2579

= 237930 mod 2579

= 662

Hasil Enkripsi Blok 15: ASCII (M) = 105, = 2122, = 662

Blok 16 - ASCII: 109 (k = 34)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^34 mod 2579:

2^34 mod 2579 = [2^32 mod 2579] × [2^2 mod 2579] mod 2579

= (1277 × 4) mod 2579

= 5108 mod 2579

= 2529

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^34 mod 2579:

949^34 mod 2579 = [949^32 mod 2579] × [949^2 mod 2579] mod 2579

= (34 × 530) mod 2579

= 18020 mod 2579

= 2546

949^34 mod 2579 = 2546

949^34 × 109 mod 2579

= 277514 mod 2579

= 1561

Hasil Enkripsi Blok 16: ASCII (M) = 109, = 2529, = 1561

Blok 17 - ASCII: 32 (k = 4)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^4 mod 2579 = 2368

949^4 × 32 mod 2579

= 75776 mod 2579

= 985

Hasil Enkripsi Blok 17: ASCII (M) = 32, = 16, = 985

Blok 18 - ASCII: 87 (k = 50)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^50 mod 2579:

2^50 mod 2579 = [2^32 mod 2579] × [2^16 mod 2579] × [2^2 mod 2579] mod 2579

= (1277 × 1061 × 4) mod 2579

= 5419588 mod 2579

= 1109

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^50 mod 2579:

949^50 mod 2579 = [949^32 mod 2579] × [949^16 mod 2579] × [949^2 mod 2579] mod 2579

= (34 × 622 × 530) mod 2579

= 11208440 mod 2579

= 106

949^50 mod 2579 = 106

949^50 × 87 mod 2579

= 9222 mod 2579

= 1485

Hasil Enkripsi Blok 18: ASCII (M) = 87, = 1109, = 1485

Blok 19 - ASCII: 105 (k = 38)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^38 mod 2579:

2^38 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] mod 2579

= (1277 × 16 × 4) mod 2579

= 81728 mod 2579

= 1779

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^38 mod 2579:

949^38 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] mod 2579

= (34 × 2368 × 530) mod 2579

= 42671360 mod 2579

= 1805

949^38 mod 2579 = 1805

949^38 × 105 mod 2579

= 189525 mod 2579

= 1258

Hasil Enkripsi Blok 19: ASCII (M) = 105, = 1779, = 1258

Blok 20 - ASCII: 98 (k = 29)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

Menghitung hasil akhir 2^29 mod 2579:

2^29 mod 2579 = [2^16 mod 2579] × [2^8 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (1061 × 256 × 16 × 2) mod 2579

= 8691712 mod 2579

= 482

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

Menghitung hasil akhir 949^29 mod 2579:

949^29 mod 2579 = [949^16 mod 2579] × [949^8 mod 2579] × [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (622 × 678 × 2368 × 949) mod 2579

= 947693690112 mod 2579

= 556

949^29 mod 2579 = 556

949^29 × 98 mod 2579

= 54488 mod 2579

= 329

Hasil Enkripsi Blok 20: ASCII (M) = 98, = 482, = 329

Blok 21 - ASCII: 105 (k = 5)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

Menghitung hasil akhir 2^5 mod 2579:

2^5 mod 2579 = [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (16 × 2) mod 2579

= 32 mod 2579

= 32

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

Menghitung hasil akhir 949^5 mod 2579:

949^5 mod 2579 = [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (2368 × 949) mod 2579

= 2247232 mod 2579

= 923

949^5 mod 2579 = 923

949^5 × 105 mod 2579

= 96915 mod 2579

= 1492

Hasil Enkripsi Blok 21: ASCII (M) = 105, = 32, = 1492

Blok 22 - ASCII: 115 (k = 10)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

Menghitung hasil akhir 2^10 mod 2579:

2^10 mod 2579 = [2^8 mod 2579] × [2^2 mod 2579] mod 2579

= (256 × 4) mod 2579

= 1024 mod 2579

= 1024

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

Menghitung hasil akhir 949^10 mod 2579:

949^10 mod 2579 = [949^8 mod 2579] × [949^2 mod 2579] mod 2579

= (678 × 530) mod 2579

= 359340 mod 2579

= 859

949^10 mod 2579 = 859

949^10 × 115 mod 2579

= 98785 mod 2579

= 783

Hasil Enkripsi Blok 22: ASCII (M) = 115, = 1024, = 783

Blok 23 - ASCII: 111 (k = 38)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^38 mod 2579:

2^38 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] mod 2579

= (1277 × 16 × 4) mod 2579

= 81728 mod 2579

= 1779

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^38 mod 2579:

949^38 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] mod 2579

= (34 × 2368 × 530) mod 2579

= 42671360 mod 2579

= 1805

949^38 mod 2579 = 1805

949^38 × 111 mod 2579

= 200355 mod 2579

= 1772

Hasil Enkripsi Blok 23: ASCII (M) = 111, = 1779, = 1772

Blok 24 - ASCII: 110 (k = 24)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

Menghitung hasil akhir 2^24 mod 2579:

2^24 mod 2579 = [2^16 mod 2579] × [2^8 mod 2579] mod 2579

= (1061 × 256) mod 2579

= 271616 mod 2579

= 821

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

Menghitung hasil akhir 949^24 mod 2579:

949^24 mod 2579 = [949^16 mod 2579] × [949^8 mod 2579] mod 2579

= (622 × 678) mod 2579

= 421716 mod 2579

= 1339

949^24 mod 2579 = 1339

949^24 × 110 mod 2579

= 147290 mod 2579

= 287

Hasil Enkripsi Blok 24: ASCII (M) = 110, = 821, = 287

Blok 25 - ASCII: 111 (k = 39)

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1277

Menghitung hasil akhir 2^39 mod 2579:

2^39 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 16 × 4 × 2) mod 2579

= 163456 mod 2579

= 979

949^1 mod 2579 = 949

949^2 mod 2579 = [949^1 mod 2579] × [949^1 mod 2579] mod 2579

= (949 × 949) mod 2579

= 530

949^4 mod 2579 = [949^2 mod 2579] × [949^2 mod 2579] mod 2579

= (530 × 530) mod 2579

= 2368

949^8 mod 2579 = [949^4 mod 2579] × [949^4 mod 2579] mod 2579

= (2368 × 2368) mod 2579

= 678

949^16 mod 2579 = [949^8 mod 2579] × [949^8 mod 2579] mod 2579

= (678 × 678) mod 2579

= 622

949^32 mod 2579 = [949^16 mod 2579] × [949^16 mod 2579] mod 2579

= (622 × 622) mod 2579

= 34

Menghitung hasil akhir 949^39 mod 2579:

949^39 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 2368 × 530 × 949) mod 2579

= 40495120640 mod 2579

= 489

949^39 mod 2579 = 489

949^39 × 111 mod 2579

= 54279 mod 2579

= 120

Hasil Enkripsi Blok 25: ASCII (M) = 111, = 979, = 120

ChipherText:

(1061, 1472) (910, 203) (512, 2309) (1061, 562) (760, 651) (1337, 434) (32, 1167) (32, 2198)

(2179, 834) (850, 2535) (2, 1643) (1410, 2379) (8, 692) (32, 1845) (2122, 662) (2529, 1561)

(16, 985) (1109, 1485) (1779, 1258) (482, 329) (32, 1492) (1024, 783) (1779, 1772) (821, 287) (979, 120)

PROSES DEKRIPSI EL GAMAL

Blok 1 - Dekripsi dengan = 1061, = 1472

1061^1 mod 2579 = 1061

1061^2 mod 2579 = [1061^1 mod 2579] × [1061^1 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1125721 mod 2579

