LAPORAN HASIL ENKRIPSI & DEKRIPSI

Nama: Azka Hafiyan Kahfi Ahshoni

NIM: 202410370110222

Kelas: Informatika E

PROSES ENKRIPSI EL GAMAL:

Blok 1 - ASCII: 65 (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 × 65 mod 2579

= 120900 mod 2579

= 2266

Hasil Enkripsi Blok 1: ASCII (M) = 65, = 910, = 2266

Blok 2 - ASCII: 90 (k = 13)

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 2^13 mod 2579:

2^13 mod 2579 = [2^8 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (256 × 16 × 2) mod 2579

= 8192 mod 2579

= 455

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 949^13 mod 2579:

949^13 mod 2579 = [949^8 mod 2579] × [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (678 × 2368 × 949) mod 2579

= 1523623296 mod 2579

= 1676

949^13 mod 2579 = 1676

949^13 × 90 mod 2579

= 150840 mod 2579

= 1258

Hasil Enkripsi Blok 2: ASCII (M) = 90, = 455, = 1258

Blok 3 - ASCII: 75 (k = 7)

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 2^7 mod 2579:

2^7 mod 2579 = [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (16 × 4 × 2) mod 2579

= 128 mod 2579

= 128

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 949^7 mod 2579:

949^7 mod 2579 = [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (2368 × 530 × 949) mod 2579

= 1191032960 mod 2579

= 1759

949^7 mod 2579 = 1759

949^7 × 75 mod 2579

= 131925 mod 2579

= 396

Hasil Enkripsi Blok 3: ASCII (M) = 75, = 128, = 396

Blok 4 - ASCII: 65 (k = 36)

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 2^36 mod 2579:

2^36 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] mod 2579

= (1277 × 16) mod 2579

= 20432 mod 2579

= 2379

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 949^36 mod 2579:

949^36 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] mod 2579

= (34 × 2368) mod 2579

= 80512 mod 2579

= 563

949^36 mod 2579 = 563

949^36 × 65 mod 2579

= 36595 mod 2579

= 489

Hasil Enkripsi Blok 4: ASCII (M) = 65, = 2379, = 489

Blok 5 - ASCII: 32 (k = 33)

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 2^33 mod 2579:

2^33 mod 2579 = [2^32 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 2) mod 2579

= 2554 mod 2579

= 2554

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 949^33 mod 2579:

949^33 mod 2579 = [949^32 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 949) mod 2579

= 32266 mod 2579

= 1318

949^33 mod 2579 = 1318

949^33 × 32 mod 2579

= 42176 mod 2579

= 912

Hasil Enkripsi Blok 5: ASCII (M) = 32, = 2554, = 912

Blok 6 - ASCII: 72 (k = 18)

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 2^18 mod 2579:

2^18 mod 2579 = [2^16 mod 2579] × [2^2 mod 2579] mod 2579

= (1061 × 4) mod 2579

= 4244 mod 2579

= 1665

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 949^18 mod 2579:

949^18 mod 2579 = [949^16 mod 2579] × [949^2 mod 2579] mod 2579

= (622 × 530) mod 2579

= 329660 mod 2579

= 2127

949^18 mod 2579 = 2127

949^18 × 72 mod 2579

= 153144 mod 2579

= 983

Hasil Enkripsi Blok 6: ASCII (M) = 72, = 1665, = 983

Blok 7 - ASCII: 65 (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 × 65 mod 2579

= 81315 mod 2579

= 1366

Hasil Enkripsi Blok 7: ASCII (M) = 65, = 512, = 1366

Blok 8 - ASCII: 70 (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 × 70 mod 2579

= 17220 mod 2579

= 1746

Hasil Enkripsi Blok 8: ASCII (M) = 70, = 760, = 1746

Blok 9 - ASCII: 73 (k = 40)

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 2^40 mod 2579:

2^40 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] mod 2579

= (1277 × 256) mod 2579

= 326912 mod 2579

= 1958

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 949^40 mod 2579:

949^40 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] mod 2579

= (34 × 678) mod 2579

= 23052 mod 2579

= 2420

949^40 mod 2579 = 2420

949^40 × 73 mod 2579

= 176660 mod 2579

= 1288

Hasil Enkripsi Blok 9: ASCII (M) = 73, = 1958, = 1288

Blok 10 - ASCII: 89 (k = 43)

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 2^43 mod 2579:

2^43 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 256 × 4 × 2) mod 2579

= 2615296 mod 2579

= 190

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 949^43 mod 2579:

949^43 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 678 × 530 × 949) mod 2579

= 11594464440 mod 2579

= 2560

949^43 mod 2579 = 2560

949^43 × 89 mod 2579

= 227840 mod 2579

= 888

Hasil Enkripsi Blok 10: ASCII (M) = 89, = 190, = 888

Blok 11 - ASCII: 65 (k = 47)

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 2^47 mod 2579:

2^47 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 256 × 16 × 4 × 2) mod 2579

= 41844736 mod 2579

= 461

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 949^47 mod 2579:

949^47 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 678 × 2368 × 530 × 949) mod 2579

= 27455691793920 mod 2579

= 1430

949^47 mod 2579 = 1430

949^47 × 65 mod 2579

= 92950 mod 2579

= 106

Hasil Enkripsi Blok 11: ASCII (M) = 65, = 461, = 106

Blok 12 - ASCII: 78 (k = 15)

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 2^15 mod 2579:

2^15 mod 2579 = [2^8 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (256 × 16 × 4 × 2) mod 2579

= 32768 mod 2579

= 1820

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 949^15 mod 2579:

949^15 mod 2579 = [949^8 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (678 × 2368 × 530 × 949) mod 2579

= 807520346880 mod 2579

= 1104

949^15 mod 2579 = 1104

949^15 × 78 mod 2579

= 86112 mod 2579

= 1005

Hasil Enkripsi Blok 12: ASCII (M) = 78, = 1820, = 1005

Blok 13 - 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 13: ASCII (M) = 32, = 32, = 1167

Blok 14 - ASCII: 75 (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 × 75 mod 2579

= 177600 mod 2579

= 2228

Hasil Enkripsi Blok 14: ASCII (M) = 75, = 16, = 2228

Blok 15 - ASCII: 65 (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 × 65 mod 2579

= 87035 mod 2579

= 1928

Hasil Enkripsi Blok 15: ASCII (M) = 65, = 821, = 1928

Blok 16 - ASCII: 72 (k = 13)

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 2^13 mod 2579:

2^13 mod 2579 = [2^8 mod 2579] × [2^4 mod 2579] × [2^1 mod 2579] mod 2579

= (256 × 16 × 2) mod 2579

= 8192 mod 2579

= 455

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 949^13 mod 2579:

949^13 mod 2579 = [949^8 mod 2579] × [949^4 mod 2579] × [949^1 mod 2579] mod 2579

= (678 × 2368 × 949) mod 2579

= 1523623296 mod 2579

= 1676

949^13 mod 2579 = 1676

949^13 × 72 mod 2579

= 120672 mod 2579

= 2038

Hasil Enkripsi Blok 16: ASCII (M) = 72, = 455, = 2038

Blok 17 - ASCII: 70 (k = 36)

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 2^36 mod 2579:

2^36 mod 2579 = [2^32 mod 2579] × [2^4 mod 2579] mod 2579

= (1277 × 16) mod 2579

= 20432 mod 2579

= 2379

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 949^36 mod 2579:

949^36 mod 2579 = [949^32 mod 2579] × [949^4 mod 2579] mod 2579

= (34 × 2368) mod 2579

= 80512 mod 2579

= 563

949^36 mod 2579 = 563

949^36 × 70 mod 2579

= 39410 mod 2579

= 725

Hasil Enkripsi Blok 17: ASCII (M) = 70, = 2379, = 725

Blok 18 - ASCII: 73 (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 × 73 mod 2579

= 4745 mod 2579

= 2166

Hasil Enkripsi Blok 18: ASCII (M) = 73, = 8, = 2166

Blok 19 - ASCII: 32 (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 × 32 mod 2579

= 40032 mod 2579

= 1347

Hasil Enkripsi Blok 19: ASCII (M) = 32, = 512, = 1347

Blok 20 - ASCII: 65 (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 × 65 mod 2579

= 36140 mod 2579

= 34

Hasil Enkripsi Blok 20: ASCII (M) = 65, = 482, = 34

Blok 21 - ASCII: 72 (k = 23)

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 2^23 mod 2579:

2^23 mod 2579 = [2^16 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (1061 × 16 × 4 × 2) mod 2579

= 135808 mod 2579

= 1700

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 949^23 mod 2579:

949^23 mod 2579 = [949^16 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (622 × 2368 × 530 × 949) mod 2579

= 740822501120 mod 2579

= 602

949^23 mod 2579 = 602

949^23 × 72 mod 2579

= 43344 mod 2579

= 2080

Hasil Enkripsi Blok 21: ASCII (M) = 72, = 1700, = 2080

Blok 22 - ASCII: 83 (k = 33)

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 2^33 mod 2579:

2^33 mod 2579 = [2^32 mod 2579] × [2^1 mod 2579] mod 2579

= (1277 × 2) mod 2579

= 2554 mod 2579

= 2554

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 949^33 mod 2579:

949^33 mod 2579 = [949^32 mod 2579] × [949^1 mod 2579] mod 2579

= (34 × 949) mod 2579

= 32266 mod 2579

= 1318

949^33 mod 2579 = 1318

949^33 × 83 mod 2579

= 109394 mod 2579

= 1076

Hasil Enkripsi Blok 22: ASCII (M) = 83, = 2554, = 1076

Blok 23 - ASCII: 72 (k = 25)

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 2^25 mod 2579:

2^25 mod 2579 = [2^16 mod 2579] × [2^8 mod 2579] × [2^1 mod 2579] mod 2579

= (1061 × 256 × 2) mod 2579

= 543232 mod 2579

= 1642

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 949^25 mod 2579:

949^25 mod 2579 = [949^16 mod 2579] × [949^8 mod 2579] × [949^1 mod 2579] mod 2579

= (622 × 678 × 949) mod 2579

= 400208484 mod 2579

= 1843

949^25 mod 2579 = 1843

949^25 × 72 mod 2579

= 132696 mod 2579

= 1167

Hasil Enkripsi Blok 23: ASCII (M) = 72, = 1642, = 1167

Blok 24 - ASCII: 79 (k = 15)

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 2^15 mod 2579:

2^15 mod 2579 = [2^8 mod 2579] × [2^4 mod 2579] × [2^2 mod 2579] × [2^1 mod 2579] mod 2579

= (256 × 16 × 4 × 2) mod 2579

= 32768 mod 2579

= 1820

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 949^15 mod 2579:

949^15 mod 2579 = [949^8 mod 2579] × [949^4 mod 2579] × [949^2 mod 2579] × [949^1 mod 2579] mod 2579

= (678 × 2368 × 530 × 949) mod 2579

= 807520346880 mod 2579

= 1104

949^15 mod 2579 = 1104

949^15 × 79 mod 2579

= 87216 mod 2579

= 2109

Hasil Enkripsi Blok 24: ASCII (M) = 79, = 1820, = 2109

Blok 25 - ASCII: 78 (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 × 78 mod 2579

= 5070 mod 2579

= 2491

Hasil Enkripsi Blok 25: ASCII (M) = 78, = 8, = 2491

Blok 26 - ASCII: 73 (k = 20)

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 2^20 mod 2579:

2^20 mod 2579 = [2^16 mod 2579] × [2^4 mod 2579] mod 2579

= (1061 × 16) mod 2579

= 16976 mod 2579

= 1502

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 949^20 mod 2579:

949^20 mod 2579 = [949^16 mod 2579] × [949^4 mod 2579] mod 2579

= (622 × 2368) mod 2579

= 1472896 mod 2579

= 287

949^20 mod 2579 = 287

949^20 × 73 mod 2579

= 20951 mod 2579

= 319

Hasil Enkripsi Blok 26: ASCII (M) = 73, = 1502, = 319

ChipherText:

(910, 2266) (455, 1258) (128, 396) (2379, 489) (2554, 912) (1665, 983) (512, 1366) (760, 1746) (1958, 1288) (190, 888) (461, 106) (1820, 1005) (32, 1167) (16, 2228) (821, 1928) (455, 2038) (2379, 725) (8, 2166) (512, 1347) (482, 34) (1700, 2080) (2554, 1076) (1642, 1167) (1820, 2109) (8, 2491) (1502, 319)