= 1277

1061^4 mod 2579 = [1061^2 mod 2579] × [1061^2 mod 2579] mod 2579

= (1277 × 1277) mod 2579

= 1630729 mod 2579

= 801

1061^8 mod 2579 = [1061^4 mod 2579] × [1061^4 mod 2579] mod 2579

= (801 × 801) mod 2579

= 641601 mod 2579

= 2009

1061^16 mod 2579 = [1061^8 mod 2579] × [1061^8 mod 2579] mod 2579

= (2009 × 2009) mod 2579

= 4036081 mod 2579

= 2525

1061^32 mod 2579 = [1061^16 mod 2579] × [1061^16 mod 2579] mod 2579

= (2525 × 2525) mod 2579

= 6375625 mod 2579

= 337

1061^64 mod 2579 = [1061^32 mod 2579] × [1061^32 mod 2579] mod 2579

= (337 × 337) mod 2579

= 113569 mod 2579

= 93

1061^128 mod 2579 = [1061^64 mod 2579] × [1061^64 mod 2579] mod 2579

= (93 × 93) mod 2579

= 8649 mod 2579

= 912

1061^256 mod 2579 = [1061^128 mod 2579] × [1061^128 mod 2579] mod 2579

= (912 × 912) mod 2579

= 831744 mod 2579

= 1306

1061^512 mod 2579 = [1061^256 mod 2579] × [1061^256 mod 2579] mod 2579

= (1306 × 1306) mod 2579

= 1705636 mod 2579

= 917

1061^1024 mod 2579 = [1061^512 mod 2579] × [1061^512 mod 2579] mod 2579

= (917 × 917) mod 2579

= 840889 mod 2579

= 135

Menghitung hasil akhir 1061^1813 mod 2579:

1061^1813 mod 2579 = [1061^1024 mod 2579] × [1061^512 mod 2579] × [1061^256 mod 2579] × [1061^16 mod 2579] × [1061^4 mod 2579] × [1061^1 mod 2579] mod 2579

= (135 × 917 × 1306 × 2525 × 801 × 1061) mod 2579

= 346940950158636750 mod 2579

= 170

Perhitungan: M = (170 × 1472) mod 2579

= 250240 mod 2579

= 77

Hasil Dekripsi Blok 1: y = 170, M = 77

Blok 2 - Dekripsi dengan = 910, = 203

910^1 mod 2579 = 910

910^2 mod 2579 = [910^1 mod 2579] × [910^1 mod 2579] mod 2579

= (910 × 910) mod 2579

= 828100 mod 2579

= 241

910^4 mod 2579 = [910^2 mod 2579] × [910^2 mod 2579] mod 2579

= (241 × 241) mod 2579

= 58081 mod 2579

= 1343

910^8 mod 2579 = [910^4 mod 2579] × [910^4 mod 2579] mod 2579

= (1343 × 1343) mod 2579

= 1803649 mod 2579

= 928

910^16 mod 2579 = [910^8 mod 2579] × [910^8 mod 2579] mod 2579

= (928 × 928) mod 2579

= 861184 mod 2579

= 2377

910^32 mod 2579 = [910^16 mod 2579] × [910^16 mod 2579] mod 2579

= (2377 × 2377) mod 2579

= 5650129 mod 2579

= 2119

910^64 mod 2579 = [910^32 mod 2579] × [910^32 mod 2579] mod 2579

= (2119 × 2119) mod 2579

= 4490161 mod 2579

= 122

910^128 mod 2579 = [910^64 mod 2579] × [910^64 mod 2579] mod 2579

= (122 × 122) mod 2579

= 14884 mod 2579

= 1989

910^256 mod 2579 = [910^128 mod 2579] × [910^128 mod 2579] mod 2579

= (1989 × 1989) mod 2579

= 3956121 mod 2579

= 2514

910^512 mod 2579 = [910^256 mod 2579] × [910^256 mod 2579] mod 2579

= (2514 × 2514) mod 2579

= 6320196 mod 2579

= 1646

910^1024 mod 2579 = [910^512 mod 2579] × [910^512 mod 2579] mod 2579

= (1646 × 1646) mod 2579

= 2709316 mod 2579

= 1366

Menghitung hasil akhir 910^1813 mod 2579:

910^1813 mod 2579 = [910^1024 mod 2579] × [910^512 mod 2579] × [910^256 mod 2579] × [910^16 mod 2579] × [910^4 mod 2579] × [910^1 mod 2579] mod 2579

= (1366 × 1646 × 2514 × 2377 × 1343 × 910) mod 2579

= 16420727356349993040 mod 2579

= 2414

Perhitungan: M = (2414 × 203) mod 2579

= 490042 mod 2579

= 32

Hasil Dekripsi Blok 2: y = 2414, M = 32

Blok 3 - Dekripsi dengan = 512, = 2309

512^1 mod 2579 = 512

512^2 mod 2579 = [512^1 mod 2579] × [512^1 mod 2579] mod 2579

= (512 × 512) mod 2579

= 262144 mod 2579

= 1665

512^4 mod 2579 = [512^2 mod 2579] × [512^2 mod 2579] mod 2579

= (1665 × 1665) mod 2579

= 2772225 mod 2579

= 2379

512^8 mod 2579 = [512^4 mod 2579] × [512^4 mod 2579] mod 2579

= (2379 × 2379) mod 2579

= 5659641 mod 2579

= 1315

512^16 mod 2579 = [512^8 mod 2579] × [512^8 mod 2579] mod 2579

= (1315 × 1315) mod 2579

= 1729225 mod 2579

= 1295

512^32 mod 2579 = [512^16 mod 2579] × [512^16 mod 2579] mod 2579

= (1295 × 1295) mod 2579

= 1677025 mod 2579

= 675

512^64 mod 2579 = [512^32 mod 2579] × [512^32 mod 2579] mod 2579

= (675 × 675) mod 2579

= 455625 mod 2579

= 1721

512^128 mod 2579 = [512^64 mod 2579] × [512^64 mod 2579] mod 2579

= (1721 × 1721) mod 2579

= 2961841 mod 2579

= 1149

512^256 mod 2579 = [512^128 mod 2579] × [512^128 mod 2579] mod 2579

= (1149 × 1149) mod 2579

= 1320201 mod 2579

= 2332

512^512 mod 2579 = [512^256 mod 2579] × [512^256 mod 2579] mod 2579

= (2332 × 2332) mod 2579

= 5438224 mod 2579

= 1692

512^1024 mod 2579 = [512^512 mod 2579] × [512^512 mod 2579] mod 2579

= (1692 × 1692) mod 2579

= 2862864 mod 2579

= 174

Menghitung hasil akhir 512^1813 mod 2579:

512^1813 mod 2579 = [512^1024 mod 2579] × [512^512 mod 2579] × [512^256 mod 2579] × [512^16 mod 2579] × [512^4 mod 2579] × [512^1 mod 2579] mod 2579

= (174 × 1692 × 2332 × 1295 × 2379 × 512) mod 2579

= 1082959772079144960 mod 2579

= 2445

Perhitungan: M = (2445 × 2309) mod 2579

= 5645505 mod 2579

= 74

Hasil Dekripsi Blok 3: y = 2445, M = 74

Blok 4 - Dekripsi dengan = 1061, = 562

1061^1 mod 2579 = 1061

1061^2 mod 2579 = [1061^1 mod 2579] × [1061^1 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1125721 mod 2579

= 1277

1061^4 mod 2579 = [1061^2 mod 2579] × [1061^2 mod 2579] mod 2579

= (1277 × 1277) mod 2579

= 1630729 mod 2579

= 801

1061^8 mod 2579 = [1061^4 mod 2579] × [1061^4 mod 2579] mod 2579

= (801 × 801) mod 2579

= 641601 mod 2579

= 2009

1061^16 mod 2579 = [1061^8 mod 2579] × [1061^8 mod 2579] mod 2579

= (2009 × 2009) mod 2579

= 4036081 mod 2579

= 2525

1061^32 mod 2579 = [1061^16 mod 2579] × [1061^16 mod 2579] mod 2579

= (2525 × 2525) mod 2579

= 6375625 mod 2579

= 337

1061^64 mod 2579 = [1061^32 mod 2579] × [1061^32 mod 2579] mod 2579

= (337 × 337) mod 2579

= 113569 mod 2579

= 93

1061^128 mod 2579 = [1061^64 mod 2579] × [1061^64 mod 2579] mod 2579

= (93 × 93) mod 2579

= 8649 mod 2579

= 912

1061^256 mod 2579 = [1061^128 mod 2579] × [1061^128 mod 2579] mod 2579

= (912 × 912) mod 2579

= 831744 mod 2579

= 1306

1061^512 mod 2579 = [1061^256 mod 2579] × [1061^256 mod 2579] mod 2579

= (1306 × 1306) mod 2579

= 1705636 mod 2579

= 917

1061^1024 mod 2579 = [1061^512 mod 2579] × [1061^512 mod 2579] mod 2579

= (917 × 917) mod 2579

= 840889 mod 2579

= 135

Menghitung hasil akhir 1061^1813 mod 2579:

1061^1813 mod 2579 = [1061^1024 mod 2579] × [1061^512 mod 2579] × [1061^256 mod 2579] × [1061^16 mod 2579] × [1061^4 mod 2579] × [1061^1 mod 2579] mod 2579

= (135 × 917 × 1306 × 2525 × 801 × 1061) mod 2579

= 3469409501586367 50 mod 2579

= 170

Perhitungan: M = (170 × 562) mod 2579

= 95540 mod 2579

= 117

Hasil Dekripsi Blok 4: y = 170, M = 117

Blok 5 - Dekripsi dengan = 760, = 651

760^1 mod 2579 = 760

760^2 mod 2579 = [760^1 mod 2579] × [760^1 mod 2579] mod 2579

= (760 × 760) mod 2579

= 577600 mod 2579

= 2483

760^4 mod 2579 = [760^2 mod 2579] × [760^2 mod 2579] mod 2579

= (2483 × 2483) mod 2579

= 6165289 mod 2579

= 1479

760^8 mod 2579 = [760^4 mod 2579] × [760^4 mod 2579] mod 2579

= (1479 × 1479) mod 2579

= 2187441 mod 2579

= 449

760^16 mod 2579 = [760^8 mod 2579] × [760^8 mod 2579] mod 2579

= (449 × 449) mod 2579

= 201601 mod 2579

= 439

760^32 mod 2579 = [760^16 mod 2579] × [760^16 mod 2579] mod 2579

= (439 × 439) mod 2579

= 192721 mod 2579

= 1875

760^64 mod 2579 = [760^32 mod 2579] × [760^32 mod 2579] mod 2579

= (1875 × 1875) mod 2579

= 3515625 mod 2579

= 448

760^128 mod 2579 = [760^64 mod 2579] × [760^64 mod 2579] mod 2579

= (448 × 448) mod 2579

= 200704 mod 2579

= 2121

760^256 mod 2579 = [760^128 mod 2579] × [760^128 mod 2579] mod 2579

= (2121 × 2121) mod 2579

= 4498641 mod 2579

= 865

760^512 mod 2579 = [760^256 mod 2579] × [760^256 mod 2579] mod 2579

= (865 × 865) mod 2579

= 748225 mod 2579

= 315

760^1024 mod 2579 = [760^512 mod 2579] × [760^512 mod 2579] mod 2579

= (315 × 315) mod 2579

= 99225 mod 2579

= 1223

Menghitung hasil akhir 760^1813 mod 2579:

760^1813 mod 2579 = [760^1024 mod 2579] × [760^512 mod 2579] × [760^256 mod 2579] × [760^16 mod 2579] × [760^4 mod 2579] × [760^1 mod 2579] mod 2579

= (1223 × 315 × 865 × 439 × 1479 × 760) mod 2579

= 164436946964703000 mod 2579

= 325

Perhitungan: M = (325 × 651) mod 2579

= 211575 mod 2579

= 97

Hasil Dekripsi Blok 5: y = 325, M = 97

Blok 6 - Dekripsi dengan = 1337, = 434

1337^1 mod 2579 = 1337

1337^2 mod 2579 = [1337^1 mod 2579] × [1337^1 mod 2579] mod 2579

= (1337 × 1337) mod 2579

= 1787569 mod 2579

= 322

1337^4 mod 2579 = [1337^2 mod 2579] × [1337^2 mod 2579] mod 2579

= (322 × 322) mod 2579

= 103684 mod 2579

= 524

1337^8 mod 2579 = [1337^4 mod 2579] × [1337^4 mod 2579] mod 2579

= (524 × 524) mod 2579

= 274576 mod 2579

= 1202

1337^16 mod 2579 = [1337^8 mod 2579] × [1337^8 mod 2579] mod 2579

= (1202 × 1202) mod 2579

= 1444804 mod 2579

= 564

1337^32 mod 2579 = [1337^16 mod 2579] × [1337^16 mod 2579] mod 2579

= (564 × 564) mod 2579

= 318096 mod 2579

= 879

1337^64 mod 2579 = [1337^32 mod 2579] × [1337^32 mod 2579] mod 2579

= (879 × 879) mod 2579

= 772641 mod 2579

= 1520

1337^128 mod 2579 = [1337^64 mod 2579] × [1337^64 mod 2579] mod 2579

= (1520 × 1520) mod 2579

= 2310400 mod 2579

= 2195

1337^256 mod 2579 = [1337^128 mod 2579] × [1337^128 mod 2579] mod 2579

= (2195 × 2195) mod 2579

= 4818025 mod 2579

= 453

1337^512 mod 2579 = [1337^256 mod 2579] × [1337^256 mod 2579] mod 2579

= (453 × 453) mod 2579

= 205209 mod 2579

= 1468

1337^1024 mod 2579 = [1337^512 mod 2579] × [1337^512 mod 2579] mod 2579

= (1468 × 1468) mod 2579

= 2155024 mod 2579

= 1559

Menghitung hasil akhir 1337^1813 mod 2579:

1337^1813 mod 2579 = [1337^1024 mod 2579] × [1337^512 mod 2579] × [1337^256 mod 2579] × [1337^16 mod 2579] × [1337^4 mod 2579] × [1337^1 mod 2579] mod 2579

= (1559 × 1468 × 453 × 564 × 524 × 1337) mod 2579

= 4096492565423771 52 mod 2579

= 1058

Perhitungan: M = (1058 × 434) mod 2579

= 459172 mod 2579

= 110

Hasil Dekripsi Blok 6: y = 1058, M = 110

Blok 7 - Dekripsi dengan = 32, = 1167

32^1 mod 2579 = 32

32^2 mod 2579 = [32^1 mod 2579] × [32^1 mod 2579] mod 2579

= (32 × 32) mod 2579

= 1024 mod 2579

= 1024

32^4 mod 2579 = [32^2 mod 2579] × [32^2 mod 2579] mod 2579

= (1024 × 1024) mod 2579

= 1048576 mod 2579

= 1502

32^8 mod 2579 = [32^4 mod 2579] × [32^4 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

32^16 mod 2579 = [32^8 mod 2579] × [32^8 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

32^32 mod 2579 = [32^16 mod 2579] × [32^16 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

32^64 mod 2579 = [32^32 mod 2579] × [32^32 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

32^128 mod 2579 = [32^64 mod 2579] × [32^64 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

32^256 mod 2579 = [32^128 mod 2579] × [32^128 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

32^512 mod 2579 = [32^256 mod 2579] × [32^256 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

32^1024 mod 2579 = [32^512 mod 2579] × [32^512 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

Menghitung hasil akhir 32^1813 mod 2579:

32^1813 mod 2579 = [32^1024 mod 2579] × [32^512 mod 2579] × [32^256 mod 2579] × [32^16 mod 2579] × [32^4 mod 2579] × [32^1 mod 2579] mod 2579

= (245 × 443 × 136 × 1370 × 1502 × 32) mod 2579

= 971961801036800 mod 2579

= 2484

Perhitungan: M = (2484 × 1167) mod 2579

= 2898828 mod 2579

= 32

Hasil Dekripsi Blok 7: y = 2484, M = 32

Blok 8 - Dekripsi dengan = 32, = 2198

32^1 mod 2579 = 32

32^2 mod 2579 = [32^1 mod 2579] × [32^1 mod 2579] mod 2579

= (32 × 32) mod 2579

= 1024 mod 2579

= 1024

32^4 mod 2579 = [32^2 mod 2579] × [32^2 mod 2579] mod 2579

= (1024 × 1024) mod 2579

= 1048576 mod 2579

= 1502

32^8 mod 2579 = [32^4 mod 2579] × [32^4 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

32^16 mod 2579 = [32^8 mod 2579] × [32^8 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