PROSES DEKRIPSI EL GAMAL

Blok 1 - Dekripsi dengan = 910, = 2266

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 × 2266) mod 2579

= 5470124 mod 2579

= 65

Hasil Dekripsi Blok 1: y = 2414, M = 65

Blok 2 - Dekripsi dengan = 455, = 1258

455^1 mod 2579 = 455

455^2 mod 2579 = [455^1 mod 2579] × [455^1 mod 2579] mod 2579

= (455 × 455) mod 2579

= 207025 mod 2579

= 705

455^4 mod 2579 = [455^2 mod 2579] × [455^2 mod 2579] mod 2579

= (705 × 705) mod 2579

= 497025 mod 2579

= 1857

455^8 mod 2579 = [455^4 mod 2579] × [455^4 mod 2579] mod 2579

= (1857 × 1857) mod 2579

= 3448449 mod 2579

= 326

455^16 mod 2579 = [455^8 mod 2579] × [455^8 mod 2579] mod 2579

= (326 × 326) mod 2579

= 106276 mod 2579

= 537

455^32 mod 2579 = [455^16 mod 2579] × [455^16 mod 2579] mod 2579

= (537 × 537) mod 2579

= 288369 mod 2579

= 2100

455^64 mod 2579 = [455^32 mod 2579] × [455^32 mod 2579] mod 2579

= (2100 × 2100) mod 2579

= 4410000 mod 2579

= 2489

455^128 mod 2579 = [455^64 mod 2579] × [455^64 mod 2579] mod 2579

= (2489 × 2489) mod 2579

= 6195121 mod 2579

= 363

455^256 mod 2579 = [455^128 mod 2579] × [455^128 mod 2579] mod 2579

= (363 × 363) mod 2579

= 131769 mod 2579

= 240

455^512 mod 2579 = [455^256 mod 2579] × [455^256 mod 2579] mod 2579

= (240 × 240) mod 2579

= 57600 mod 2579

= 862

455^1024 mod 2579 = [455^512 mod 2579] × [455^512 mod 2579] mod 2579

= (862 × 862) mod 2579

= 743044 mod 2579

= 292

Menghitung hasil akhir 455^1813 mod 2579:

455^1813 mod 2579 = [455^1024 mod 2579] × [455^512 mod 2579] × [455^256 mod 2579] × [455^16 mod 2579] × [455^4 mod 2579] × [455^1 mod 2579] mod 2579

= (292 × 862 × 240 × 537 × 1857 × 455) mod 2579

= 27409363159651200 mod 2579

= 734

Perhitungan: M = (734 × 1258) mod 2579

= 923372 mod 2579

= 90

Hasil Dekripsi Blok 2: y = 734, M = 90

Blok 3 - Dekripsi dengan = 128, = 396

128^1 mod 2579 = 128

128^2 mod 2579 = [128^1 mod 2579] × [128^1 mod 2579] mod 2579

= (128 × 128) mod 2579

= 16384 mod 2579

= 910

128^4 mod 2579 = [128^2 mod 2579] × [128^2 mod 2579] mod 2579

= (910 × 910) mod 2579

= 828100 mod 2579

= 241

128^8 mod 2579 = [128^4 mod 2579] × [128^4 mod 2579] mod 2579

= (241 × 241) mod 2579

= 58081 mod 2579

= 1343

128^16 mod 2579 = [128^8 mod 2579] × [128^8 mod 2579] mod 2579

= (1343 × 1343) mod 2579

= 1803649 mod 2579

= 928

128^32 mod 2579 = [128^16 mod 2579] × [128^16 mod 2579] mod 2579

= (928 × 928) mod 2579

= 861184 mod 2579

= 2377

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

= (2377 × 2377) mod 2579

= 5650129 mod 2579

= 2119

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

= (2119 × 2119) mod 2579

= 4490161 mod 2579

= 122

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

= (122 × 122) mod 2579

= 14884 mod 2579

= 1989

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

= (1989 × 1989) mod 2579

= 3956121 mod 2579

= 2514

128^1024 mod 2579 = [128^512 mod 2579] × [128^512 mod 2579] mod 2579

= (2514 × 2514) mod 2579

= 6320196 mod 2579

= 1646

Menghitung hasil akhir 128^1813 mod 2579:

128^1813 mod 2579 = [128^1024 mod 2579] × [128^512 mod 2579] × [128^256 mod 2579] × [128^16 mod 2579] × [128^4 mod 2579] × [128^1 mod 2579] mod 2579

= (1646 × 2514 × 1989 × 928 × 241 × 128) mod 2579

= 235616052622639104 mod 2579

= 1192

Perhitungan: M = (1192 × 396) mod 2579

= 472032 mod 2579

= 75

Hasil Dekripsi Blok 3: y = 1192, M = 75

Blok 4 - Dekripsi dengan = 2379, = 489

2379^1 mod 2579 = 2379

2379^2 mod 2579 = [2379^1 mod 2579] × [2379^1 mod 2579] mod 2579

= (2379 × 2379) mod 2579

= 5659641 mod 2579

= 1315

2379^4 mod 2579 = [2379^2 mod 2579] × [2379^2 mod 2579] mod 2579

= (1315 × 1315) mod 2579

= 1729225 mod 2579

= 1295

2379^8 mod 2579 = [2379^4 mod 2579] × [2379^4 mod 2579] mod 2579

= (1295 × 1295) mod 2579

= 1677025 mod 2579

= 675

2379^16 mod 2579 = [2379^8 mod 2579] × [2379^8 mod 2579] mod 2579

= (675 × 675) mod 2579

= 455625 mod 2579

= 1721

2379^32 mod 2579 = [2379^16 mod 2579] × [2379^16 mod 2579] mod 2579

= (1721 × 1721) mod 2579

= 2961841 mod 2579

= 1149

2379^64 mod 2579 = [2379^32 mod 2579] × [2379^32 mod 2579] mod 2579

= (1149 × 1149) mod 2579

= 1320201 mod 2579

= 2332

2379^128 mod 2579 = [2379^64 mod 2579] × [2379^64 mod 2579] mod 2579

= (2332 × 2332) mod 2579

= 5438224 mod 2579

= 1692

2379^256 mod 2579 = [2379^128 mod 2579] × [2379^128 mod 2579] mod 2579

= (1692 × 1692) mod 2579

= 2862864 mod 2579

= 174

2379^512 mod 2579 = [2379^256 mod 2579] × [2379^256 mod 2579] mod 2579

= (174 × 174) mod 2579

= 30276 mod 2579

= 1907

2379^1024 mod 2579 = [2379^512 mod 2579] × [2379^512 mod 2579] mod 2579

= (1907 × 1907) mod 2579

= 3636649 mod 2579

= 259

Menghitung hasil akhir 2379^1813 mod 2579:

2379^1813 mod 2579 = [2379^1024 mod 2579] × [2379^512 mod 2579] × [2379^256 mod 2579] × [2379^16 mod 2579] × [2379^4 mod 2579] × [2379^1 mod 2579] mod 2579

= (259 × 1907 × 174 × 1721 × 1295 × 2379) mod 2579

= 455664071286079110 mod 2579

= 1672

Perhitungan: M = (1672 × 489) mod 2579

= 817608 mod 2579

= 65

Hasil Dekripsi Blok 4: y = 1672, M = 65

Blok 5 - Dekripsi dengan = 2554, = 912

2554^1 mod 2579 = 2554

2554^2 mod 2579 = [2554^1 mod 2579] × [2554^1 mod 2579] mod 2579

= (2554 × 2554) mod 2579

= 6522916 mod 2579

= 625

2554^4 mod 2579 = [2554^2 mod 2579] × [2554^2 mod 2579] mod 2579

= (625 × 625) mod 2579

= 390625 mod 2579

= 1196

2554^8 mod 2579 = [2554^4 mod 2579] × [2554^4 mod 2579] mod 2579

= (1196 × 1196) mod 2579

= 1430416 mod 2579

= 1650

2554^16 mod 2579 = [2554^8 mod 2579] × [2554^8 mod 2579] mod 2579

= (1650 × 1650) mod 2579

= 2722500 mod 2579

= 1655

2554^32 mod 2579 = [2554^16 mod 2579] × [2554^16 mod 2579] mod 2579

= (1655 × 1655) mod 2579

= 2739025 mod 2579

= 127

2554^64 mod 2579 = [2554^32 mod 2579] × [2554^32 mod 2579] mod 2579

= (127 × 127) mod 2579

= 16129 mod 2579

= 655

2554^128 mod 2579 = [2554^64 mod 2579] × [2554^64 mod 2579] mod 2579

= (655 × 655) mod 2579

= 429025 mod 2579

= 911

2554^256 mod 2579 = [2554^128 mod 2579] × [2554^128 mod 2579] mod 2579

= (911 × 911) mod 2579

= 829921 mod 2579

= 2062

2554^512 mod 2579 = [2554^256 mod 2579] × [2554^256 mod 2579] mod 2579

= (2062 × 2062) mod 2579

= 4251844 mod 2579

= 1652

2554^1024 mod 2579 = [2554^512 mod 2579] × [2554^512 mod 2579] mod 2579

= (1652 × 1652) mod 2579

= 2729104 mod 2579

= 522

Menghitung hasil akhir 2554^1813 mod 2579:

2554^1813 mod 2579 = [2554^1024 mod 2579] × [2554^512 mod 2579] × [2554^256 mod 2579] × [2554^16 mod 2579] × [2554^4 mod 2579] × [2554^1 mod 2579] mod 2579

= (522 × 1652 × 2062 × 1655 × 1196 × 2554) mod 2579

= 8989163457197938560 mod 2579

= 362

Perhitungan: M = (362 × 912) mod 2579

= 330144 mod 2579

= 32

Hasil Dekripsi Blok 5: y = 362, M = 32

Blok 6 - Dekripsi dengan = 1665, = 983

1665^1 mod 2579 = 1665

1665^2 mod 2579 = [1665^1 mod 2579] × [1665^1 mod 2579] mod 2579

= (1665 × 1665) mod 2579

= 2772225 mod 2579

= 2379

1665^4 mod 2579 = [1665^2 mod 2579] × [1665^2 mod 2579] mod 2579

= (2379 × 2379) mod 2579

= 5659641 mod 2579

= 1315

1665^8 mod 2579 = [1665^4 mod 2579] × [1665^4 mod 2579] mod 2579

= (1315 × 1315) mod 2579

= 1729225 mod 2579

= 1295

1665^16 mod 2579 = [1665^8 mod 2579] × [1665^8 mod 2579] mod 2579

= (1295 × 1295) mod 2579

= 1677025 mod 2579

= 675

1665^32 mod 2579 = [1665^16 mod 2579] × [1665^16 mod 2579] mod 2579

= (675 × 675) mod 2579

= 455625 mod 2579

= 1721

1665^64 mod 2579 = [1665^32 mod 2579] × [1665^32 mod 2579] mod 2579

= (1721 × 1721) mod 2579

= 2961841 mod 2579

= 1149

1665^128 mod 2579 = [1665^64 mod 2579] × [1665^64 mod 2579] mod 2579

= (1149 × 1149) mod 2579

= 1320201 mod 2579

= 2332

1665^256 mod 2579 = [1665^128 mod 2579] × [1665^128 mod 2579] mod 2579

= (2332 × 2332) mod 2579

= 5438224 mod 2579

= 1692

1665^512 mod 2579 = [1665^256 mod 2579] × [1665^256 mod 2579] mod 2579

= (1692 × 1692) mod 2579

= 2862864 mod 2579

= 174

1665^1024 mod 2579 = [1665^512 mod 2579] × [1665^512 mod 2579] mod 2579

= (174 × 174) mod 2579

= 30276 mod 2579

= 1907

Menghitung hasil akhir 1665^1813 mod 2579:

1665^1813 mod 2579 = [1665^1024 mod 2579] × [1665^512 mod 2579] × [1665^256 mod 2579] × [1665^16 mod 2579] × [1665^4 mod 2579] × [1665^1 mod 2579] mod 2579