32^32 mod 2579 = [32^16 mod 2579] × [32^16 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

32^64 mod 2579 = [32^32 mod 2579] × [32^32 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

32^128 mod 2579 = [32^64 mod 2579] × [32^64 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

32^256 mod 2579 = [32^128 mod 2579] × [32^128 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

32^512 mod 2579 = [32^256 mod 2579] × [32^256 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

32^1024 mod 2579 = [32^512 mod 2579] × [32^512 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

Menghitung hasil akhir 32^1813 mod 2579:

32^1813 mod 2579 = [32^1024 mod 2579] × [32^512 mod 2579] × [32^256 mod 2579] × [32^16 mod 2579] × [32^4 mod 2579] × [32^1 mod 2579] mod 2579

= (245 × 443 × 136 × 1370 × 1502 × 32) mod 2579

= 971961801036800 mod 2579

= 2484

Perhitungan: M = (2484 × 2198) mod 2579

= 5459832 mod 2579

= 89

Hasil Dekripsi Blok 8: y = 2484, M = 89

Blok 9 - Dekripsi dengan = 2179, = 834

2179^1 mod 2579 = 2179

2179^2 mod 2579 = [2179^1 mod 2579] × [2179^1 mod 2579] mod 2579

= (2179 × 2179) mod 2579

= 4748041 mod 2579

= 102

2179^4 mod 2579 = [2179^2 mod 2579] × [2179^2 mod 2579] mod 2579

= (102 × 102) mod 2579

= 10404 mod 2579

= 88

2179^8 mod 2579 = [2179^4 mod 2579] × [2179^4 mod 2579] mod 2579

= (88 × 88) mod 2579

= 7744 mod 2579

= 7

2179^16 mod 2579 = [2179^8 mod 2579] × [2179^8 mod 2579] mod 2579

= (7 × 7) mod 2579

= 49 mod 2579

= 49

2179^32 mod 2579 = [2179^16 mod 2579] × [2179^16 mod 2579] mod 2579

= (49 × 49) mod 2579

= 2401 mod 2579

= 2401

2179^64 mod 2579 = [2179^32 mod 2579] × [2179^32 mod 2579] mod 2579

= (2401 × 2401) mod 2579

= 5764801 mod 2579

= 736

2179^128 mod 2579 = [2179^64 mod 2579] × [2179^64 mod 2579] mod 2579

= (736 × 736) mod 2579

= 541696 mod 2579

= 106

2179^256 mod 2579 = [2179^128 mod 2579] × [2179^128 mod 2579] mod 2579

= (106 × 106) mod 2579

= 11236 mod 2579

= 920

2179^512 mod 2579 = [2179^256 mod 2579] × [2179^256 mod 2579] mod 2579

= (920 × 920) mod 2579

= 846400 mod 2579

= 488

2179^1024 mod 2579 = [2179^512 mod 2579] × [2179^512 mod 2579] mod 2579

= (488 × 488) mod 2579

= 238144 mod 2579

= 876

Menghitung hasil akhir 2179^1813 mod 2579:

2179^1813 mod 2579 = [2179^1024 mod 2579] × [2179^512 mod 2579] × [2179^256 mod 2579] × [2179^16 mod 2579] × [2179^4 mod 2579] × [2179^1 mod 2579] mod 2579

= (876 × 488 × 920 × 49 × 88 × 2179) mod 2579

= 3695283288238080 mod 2579

= 1135

Perhitungan: M = (1135 × 834) mod 2579

= 946590 mod 2579

= 97

Hasil Dekripsi Blok 9: y = 1135, M = 97

Blok 10 - Dekripsi dengan = 850, = 2535

850^1 mod 2579 = 850

850^2 mod 2579 = [850^1 mod 2579] × [850^1 mod 2579] mod 2579

= (850 × 850) mod 2579

= 722500 mod 2579

= 380

850^4 mod 2579 = [850^2 mod 2579] × [850^2 mod 2579] mod 2579

= (380 × 380) mod 2579

= 144400 mod 2579

= 2555

850^8 mod 2579 = [850^4 mod 2579] × [850^4 mod 2579] mod 2579

= (2555 × 2555) mod 2579

= 6528025 mod 2579

= 576

850^16 mod 2579 = [850^8 mod 2579] × [850^8 mod 2579] mod 2579

= (576 × 576) mod 2579

= 331776 mod 2579

= 1664

850^32 mod 2579 = [850^16 mod 2579] × [850^16 mod 2579] mod 2579

= (1664 × 1664) mod 2579

= 2768896 mod 2579

= 1629

850^64 mod 2579 = [850^32 mod 2579] × [850^32 mod 2579] mod 2579

= (1629 × 1629) mod 2579

= 2653641 mod 2579

= 2429

850^128 mod 2579 = [850^64 mod 2579] × [850^64 mod 2579] mod 2579

= (2429 × 2429) mod 2579

= 5900041 mod 2579

= 1868

850^256 mod 2579 = [850^128 mod 2579] × [850^128 mod 2579] mod 2579

= (1868 × 1868) mod 2579

= 3489424 mod 2579

= 37

850^512 mod 2579 = [850^256 mod 2579] × [850^256 mod 2579] mod 2579

= (37 × 37) mod 2579

= 1369 mod 2579

= 1369

850^1024 mod 2579 = [850^512 mod 2579] × [850^512 mod 2579] mod 2579

= (1369 × 1369) mod 2579

= 1874161 mod 2579

= 1807

Menghitung hasil akhir 850^1813 mod 2579:

850^1813 mod 2579 = [850^1024 mod 2579] × [850^512 mod 2579] × [850^256 mod 2579] × [850^16 mod 2579] × [850^4 mod 2579] × [850^1 mod 2579] mod 2579

= (1807 × 1369 × 37 × 1664 × 2555 × 850) mod 2579

= 330770276960032000 mod 2579

= 2225

Perhitungan: M = (2225 × 2535) mod 2579

= 5640375 mod 2579

= 102

Hasil Dekripsi Blok 10: y = 2225, M = 102

Blok 11 - Dekripsi dengan = 2, = 1643

2^1 mod 2579 = 2

2^2 mod 2579 = [2^1 mod 2579] × [2^1 mod 2579] mod 2579

= (2 × 2) mod 2579

= 4 mod 2579

= 4

2^4 mod 2579 = [2^2 mod 2579] × [2^2 mod 2579] mod 2579

= (4 × 4) mod 2579

= 16 mod 2579

= 16

2^8 mod 2579 = [2^4 mod 2579] × [2^4 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256 mod 2579

= 256

2^16 mod 2579 = [2^8 mod 2579] × [2^8 mod 2579] mod 2579

= (256 × 256) mod 2579

= 65536 mod 2579

= 1061

2^32 mod 2579 = [2^16 mod 2579] × [2^16 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1125721 mod 2579

= 1277

2^64 mod 2579 = [2^32 mod 2579] × [2^32 mod 2579] mod 2579

= (1277 × 1277) mod 2579

= 1630729 mod 2579

= 801

2^128 mod 2579 = [2^64 mod 2579] × [2^64 mod 2579] mod 2579

= (801 × 801) mod 2579

= 641601 mod 2579

= 2009

2^256 mod 2579 = [2^128 mod 2579] × [2^128 mod 2579] mod 2579

= (2009 × 2009) mod 2579

= 4036081 mod 2579

= 2525

2^512 mod 2579 = [2^256 mod 2579] × [2^256 mod 2579] mod 2579

= (2525 × 2525) mod 2579

= 6375625 mod 2579

= 337

2^1024 mod 2579 = [2^512 mod 2579] × [2^512 mod 2579] mod 2579

= (337 × 337) mod 2579

= 113569 mod 2579

= 93

Menghitung hasil akhir 2^1813 mod 2579:

2^1813 mod 2579 = [2^1024 mod 2579] × [2^512 mod 2579] × [2^256 mod 2579] × [2^16 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (93 × 337 × 2525 × 1061 × 16 × 2) mod 2579