= (1907 × 174 × 1692 × 675 × 1315 × 1665) mod 2579

= 829743890879655000 mod 2579

= 2482

Perhitungan: M = (2482 × 983) mod 2579

= 2439806 mod 2579

= 72

Hasil Dekripsi Blok 6: y = 2482, M = 72

Blok 7 - Dekripsi dengan = 512, = 1366

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

= 10829597720791449 60 mod 2579

= 2445

Perhitungan: M = (2445 × 1366) mod 2579

= 3339870 mod 2579

= 65

Hasil Dekripsi Blok 7: y = 2445, M = 65

Blok 8 - Dekripsi dengan = 760, = 1746

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 × 1746) mod 2579

= 567450 mod 2579

= 70

Hasil Dekripsi Blok 8: y = 325, M = 70

Blok 9 - Dekripsi dengan = 1958, = 1288

1958^1 mod 2579 = 1958

1958^2 mod 2579 = [1958^1 mod 2579] × [1958^1 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

1958^4 mod 2579 = [1958^2 mod 2579] × [1958^2 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

1958^8 mod 2579 = [1958^4 mod 2579] × [1958^4 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

1958^16 mod 2579 = [1958^8 mod 2579] × [1958^8 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

1958^32 mod 2579 = [1958^16 mod 2579] × [1958^16 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

1958^64 mod 2579 = [1958^32 mod 2579] × [1958^32 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

1958^128 mod 2579 = [1958^64 mod 2579] × [1958^64 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

1958^256 mod 2579 = [1958^128 mod 2579] × [1958^128 mod 2579] mod 2579

= (245 × 245) mod 2579

= 60025 mod 2579

= 708

1958^512 mod 2579 = [1958^256 mod 2579] × [1958^256 mod 2579] mod 2579

= (708 × 708) mod 2579

= 501264 mod 2579

= 938

1958^1024 mod 2579 = [1958^512 mod 2579] × [1958^512 mod 2579] mod 2579

= (938 × 938) mod 2579

= 879844 mod 2579

= 405

Menghitung hasil akhir 1958^1813 mod 2579:

1958^1813 mod 2579 = [1958^1024 mod 2579] × [1958^512 mod 2579] × [1958^256 mod 2579] × [1958^16 mod 2579] × [1958^4 mod 2579] × [1958^1 mod 2579] mod 2579

= (405 × 938 × 708 × 1335 × 1967 × 1958) mod 2579

= 1382895719570257200 mod 2579

= 811

Perhitungan: M = (811 × 1288) mod 2579

= 1044568 mod 2579

= 73

Hasil Dekripsi Blok 9: y = 811, M = 73

Blok 10 - Dekripsi dengan = 190, = 888

190^1 mod 2579 = 190

190^2 mod 2579 = [190^1 mod 2579] × [190^1 mod 2579] mod 2579

= (190 × 190) mod 2579

= 36100 mod 2579

= 2573

190^4 mod 2579 = [190^2 mod 2579] × [190^2 mod 2579] mod 2579

= (2573 × 2573) mod 2579

= 6620329 mod 2579

= 36

190^8 mod 2579 = [190^4 mod 2579] × [190^4 mod 2579] mod 2579

= (36 × 36) mod 2579

= 1296 mod 2579

= 1296

190^16 mod 2579 = [190^8 mod 2579] × [190^8 mod 2579] mod 2579

= (1296 × 1296) mod 2579

= 1679616 mod 2579

= 687

190^32 mod 2579 = [190^16 mod 2579] × [190^16 mod 2579] mod 2579

= (687 × 687) mod 2579

= 471969 mod 2579

= 12

190^64 mod 2579 = [190^32 mod 2579] × [190^32 mod 2579] mod 2579

= (12 × 12) mod 2579

= 144 mod 2579

= 144

190^128 mod 2579 = [190^64 mod 2579] × [190^64 mod 2579] mod 2579

= (144 × 144) mod 2579

= 20736 mod 2579

= 104

190^256 mod 2579 = [190^128 mod 2579] × [190^128 mod 2579] mod 2579

= (104 × 104) mod 2579

= 10816 mod 2579

= 500

190^512 mod 2579 = [190^256 mod 2579] × [190^256 mod 2579] mod 2579

= (500 × 500) mod 2579

= 250000 mod 2579

= 2416

190^1024 mod 2579 = [190^512 mod 2579] × [190^512 mod 2579] mod 2579

= (2416 × 2416) mod 2579

= 5837056 mod 2579

= 779

Menghitung hasil akhir 190^1813 mod 2579:

190^1813 mod 2579 = [190^1024 mod 2579] × [190^512 mod 2579] × [190^256 mod 2579] × [190^16 mod 2579] × [190^4 mod 2579] × [190^1 mod 2579] mod 2579

= (779 × 2416 × 500 × 687 × 36 × 190) mod 2579

= 4421984650560000 mod 2579

= 2036

Perhitungan: M = (2036 × 888) mod 2579

= 1807968 mod 2579

= 89

Hasil Dekripsi Blok 10: y = 2036, M = 89

Blok 11 - Dekripsi dengan = 461, = 106

461^1 mod 2579 = 461

461^2 mod 2579 = [461^1 mod 2579] × [461^1 mod 2579] mod 2579

= (461 × 461) mod 2579

= 212521 mod 2579

= 1043

461^4 mod 2579 = [461^2 mod 2579] × [461^2 mod 2579] mod 2579

= (1043 × 1043) mod 2579

= 1087849 mod 2579

= 2090

461^8 mod 2579 = [461^4 mod 2579] × [461^4 mod 2579] mod 2579

= (2090 × 2090) mod 2579

= 4368100 mod 2579

= 1853

461^16 mod 2579 = [461^8 mod 2579] × [461^8 mod 2579] mod 2579

= (1853 × 1853) mod 2579

= 3433609 mod 2579

= 960

461^32 mod 2579 = [461^16 mod 2579] × [461^16 mod 2579] mod 2579

= (960 × 960) mod 2579

= 921600 mod 2579

= 897

461^64 mod 2579 = [461^32 mod 2579] × [461^32 mod 2579] mod 2579

= (897 × 897) mod 2579

= 804609 mod 2579

= 2540

461^128 mod 2579 = [461^64 mod 2579] × [461^64 mod 2579] mod 2579

= (2540 × 2540) mod 2579

= 6451600 mod 2579

= 1521

461^256 mod 2579 = [461^128 mod 2579] × [461^128 mod 2579] mod 2579

= (1521 × 1521) mod 2579

= 2313441 mod 2579

= 78

461^512 mod 2579 = [461^256 mod 2579] × [461^256 mod 2579] mod 2579

= (78 × 78) mod 2579

= 6084 mod 2579

= 926

461^1024 mod 2579 = [461^512 mod 2579] × [461^512 mod 2579] mod 2579

= (926 × 926) mod 2579

= 857476 mod 2579

= 1248

Menghitung hasil akhir 461^1813 mod 2579:

461^1813 mod 2579 = [461^1024 mod 2579] × [461^512 mod 2579] × [461^256 mod 2579] × [461^16 mod 2579] × [461^4 mod 2579] × [461^1 mod 2579] mod 2579

= (1248 × 926 × 78 × 960 × 2090 × 461) mod 2579

= 83375532229017600 mod 2579

= 2166

Perhitungan: M = (2166 × 106) mod 2579

= 229596 mod 2579

= 65

Hasil Dekripsi Blok 11: y = 2166, M = 65

Blok 12 - Dekripsi dengan = 1820, = 1005

1820^1 mod 2579 = 1820

1820^2 mod 2579 = [1820^1 mod 2579] × [1820^1 mod 2579] mod 2579

= (1820 × 1820) mod 2579

= 3312400 mod 2579

= 964

1820^4 mod 2579 = [1820^2 mod 2579] × [1820^2 mod 2579] mod 2579

= (964 × 964) mod 2579

= 929296 mod 2579

= 856

1820^8 mod 2579 = [1820^4 mod 2579] × [1820^4 mod 2579] mod 2579

= (856 × 856) mod 2579

= 732736 mod 2579

= 300

1820^16 mod 2579 = [1820^8 mod 2579] × [1820^8 mod 2579] mod 2579

= (300 × 300) mod 2579

= 90000 mod 2579

= 2314

1820^32 mod 2579 = [1820^16 mod 2579] × [1820^16 mod 2579] mod 2579

= (2314 × 2314) mod 2579

= 5354596 mod 2579

= 592

1820^64 mod 2579 = [1820^32 mod 2579] × [1820^32 mod 2579] mod 2579

= (592 × 592) mod 2579

= 350464 mod 2579

= 2299

1820^128 mod 2579 = [1820^64 mod 2579] × [1820^64 mod 2579] mod 2579

= (2299 × 2299) mod 2579

= 5285401 mod 2579

= 1030

1820^256 mod 2579 = [1820^128 mod 2579] × [1820^128 mod 2579] mod 2579

= (1030 × 1030) mod 2579

= 1060900 mod 2579

= 931

1820^512 mod 2579 = [1820^256 mod 2579] × [1820^256 mod 2579] mod 2579

= (931 × 931) mod 2579

= 866761 mod 2579

= 217

1820^1024 mod 2579 = [1820^512 mod 2579] × [1820^512 mod 2579] mod 2579

= (217 × 217) mod 2579

= 47089 mod 2579

= 667

Menghitung hasil akhir 1820^1813 mod 2579:

1820^1813 mod 2579 = [1820^1024 mod 2579] × [1820^512 mod 2579] × [1820^256 mod 2579] × [1820^16 mod 2579] × [1820^4 mod 2579] × [1820^1 mod 2579] mod 2579

= (667 × 217 × 931 × 2314 × 856 × 1820) mod 2579

= 485784614579001920 mod 2579

= 1432

Perhitungan: M = (1432 × 1005) mod 2579

= 1439160 mod 2579

= 78

Hasil Dekripsi Blok 12: y = 1432, M = 78

Blok 13 - 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 13: y = 2484, M = 32

Blok 14 - Dekripsi dengan = 16, = 2228

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 × 2228) mod 2579

= 245080 mod 2579

= 75

Hasil Dekripsi Blok 14: y = 110, M = 75

Blok 15 - Dekripsi dengan = 821, = 1928

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 × 1928) mod 2579

= 2963336 mod 2579

= 65

Hasil Dekripsi Blok 15: y = 1537, M = 65

Blok 16 - Dekripsi dengan = 455, = 2038

455^1 mod 2579 = 455

455^2 mod 2579 = [455^1 mod 2579] × [455^1 mod 2579] mod 2579

= (455 × 455) mod 2579

= 207025 mod 2579

= 705

455^4 mod 2579 = [455^2 mod 2579] × [455^2 mod 2579] mod 2579

= (705 × 705) mod 2579

= 497025 mod 2579

= 1857

455^8 mod 2579 = [455^4 mod 2579] × [455^4 mod 2579] mod 2579

= (1857 × 1857) mod 2579

= 3448449 mod 2579

= 326

455^16 mod 2579 = [455^8 mod 2579] × [455^8 mod 2579] mod 2579

= (326 × 326) mod 2579

= 106276 mod 2579

= 537

455^32 mod 2579 = [455^16 mod 2579] × [455^16 mod 2579] mod 2579

= (537 × 537) mod 2579

= 288369 mod 2579

= 2100

455^64 mod 2579 = [455^32 mod 2579] × [455^32 mod 2579] mod 2579

= (2100 × 2100) mod 2579

= 4410000 mod 2579

= 2489

455^128 mod 2579 = [455^64 mod 2579] × [455^64 mod 2579] mod 2579

= (2489 × 2489) mod 2579

= 6195121 mod 2579

= 363

455^256 mod 2579 = [455^128 mod 2579] × [455^128 mod 2579] mod 2579

= (363 × 363) mod 2579

= 131769 mod 2579

= 240

455^512 mod 2579 = [455^256 mod 2579] × [455^256 mod 2579] mod 2579

= (240 × 240) mod 2579

= 57600 mod 2579

= 862

455^1024 mod 2579 = [455^512 mod 2579] × [455^512 mod 2579] mod 2579

= (862 × 862) mod 2579

= 743044 mod 2579

= 292

Menghitung hasil akhir 455^1813 mod 2579:

455^1813 mod 2579 = [455^1024 mod 2579] × [455^512 mod 2579] × [455^256 mod 2579] × [455^16 mod 2579] × [455^4 mod 2579] × [455^1 mod 2579] mod 2579