= 2686826320800 mod 2579

= 1992

Perhitungan: M = (1992 × 1643) mod 2579

= 3272856 mod 2579

= 105

Hasil Dekripsi Blok 11: y = 1992, M = 105

Blok 12 - Dekripsi dengan = 1410, = 2379

1410^1 mod 2579 = 1410

1410^2 mod 2579 = [1410^1 mod 2579] × [1410^1 mod 2579] mod 2579

= (1410 × 1410) mod 2579

= 1988100 mod 2579

= 2270

1410^4 mod 2579 = [1410^2 mod 2579] × [1410^2 mod 2579] mod 2579

= (2270 × 2270) mod 2579

= 5152900 mod 2579

= 58

1410^8 mod 2579 = [1410^4 mod 2579] × [1410^4 mod 2579] mod 2579

= (58 × 58) mod 2579

= 3364 mod 2579

= 785

1410^16 mod 2579 = [1410^8 mod 2579] × [1410^8 mod 2579] mod 2579

= (785 × 785) mod 2579

= 616225 mod 2579

= 2423

1410^32 mod 2579 = [1410^16 mod 2579] × [1410^16 mod 2579] mod 2579

= (2423 × 2423) mod 2579

= 5870929 mod 2579

= 1125

1410^64 mod 2579 = [1410^32 mod 2579] × [1410^32 mod 2579] mod 2579

= (1125 × 1125) mod 2579

= 1265625 mod 2579

= 1915

1410^128 mod 2579 = [1410^64 mod 2579] × [1410^64 mod 2579] mod 2579

= (1915 × 1915) mod 2579

= 3667225 mod 2579

= 2466

1410^256 mod 2579 = [1410^128 mod 2579] × [1410^128 mod 2579] mod 2579

= (2466 × 2466) mod 2579

= 6081156 mod 2579

= 2453

1410^512 mod 2579 = [1410^256 mod 2579] × [1410^256 mod 2579] mod 2579

= (2453 × 2453) mod 2579

= 6017209 mod 2579

= 402

1410^1024 mod 2579 = [1410^512 mod 2579] × [1410^512 mod 2579] mod 2579

= (402 × 402) mod 2579

= 161604 mod 2579

= 1706

Menghitung hasil akhir 1410^1813 mod 2579:

1410^1813 mod 2579 = [1410^1024 mod 2579] × [1410^512 mod 2579] × [1410^256 mod 2579] × [1410^16 mod 2579] × [1410^4 mod 2579] × [1410^1 mod 2579] mod 2579

= (1706 × 402 × 2453 × 2423 × 58 × 1410) mod 2579

= 3333520640060978 40 mod 2579

= 103

Perhitungan: M = (103 × 2379) mod 2579

= 245037 mod 2579

= 32

Hasil Dekripsi Blok 12: y = 103, M = 32

Blok 13 - Dekripsi dengan = 8, = 692

8^1 mod 2579 = 8

8^2 mod 2579 = [8^1 mod 2579] × [8^1 mod 2579] mod 2579

= (8 × 8) mod 2579

= 64 mod 2579

= 64

8^4 mod 2579 = [8^2 mod 2579] × [8^2 mod 2579] mod 2579

= (64 × 64) mod 2579

= 4096 mod 2579

= 1517

8^8 mod 2579 = [8^4 mod 2579] × [8^4 mod 2579] mod 2579

= (1517 × 1517) mod 2579

= 2301289 mod 2579

= 821

8^16 mod 2579 = [8^8 mod 2579] × [8^8 mod 2579] mod 2579

= (821 × 821) mod 2579

= 674041 mod 2579

= 922

8^32 mod 2579 = [8^16 mod 2579] × [8^16 mod 2579] mod 2579

= (922 × 922) mod 2579

= 850084 mod 2579

= 1593

8^64 mod 2579 = [8^32 mod 2579] × [8^32 mod 2579] mod 2579

= (1593 × 1593) mod 2579

= 2537649 mod 2579

= 2492

8^128 mod 2579 = [8^64 mod 2579] × [8^64 mod 2579] mod 2579

= (2492 × 2492) mod 2579

= 6210064 mod 2579

= 2411

8^256 mod 2579 = [8^128 mod 2579] × [8^128 mod 2579] mod 2579

= (2411 × 2411) mod 2579

= 5812921 mod 2579

= 2434

8^512 mod 2579 = [8^256 mod 2579] × [8^256 mod 2579] mod 2579

= (2434 × 2434) mod 2579

= 5924356 mod 2579

= 393

8^1024 mod 2579 = [8^512 mod 2579] × [8^512 mod 2579] mod 2579

= (393 × 393) mod 2579

= 154449 mod 2579

= 2288

Menghitung hasil akhir 8^1813 mod 2579:

8^1813 mod 2579 = [8^1024 mod 2579] × [8^512 mod 2579] × [8^256 mod 2579] × [8^16 mod 2579] × [8^4 mod 2579] × [8^1 mod 2579] mod 2579

= (2288 × 393 × 2434 × 922 × 1517 × 8) mod 2579

= 24489258371415552 mod 2579

= 1230

Perhitungan: M = (1230 × 692) mod 2579

= 851160 mod 2579

= 90

Hasil Dekripsi Blok 13: y = 1230, M = 90

Blok 14 - Dekripsi dengan = 32, = 1845

32^1 mod 2579 = 32

32^2 mod 2579 = [32^1 mod 2579] × [32^1 mod 2579] mod 2579

= (32 × 32) mod 2579

= 1024 mod 2579

= 1024

32^4 mod 2579 = [32^2 mod 2579] × [32^2 mod 2579] mod 2579

= (1024 × 1024) mod 2579

= 1048576 mod 2579

= 1502

32^8 mod 2579 = [32^4 mod 2579] × [32^4 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

32^16 mod 2579 = [32^8 mod 2579] × [32^8 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

32^32 mod 2579 = [32^16 mod 2579] × [32^16 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

32^64 mod 2579 = [32^32 mod 2579] × [32^32 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

32^128 mod 2579 = [32^64 mod 2579] × [32^64 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

32^256 mod 2579 = [32^128 mod 2579] × [32^128 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

32^512 mod 2579 = [32^256 mod 2579] × [32^256 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

32^1024 mod 2579 = [32^512 mod 2579] × [32^512 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

Menghitung hasil akhir 32^1813 mod 2579:

32^1813 mod 2579 = [32^1024 mod 2579] × [32^512 mod 2579] × [32^256 mod 2579] × [32^16 mod 2579] × [32^4 mod 2579] × [32^1 mod 2579] mod 2579

= (245 × 443 × 136 × 1370 × 1502 × 32) mod 2579

= 971961801036800 mod 2579

= 2484

Perhitungan: M = (2484 × 1845) mod 2579

= 4582980 mod 2579

= 97

Hasil Dekripsi Blok 14: y = 2484, M = 97

Blok 15 - Dekripsi dengan = 2122, = 662

2122^1 mod 2579 = 2122

2122^2 mod 2579 = [2122^1 mod 2579] × [2122^1 mod 2579] mod 2579

= (2122 × 2122) mod 2579

= 4502884 mod 2579

= 2529

2122^4 mod 2579 = [2122^2 mod 2579] × [2122^2 mod 2579] mod 2579

= (2529 × 2529) mod 2579

= 6395841 mod 2579

= 2500

2122^8 mod 2579 = [2122^4 mod 2579] × [2122^4 mod 2579] mod 2579

= (2500 × 2500) mod 2579

= 6250000 mod 2579

= 1083

2122^16 mod 2579 = [2122^8 mod 2579] × [2122^8 mod 2579] mod 2579

= (1083 × 1083) mod 2579

= 1172889 mod 2579

= 2023

2122^32 mod 2579 = [2122^16 mod 2579] × [2122^16 mod 2579] mod 2579

= (2023 × 2023) mod 2579

= 4092529 mod 2579

= 2235

2122^64 mod 2579 = [2122^32 mod 2579] × [2122^32 mod 2579] mod 2579

= (2235 × 2235) mod 2579

= 4995225 mod 2579

= 2281

2122^128 mod 2579 = [2122^64 mod 2579] × [2122^64 mod 2579] mod 2579

= (2281 × 2281) mod 2579

= 5202961 mod 2579

= 1118

2122^256 mod 2579 = [2122^128 mod 2579] × [2122^128 mod 2579] mod 2579

= (1118 × 1118) mod 2579

= 1249924 mod 2579

= 1688

2122^512 mod 2579 = [2122^256 mod 2579] × [2122^256 mod 2579] mod 2579

= (1688 × 1688) mod 2579

= 2849344 mod 2579

= 2128

2122^1024 mod 2579 = [2122^512 mod 2579] × [2122^512 mod 2579] mod 2579

= (2128 × 2128) mod 2579

= 4528384 mod 2579

= 2239

Menghitung hasil akhir 2122^1813 mod 2579:

2122^1813 mod 2579 = [2122^1024 mod 2579] × [2122^512 mod 2579] × [2122^256 mod 2579] × [2122^16 mod 2579] × [2122^4 mod 2579] × [2122^1 mod 2579] mod 2579

= (2239 × 2128 × 1688 × 2023 × 2500 × 2122) mod 2579

= 86313639708141440000 mod 2579

= 791

Perhitungan: M = (791 × 662) mod 2579

= 523642 mod 2579

= 105

Hasil Dekripsi Blok 15: y = 791, M = 105

Blok 16 - Dekripsi dengan = 2529, = 1561

2529^1 mod 2579 = 2529

2529^2 mod 2579 = [2529^1 mod 2579] × [2529^1 mod 2579] mod 2579

= (2529 × 2529) mod 2579

= 6395841 mod 2579

= 2500

2529^4 mod 2579 = [2529^2 mod 2579] × [2529^2 mod 2579] mod 2579

= (2500 × 2500) mod 2579

= 6250000 mod 2579

= 1083

2529^8 mod 2579 = [2529^4 mod 2579] × [2529^4 mod 2579] mod 2579

= (1083 × 1083) mod 2579

= 1172889 mod 2579

= 2023

2529^16 mod 2579 = [2529^8 mod 2579] × [2529^8 mod 2579] mod 2579

= (2023 × 2023) mod 2579

= 4092529 mod 2579

= 2235

2529^32 mod 2579 = [2529^16 mod 2579] × [2529^16 mod 2579] mod 2579

= (2235 × 2235) mod 2579

= 4995225 mod 2579

= 2281

2529^64 mod 2579 = [2529^32 mod 2579] × [2529^32 mod 2579] mod 2579

= (2281 × 2281) mod 2579

= 5202961 mod 2579

= 1118

2529^128 mod 2579 = [2529^64 mod 2579] × [2529^64 mod 2579] mod 2579

= (1118 × 1118) mod 2579

= 1249924 mod 2579

= 1688

2529^256 mod 2579 = [2529^128 mod 2579] × [2529^128 mod 2579] mod 2579

= (1688 × 1688) mod 2579

= 2849344 mod 2579

= 2128

2529^512 mod 2579 = [2529^256 mod 2579] × [2529^256 mod 2579] mod 2579

= (2128 × 2128) mod 2579

= 4528384 mod 2579

= 2239

2529^1024 mod 2579 = [2529^512 mod 2579] × [2529^512 mod 2579] mod 2579

= (2239 × 2239) mod 2579

= 5013121 mod 2579

= 2124

Menghitung hasil akhir 2529^1813 mod 2579:

2529^1813 mod 2579 = [2529^1024 mod 2579] × [2529^512 mod 2579] × [2529^256 mod 2579] × [2529^16 mod 2579] × [2529^4 mod 2579] × [2529^1 mod 2579] mod 2579

= (2124 × 2239 × 2128 × 2235 × 1083 × 2529) mod 2579

= 61949105954754500160 mod 2579

= 1563

Perhitungan: M = (1563 × 1561) mod 2579

= 2439843 mod 2579

= 109

Hasil Dekripsi Blok 16: y = 1563, M = 109

Blok 17 - Dekripsi dengan = 16, = 985

16^1 mod 2579 = 16

16^2 mod 2579 = [16^1 mod 2579] × [16^1 mod 2579] mod 2579

= (16 × 16) mod 2579

= 256 mod 2579

= 256

16^4 mod 2579 = [16^2 mod 2579] × [16^2 mod 2579] mod 2579

= (256 × 256) mod 2579

= 65536 mod 2579

= 1061

16^8 mod 2579 = [16^4 mod 2579] × [16^4 mod 2579] mod 2579

= (1061 × 1061) mod 2579

= 1125721 mod 2579

= 1277

16^16 mod 2579 = [16^8 mod 2579] × [16^8 mod 2579] mod 2579

= (1277 × 1277) mod 2579

= 1630729 mod 2579

= 801

16^32 mod 2579 = [16^16 mod 2579] × [16^16 mod 2579] mod 2579

= (801 × 801) mod 2579

= 641601 mod 2579

= 2009

16^64 mod 2579 = [16^32 mod 2579] × [16^32 mod 2579] mod 2579

= (2009 × 2009) mod 2579

= 4036081 mod 2579

= 2525

16^128 mod 2579 = [16^64 mod 2579] × [16^64 mod 2579] mod 2579

= (2525 × 2525) mod 2579

= 6375625 mod 2579

= 337

16^256 mod 2579 = [16^128 mod 2579] × [16^128 mod 2579] mod 2579

= (337 × 337) mod 2579

= 113569 mod 2579

= 93

16^512 mod 2579 = [16^256 mod 2579] × [16^256 mod 2579] mod 2579

= (93 × 93) mod 2579

= 8649 mod 2579

= 912

16^1024 mod 2579 = [16^512 mod 2579] × [16^512 mod 2579] mod 2579

= (912 × 912) mod 2579

= 831744 mod 2579

= 1306

Menghitung hasil akhir 16^1813 mod 2579:

16^1813 mod 2579 = [16^1024 mod 2579] × [16^512 mod 2579] × [16^256 mod 2579] × [16^16 mod 2579] × [16^4 mod 2579] × [16^1 mod 2579] mod 2579

= (1306 × 912 × 93 × 801 × 1061 × 16) mod 2579

= 1506221513796096 mod 2579

= 110

Perhitungan: M = (110 × 985) mod 2579

= 108350 mod 2579

= 32

Hasil Dekripsi Blok 17: y = 110, M = 32

Blok 18 - Dekripsi dengan = 1109, = 1485

1109^1 mod 2579 = 1109

1109^2 mod 2579 = [1109^1 mod 2579] × [1109^1 mod 2579] mod 2579

= (1109 × 1109) mod 2579

= 1229881 mod 2579

= 2277

1109^4 mod 2579 = [1109^2 mod 2579] × [1109^2 mod 2579] mod 2579

= (2277 × 2277) mod 2579

= 5184729 mod 2579

= 939

1109^8 mod 2579 = [1109^4 mod 2579] × [1109^4 mod 2579] mod 2579

= (939 × 939) mod 2579

= 881721 mod 2579

= 2282

1109^16 mod 2579 = [1109^8 mod 2579] × [1109^8 mod 2579] mod 2579

= (2282 × 2282) mod 2579

= 5207524 mod 2579

= 523

1109^32 mod 2579 = [1109^16 mod 2579] × [1109^16 mod 2579] mod 2579

= (523 × 523) mod 2579

= 273529 mod 2579

= 155

1109^64 mod 2579 = [1109^32 mod 2579] × [1109^32 mod 2579] mod 2579

= (155 × 155) mod 2579

= 24025 mod 2579

= 814

1109^128 mod 2579 = [1109^64 mod 2579] × [1109^64 mod 2579] mod 2579

= (814 × 814) mod 2579

= 662596 mod 2579

= 2372

1109^256 mod 2579 = [1109^128 mod 2579] × [1109^128 mod 2579] mod 2579

= (2372 × 2372) mod 2579

= 5626384 mod 2579

= 1585

1109^512 mod 2579 = [1109^256 mod 2579] × [1109^256 mod 2579] mod 2579

= (1585 × 1585) mod 2579

= 2512225 mod 2579

= 279

1109^1024 mod 2579 = [1109^512 mod 2579] × [1109^512 mod 2579] mod 2579

= (279 × 279) mod 2579

= 77841 mod 2579

= 471

Menghitung hasil akhir 1109^1813 mod 2579:

1109^1813 mod 2579 = [1109^1024 mod 2579] × [1109^512 mod 2579] × [1109^256 mod 2579] × [1109^16 mod 2579] × [1109^4 mod 2579] × [1109^1 mod 2579] mod 2579

= (471 × 279 × 1585 × 523 × 939 × 1109) mod 2579

= 113436600830200845 mod 2579

= 73

Perhitungan: M = (73 × 1485) mod 2579

= 108405 mod 2579

= 87

Hasil Dekripsi Blok 18: y = 73, M = 87

Blok 19 - Dekripsi dengan = 1779, = 1258

1779^1 mod 2579 = 1779

1779^2 mod 2579 = [1779^1 mod 2579] × [1779^1 mod 2579] mod 2579

= (1779 × 1779) mod 2579

= 3164841 mod 2579

= 408

1779^4 mod 2579 = [1779^2 mod 2579] × [1779^2 mod 2579] mod 2579

= (408 × 408) mod 2579

= 166464 mod 2579

= 1408

1779^8 mod 2579 = [1779^4 mod 2579] × [1779^4 mod 2579] mod 2579

= (1408 × 1408) mod 2579

= 1982464 mod 2579

= 1792

1779^16 mod 2579 = [1779^8 mod 2579] × [1779^8 mod 2579] mod 2579

= (1792 × 1792) mod 2579

= 3211264 mod 2579

= 409

1779^32 mod 2579 = [1779^16 mod 2579] × [1779^16 mod 2579] mod 2579

= (409 × 409) mod 2579

= 167281 mod 2579

= 2225

1779^64 mod 2579 = [1779^32 mod 2579] × [1779^32 mod 2579] mod 2579

= (2225 × 2225) mod 2579

= 4950625 mod 2579

= 1524

1779^128 mod 2579 = [1779^64 mod 2579] × [1779^64 mod 2579] mod 2579

= (1524 × 1524) mod 2579

= 2322576 mod 2579

= 1476

1779^256 mod 2579 = [1779^128 mod 2579] × [1779^128 mod 2579] mod 2579

= (1476 × 1476) mod 2579

= 2178576 mod 2579

= 1900

1779^512 mod 2579 = [1779^256 mod 2579] × [1779^256 mod 2579] mod 2579

= (1900 × 1900) mod 2579

= 3610000 mod 2579

= 1979

1779^1024 mod 2579 = [1779^512 mod 2579] × [1779^512 mod 2579] mod 2579

= (1979 × 1979) mod 2579

= 3916441 mod 2579

= 1519

Menghitung hasil akhir 1779^1813 mod 2579:

1779^1813 mod 2579 = [1779^1024 mod 2579] × [1779^512 mod 2579] × [1779^256 mod 2579] × [1779^16 mod 2579] × [1779^4 mod 2579] × [1779^1 mod 2579] mod 2579

= (1519 × 1979 × 1900 × 409 × 1408 × 1779) mod 2579

= 5851390468282867200 mod 2579

= 1716

Perhitungan: M = (1716 × 1258) mod 2579

= 2158728 mod 2579

= 105

Hasil Dekripsi Blok 19: y = 1716, M = 105

Blok 20 - Dekripsi dengan = 482, = 329

482^1 mod 2579 = 482

482^2 mod 2579 = [482^1 mod 2579] × [482^1 mod 2579] mod 2579

= (482 × 482) mod 2579

= 232324 mod 2579

= 214

482^4 mod 2579 = [482^2 mod 2579] × [482^2 mod 2579] mod 2579

= (214 × 214) mod 2579

= 45796 mod 2579

= 1953

482^8 mod 2579 = [482^4 mod 2579] × [482^4 mod 2579] mod 2579

= (1953 × 1953) mod 2579

= 3814209 mod 2579

= 2447

482^16 mod 2579 = [482^8 mod 2579] × [482^8 mod 2579] mod 2579

= (2447 × 2447) mod 2579

= 5987809 mod 2579

= 1950

482^32 mod 2579 = [482^16 mod 2579] × [482^16 mod 2579] mod 2579

= (1950 × 1950) mod 2579

= 3802500 mod 2579

= 1054

482^64 mod 2579 = [482^32 mod 2579] × [482^32 mod 2579] mod 2579

= (1054 × 1054) mod 2579

= 1110916 mod 2579

= 1946

482^128 mod 2579 = [482^64 mod 2579] × [482^64 mod 2579] mod 2579

= (1946 × 1946) mod 2579

= 3786916 mod 2579

= 944

482^256 mod 2579 = [482^128 mod 2579] × [482^128 mod 2579] mod 2579

= (944 × 944) mod 2579

= 891136 mod 2579

= 1381

482^512 mod 2579 = [482^256 mod 2579] × [482^256 mod 2579] mod 2579

= (1381 × 1381) mod 2579

= 1907161 mod 2579

= 1280

482^1024 mod 2579 = [482^512 mod 2579] × [482^512 mod 2579] mod 2579

= (1280 × 1280) mod 2579

= 1638400 mod 2579

= 735

Menghitung hasil akhir 482^1813 mod 2579:

482^1813 mod 2579 = [482^1024 mod 2579] × [482^512 mod 2579] × [482^256 mod 2579] × [482^16 mod 2579] × [482^4 mod 2579] × [482^1 mod 2579] mod 2579

= (735 × 1280 × 1381 × 1950 × 1953 × 482) mod 2579

= 2384925846226560000 mod 2579

= 988

Perhitungan: M = (988 × 329) mod 2579

= 325052 mod 2579

= 98

Hasil Dekripsi Blok 20: y = 988, M = 98

Blok 21 - Dekripsi dengan = 32, = 1492

32^1 mod 2579 = 32

32^2 mod 2579 = [32^1 mod 2579] × [32^1 mod 2579] mod 2579

= (32 × 32) mod 2579

= 1024 mod 2579

= 1024

32^4 mod 2579 = [32^2 mod 2579] × [32^2 mod 2579] mod 2579

= (1024 × 1024) mod 2579

= 1048576 mod 2579

= 1502

32^8 mod 2579 = [32^4 mod 2579] × [32^4 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

32^16 mod 2579 = [32^8 mod 2579] × [32^8 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

32^32 mod 2579 = [32^16 mod 2579] × [32^16 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

32^64 mod 2579 = [32^32 mod 2579] × [32^32 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

32^128 mod 2579 = [32^64 mod 2579] × [32^64 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

32^256 mod 2579 = [32^128 mod 2579] × [32^128 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

32^512 mod 2579 = [32^256 mod 2579] × [32^256 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

32^1024 mod 2579 = [32^512 mod 2579] × [32^512 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

Menghitung hasil akhir 32^1813 mod 2579:

32^1813 mod 2579 = [32^1024 mod 2579] × [32^512 mod 2579] × [32^256 mod 2579] × [32^16 mod 2579] × [32^4 mod 2579] × [32^1 mod 2579] mod 2579

= (245 × 443 × 136 × 1370 × 1502 × 32) mod 2579

= 971961801036800 mod 2579

= 2484

Perhitungan: M = (2484 × 1492) mod 2579

= 3706128 mod 2579

= 105

Hasil Dekripsi Blok 21: y = 2484, M = 105

Blok 22 - Dekripsi dengan = 1024, = 783

1024^1 mod 2579 = 1024

1024^2 mod 2579 = [1024^1 mod 2579] × [1024^1 mod 2579] mod 2579

= (1024 × 1024) mod 2579

= 1048576 mod 2579

= 1502

1024^4 mod 2579 = [1024^2 mod 2579] × [1024^2 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

1024^8 mod 2579 = [1024^4 mod 2579] × [1024^4 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

1024^16 mod 2579 = [1024^8 mod 2579] × [1024^8 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

1024^32 mod 2579 = [1024^16 mod 2579] × [1024^16 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

1024^64 mod 2579 = [1024^32 mod 2579] × [1024^32 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

1024^128 mod 2579 = [1024^64 mod 2579] × [1024^64 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

1024^256 mod 2579 = [1024^128 mod 2579] × [1024^128 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

1024^512 mod 2579 = [1024^256 mod 2579] × [1024^256 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