= (292 × 862 × 240 × 537 × 1857 × 455) mod 2579

= 27409363159651200 mod 2579

= 734

Perhitungan: M = (734 × 2038) mod 2579

= 1495892 mod 2579

= 72

Hasil Dekripsi Blok 16: y = 734, M = 72

Blok 17 - Dekripsi dengan = 2379, = 725

2379^1 mod 2579 = 2379

2379^2 mod 2579 = [2379^1 mod 2579] × [2379^1 mod 2579] mod 2579

= (2379 × 2379) mod 2579

= 5659641 mod 2579

= 1315

2379^4 mod 2579 = [2379^2 mod 2579] × [2379^2 mod 2579] mod 2579

= (1315 × 1315) mod 2579

= 1729225 mod 2579

= 1295

2379^8 mod 2579 = [2379^4 mod 2579] × [2379^4 mod 2579] mod 2579

= (1295 × 1295) mod 2579

= 1677025 mod 2579

= 675

2379^16 mod 2579 = [2379^8 mod 2579] × [2379^8 mod 2579] mod 2579

= (675 × 675) mod 2579

= 455625 mod 2579

= 1721

2379^32 mod 2579 = [2379^16 mod 2579] × [2379^16 mod 2579] mod 2579

= (1721 × 1721) mod 2579

= 2961841 mod 2579

= 1149

2379^64 mod 2579 = [2379^32 mod 2579] × [2379^32 mod 2579] mod 2579

= (1149 × 1149) mod 2579

= 1320201 mod 2579

= 2332

2379^128 mod 2579 = [2379^64 mod 2579] × [2379^64 mod 2579] mod 2579

= (2332 × 2332) mod 2579

= 5438224 mod 2579

= 1692

2379^256 mod 2579 = [2379^128 mod 2579] × [2379^128 mod 2579] mod 2579

= (1692 × 1692) mod 2579

= 2862864 mod 2579

= 174

2379^512 mod 2579 = [2379^256 mod 2579] × [2379^256 mod 2579] mod 2579

= (174 × 174) mod 2579

= 30276 mod 2579

= 1907

2379^1024 mod 2579 = [2379^512 mod 2579] × [2379^512 mod 2579] mod 2579

= (1907 × 1907) mod 2579

= 3636649 mod 2579

= 259

Menghitung hasil akhir 2379^1813 mod 2579:

2379^1813 mod 2579 = [2379^1024 mod 2579] × [2379^512 mod 2579] × [2379^256 mod 2579] × [2379^16 mod 2579] × [2379^4 mod 2579] × [2379^1 mod 2579] mod 2579

= (259 × 1907 × 174 × 1721 × 1295 × 2379) mod 2579

= 455664071286079110 mod 2579

= 1672

Perhitungan: M = (1672 × 725) mod 2579

= 1212200 mod 2579

= 70

Hasil Dekripsi Blok 17: y = 1672, M = 70

Blok 18 - Dekripsi dengan = 8, = 2166

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 × 2166) mod 2579

= 2664180 mod 2579

= 73

Hasil Dekripsi Blok 18: y = 1230, M = 73

Blok 19 - Dekripsi dengan = 512, = 1347

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

= 10829597720791449 60 mod 2579

= 2445

Perhitungan: M = (2445 × 1347) mod 2579

= 3293415 mod 2579

= 32

Hasil Dekripsi Blok 19: y = 2445, M = 32

Blok 20 - Dekripsi dengan = 482, = 34

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 × 34) mod 2579

= 33592 mod 2579

= 65

Hasil Dekripsi Blok 20: y = 988, M = 65

Blok 21 - Dekripsi dengan = 1700, = 2080

1700^1 mod 2579 = 1700

1700^2 mod 2579 = [1700^1 mod 2579] × [1700^1 mod 2579] mod 2579

= (1700 × 1700) mod 2579

= 2890000 mod 2579

= 1520

1700^4 mod 2579 = [1700^2 mod 2579] × [1700^2 mod 2579] mod 2579

= (1520 × 1520) mod 2579

= 2310400 mod 2579

= 2195

1700^8 mod 2579 = [1700^4 mod 2579] × [1700^4 mod 2579] mod 2579

= (2195 × 2195) mod 2579

= 4818025 mod 2579

= 453

1700^16 mod 2579 = [1700^8 mod 2579] × [1700^8 mod 2579] mod 2579

= (453 × 453) mod 2579

= 205209 mod 2579

= 1468

1700^32 mod 2579 = [1700^16 mod 2579] × [1700^16 mod 2579] mod 2579

= (1468 × 1468) mod 2579

= 2155024 mod 2579

= 1559

1700^64 mod 2579 = [1700^32 mod 2579] × [1700^32 mod 2579] mod 2579

= (1559 × 1559) mod 2579

= 2430481 mod 2579

= 1063

1700^128 mod 2579 = [1700^64 mod 2579] × [1700^64 mod 2579] mod 2579

= (1063 × 1063) mod 2579

= 1129969 mod 2579

= 367

1700^256 mod 2579 = [1700^128 mod 2579] × [1700^128 mod 2579] mod 2579

= (367 × 367) mod 2579

= 134689 mod 2579

= 581

1700^512 mod 2579 = [1700^256 mod 2579] × [1700^256 mod 2579] mod 2579

= (581 × 581) mod 2579

= 337561 mod 2579

= 2291

1700^1024 mod 2579 = [1700^512 mod 2579] × [1700^512 mod 2579] mod 2579

= (2291 × 2291) mod 2579

= 5248681 mod 2579

= 416

Menghitung hasil akhir 1700^1813 mod 2579:

1700^1813 mod 2579 = [1700^1024 mod 2579] × [1700^512 mod 2579] × [1700^256 mod 2579] × [1700^16 mod 2579] × [1700^4 mod 2579] × [1700^1 mod 2579] mod 2579