1024^1024 mod 2579 = [1024^512 mod 2579] × [1024^512 mod 2579] mod 2579

= (245 × 245) mod 2579

= 60025 mod 2579

= 708

Menghitung hasil akhir 1024^1813 mod 2579:

1024^1813 mod 2579 = [1024^1024 mod 2579] × [1024^512 mod 2579] × [1024^256 mod 2579] × [1024^16 mod 2579] × [1024^4 mod 2579] × [1024^1 mod 2579] mod 2579

= (708 × 245 × 443 × 1967 × 1958 × 1024) mod 2579

= 303054036063313920 mod 2579

= 1288

Perhitungan: M = (1288 × 783) mod 2579

= 1008504 mod 2579

= 115

Hasil Dekripsi Blok 22: y = 1288, M = 115

Blok 23 - Dekripsi dengan = 1779, = 1772

1779^1 mod 2579 = 1779

1779^2 mod 2579 = [1779^1 mod 2579] × [1779^1 mod 2579] mod 2579

= (1779 × 1779) mod 2579

= 3164841 mod 2579

= 408

1779^4 mod 2579 = [1779^2 mod 2579] × [1779^2 mod 2579] mod 2579

= (408 × 408) mod 2579

= 166464 mod 2579

= 1408

1779^8 mod 2579 = [1779^4 mod 2579] × [1779^4 mod 2579] mod 2579

= (1408 × 1408) mod 2579

= 1982464 mod 2579

= 1792

1779^16 mod 2579 = [1779^8 mod 2579] × [1779^8 mod 2579] mod 2579

= (1792 × 1792) mod 2579

= 3211264 mod 2579

= 409

1779^32 mod 2579 = [1779^16 mod 2579] × [1779^16 mod 2579] mod 2579

= (409 × 409) mod 2579

= 167281 mod 2579

= 2225

1779^64 mod 2579 = [1779^32 mod 2579] × [1779^32 mod 2579] mod 2579

= (2225 × 2225) mod 2579

= 4950625 mod 2579

= 1524

1779^128 mod 2579 = [1779^64 mod 2579] × [1779^64 mod 2579] mod 2579

= (1524 × 1524) mod 2579

= 2322576 mod 2579

= 1476

1779^256 mod 2579 = [1779^128 mod 2579] × [1779^128 mod 2579] mod 2579

= (1476 × 1476) mod 2579

= 2178576 mod 2579

= 1900

1779^512 mod 2579 = [1779^256 mod 2579] × [1779^256 mod 2579] mod 2579

= (1900 × 1900) mod 2579

= 3610000 mod 2579

= 1979

1779^1024 mod 2579 = [1779^512 mod 2579] × [1779^512 mod 2579] mod 2579

= (1979 × 1979) mod 2579

= 3916441 mod 2579

= 1519

Menghitung hasil akhir 1779^1813 mod 2579:

1779^1813 mod 2579 = [1779^1024 mod 2579] × [1779^512 mod 2579] × [1779^256 mod 2579] × [1779^16 mod 2579] × [1779^4 mod 2579] × [1779^1 mod 2579] mod 2579

= (1519 × 1979 × 1900 × 409 × 1408 × 1779) mod 2579

= 5851390468282867200 mod 2579

= 1716

Perhitungan: M = (1716 × 1772) mod 2579

= 3040752 mod 2579

= 111

Hasil Dekripsi Blok 23: y = 1716, M = 111

Blok 24 - Dekripsi dengan = 821, = 287

821^1 mod 2579 = 821

821^2 mod 2579 = [821^1 mod 2579] × [821^1 mod 2579] mod 2579

= (821 × 821) mod 2579

= 674041 mod 2579

= 922

821^4 mod 2579 = [821^2 mod 2579] × [821^2 mod 2579] mod 2579

= (922 × 922) mod 2579

= 850084 mod 2579

= 1593

821^8 mod 2579 = [821^4 mod 2579] × [821^4 mod 2579] mod 2579

= (1593 × 1593) mod 2579

= 2537649 mod 2579

= 2492

821^16 mod 2579 = [821^8 mod 2579] × [821^8 mod 2579] mod 2579

= (2492 × 2492) mod 2579

= 6210064 mod 2579

= 2411

821^32 mod 2579 = [821^16 mod 2579] × [821^16 mod 2579] mod 2579

= (2411 × 2411) mod 2579

= 5812921 mod 2579

= 2434

821^64 mod 2579 = [821^32 mod 2579] × [821^32 mod 2579] mod 2579

= (2434 × 2434) mod 2579

= 5924356 mod 2579

= 393

821^128 mod 2579 = [821^64 mod 2579] × [821^64 mod 2579] mod 2579

= (393 × 393) mod 2579

= 154449 mod 2579

= 2288

821^256 mod 2579 = [821^128 mod 2579] × [821^128 mod 2579] mod 2579

= (2288 × 2288) mod 2579

= 5234944 mod 2579

= 2153

821^512 mod 2579 = [821^256 mod 2579] × [821^256 mod 2579] mod 2579

= (2153 × 2153) mod 2579

= 4635409 mod 2579

= 946

821^1024 mod 2579 = [821^512 mod 2579] × [821^512 mod 2579] mod 2579

= (946 × 946) mod 2579

= 894916 mod 2579

= 3

Menghitung hasil akhir 821^1813 mod 2579:

821^1813 mod 2579 = [821^1024 mod 2579] × [821^512 mod 2579] × [821^256 mod 2579] × [821^16 mod 2579] × [821^4 mod 2579] × [821^1 mod 2579] mod 2579

= (3 × 946 × 2153 × 2411 × 1593 × 821) mod 2579

= 19266931984116762 mod 2579

= 1537

Perhitungan: M = (1537 × 287) mod 2579

= 441119 mod 2579

= 110

Hasil Dekripsi Blok 24: y = 1537, M = 110

Blok 25 - Dekripsi dengan = 979, = 120

979^1 mod 2579 = 979

979^2 mod 2579 = [979^1 mod 2579] × [979^1 mod 2579] mod 2579

= (979 × 979) mod 2579

= 958441 mod 2579

= 1632

979^4 mod 2579 = [979^2 mod 2579] × [979^2 mod 2579] mod 2579

= (1632 × 1632) mod 2579

= 2663424 mod 2579

= 1896

979^8 mod 2579 = [979^4 mod 2579] × [979^4 mod 2579] mod 2579

= (1896 × 1896) mod 2579

= 3594816 mod 2579

= 2269

979^16 mod 2579 = [979^8 mod 2579] × [979^8 mod 2579] mod 2579

= (2269 × 2269) mod 2579

= 5148361 mod 2579

= 677

979^32 mod 2579 = [979^16 mod 2579] × [979^16 mod 2579] mod 2579

= (677 × 677) mod 2579

= 458329 mod 2579

= 1846

979^64 mod 2579 = [979^32 mod 2579] × [979^32 mod 2579] mod 2579

= (1846 × 1846) mod 2579

= 3407716 mod 2579

= 857

979^128 mod 2579 = [979^64 mod 2579] × [979^64 mod 2579] mod 2579

= (857 × 857) mod 2579

= 734449 mod 2579

= 2013

979^256 mod 2579 = [979^128 mod 2579] × [979^128 mod 2579] mod 2579

= (2013 × 2013) mod 2579

= 4052169 mod 2579

= 560

979^512 mod 2579 = [979^256 mod 2579] × [979^256 mod 2579] mod 2579

= (560 × 560) mod 2579

= 313600 mod 2579

= 1541

979^1024 mod 2579 = [979^512 mod 2579] × [979^512 mod 2579] mod 2579

= (1541 × 1541) mod 2579

= 2374681 mod 2579

= 2001

Menghitung hasil akhir 979^1813 mod 2579:

979^1813 mod 2579 = [979^1024 mod 2579] × [979^512 mod 2579] × [979^256 mod 2579] × [979^16 mod 2579] × [979^4 mod 2579] × [979^1 mod 2579] mod 2579

= (2001 × 1541 × 560 × 677 × 1896 × 979) mod 2579

= 2169938612535281280 mod 2579

= 1097

Perhitungan: M = (1097 × 120) mod 2579

= 131640 mod 2579

= 111

Hasil Dekripsi Blok 25: y = 1097, M = 111