= (416 × 2291 × 581 × 1468 × 2195 × 1700) mod 2579

= 30332209975733120000 mod 2579

= 1478

Perhitungan: M = (1478 × 2080) mod 2579

= 3074240 mod 2579

= 72

Hasil Dekripsi Blok 21: y = 1478, M = 72

Blok 22 - Dekripsi dengan = 2554, = 1076

2554^1 mod 2579 = 2554

2554^2 mod 2579 = [2554^1 mod 2579] × [2554^1 mod 2579] mod 2579

= (2554 × 2554) mod 2579

= 6522916 mod 2579

= 625

2554^4 mod 2579 = [2554^2 mod 2579] × [2554^2 mod 2579] mod 2579

= (625 × 625) mod 2579

= 390625 mod 2579

= 1196

2554^8 mod 2579 = [2554^4 mod 2579] × [2554^4 mod 2579] mod 2579

= (1196 × 1196) mod 2579

= 1430416 mod 2579

= 1650

2554^16 mod 2579 = [2554^8 mod 2579] × [2554^8 mod 2579] mod 2579

= (1650 × 1650) mod 2579

= 2722500 mod 2579

= 1655

2554^32 mod 2579 = [2554^16 mod 2579] × [2554^16 mod 2579] mod 2579

= (1655 × 1655) mod 2579

= 2739025 mod 2579

= 127

2554^64 mod 2579 = [2554^32 mod 2579] × [2554^32 mod 2579] mod 2579

= (127 × 127) mod 2579

= 16129 mod 2579

= 655

2554^128 mod 2579 = [2554^64 mod 2579] × [2554^64 mod 2579] mod 2579

= (655 × 655) mod 2579

= 429025 mod 2579

= 911

2554^256 mod 2579 = [2554^128 mod 2579] × [2554^128 mod 2579] mod 2579

= (911 × 911) mod 2579

= 829921 mod 2579

= 2062

2554^512 mod 2579 = [2554^256 mod 2579] × [2554^256 mod 2579] mod 2579

= (2062 × 2062) mod 2579

= 4251844 mod 2579

= 1652

2554^1024 mod 2579 = [2554^512 mod 2579] × [2554^512 mod 2579] mod 2579

= (1652 × 1652) mod 2579

= 2729104 mod 2579

= 522

Menghitung hasil akhir 2554^1813 mod 2579:

2554^1813 mod 2579 = [2554^1024 mod 2579] × [2554^512 mod 2579] × [2554^256 mod 2579] × [2554^16 mod 2579] × [2554^4 mod 2579] × [2554^1 mod 2579] mod 2579

= (522 × 1652 × 2062 × 1655 × 1196 × 2554) mod 2579

= 8989163457197938560 mod 2579

= 362

Perhitungan: M = (362 × 1076) mod 2579

= 389512 mod 2579

= 83

Hasil Dekripsi Blok 22: y = 362, M = 83

Blok 23 - Dekripsi dengan = 1642, = 1167

1642^1 mod 2579 = 1642

1642^2 mod 2579 = [1642^1 mod 2579] × [1642^1 mod 2579] mod 2579

= (1642 × 1642) mod 2579

= 2696164 mod 2579

= 1109

1642^4 mod 2579 = [1642^2 mod 2579] × [1642^2 mod 2579] mod 2579

= (1109 × 1109) mod 2579

= 1229881 mod 2579

= 2277

1642^8 mod 2579 = [1642^4 mod 2579] × [1642^4 mod 2579] mod 2579

= (2277 × 2277) mod 2579

= 5184729 mod 2579

= 939

1642^16 mod 2579 = [1642^8 mod 2579] × [1642^8 mod 2579] mod 2579

= (939 × 939) mod 2579

= 881721 mod 2579

= 2282

1642^32 mod 2579 = [1642^16 mod 2579] × [1642^16 mod 2579] mod 2579

= (2282 × 2282) mod 2579

= 5207524 mod 2579

= 523

1642^64 mod 2579 = [1642^32 mod 2579] × [1642^32 mod 2579] mod 2579

= (523 × 523) mod 2579

= 273529 mod 2579

= 155

1642^128 mod 2579 = [1642^64 mod 2579] × [1642^64 mod 2579] mod 2579

= (155 × 155) mod 2579

= 24025 mod 2579

= 814

1642^256 mod 2579 = [1642^128 mod 2579] × [1642^128 mod 2579] mod 2579

= (814 × 814) mod 2579

= 662596 mod 2579

= 2372

1642^512 mod 2579 = [1642^256 mod 2579] × [1642^256 mod 2579] mod 2579

= (2372 × 2372) mod 2579

= 5626384 mod 2579

= 1585

1642^1024 mod 2579 = [1642^512 mod 2579] × [1642^512 mod 2579] mod 2579

= (1585 × 1585) mod 2579

= 2512225 mod 2579

= 279

Menghitung hasil akhir 1642^1813 mod 2579:

1642^1813 mod 2579 = [1642^1024 mod 2579] × [1642^512 mod 2579] × [1642^256 mod 2579] × [1642^16 mod 2579] × [1642^4 mod 2579] × [1642^1 mod 2579] mod 2579

= (279 × 1585 × 2372 × 2282 × 2277 × 1642) mod 2579

= 8949524844305208240 mod 2579

= 431

Perhitungan: M = (431 × 1167) mod 2579

= 502977 mod 2579

= 72

Hasil Dekripsi Blok 23: y = 431, M = 72

Blok 24 - Dekripsi dengan = 1820, = 2109

1820^1 mod 2579 = 1820

1820^2 mod 2579 = [1820^1 mod 2579] × [1820^1 mod 2579] mod 2579

= (1820 × 1820) mod 2579

= 3312400 mod 2579

= 964

1820^4 mod 2579 = [1820^2 mod 2579] × [1820^2 mod 2579] mod 2579

= (964 × 964) mod 2579

= 929296 mod 2579

= 856

1820^8 mod 2579 = [1820^4 mod 2579] × [1820^4 mod 2579] mod 2579

= (856 × 856) mod 2579

= 732736 mod 2579

= 300

1820^16 mod 2579 = [1820^8 mod 2579] × [1820^8 mod 2579] mod 2579

= (300 × 300) mod 2579

= 90000 mod 2579

= 2314

1820^32 mod 2579 = [1820^16 mod 2579] × [1820^16 mod 2579] mod 2579

= (2314 × 2314) mod 2579

= 5354596 mod 2579

= 592

1820^64 mod 2579 = [1820^32 mod 2579] × [1820^32 mod 2579] mod 2579

= (592 × 592) mod 2579

= 350464 mod 2579

= 2299

1820^128 mod 2579 = [1820^64 mod 2579] × [1820^64 mod 2579] mod 2579

= (2299 × 2299) mod 2579

= 5285401 mod 2579

= 1030

1820^256 mod 2579 = [1820^128 mod 2579] × [1820^128 mod 2579] mod 2579

= (1030 × 1030) mod 2579

= 1060900 mod 2579

= 931

1820^512 mod 2579 = [1820^256 mod 2579] × [1820^256 mod 2579] mod 2579

= (931 × 931) mod 2579

= 866761 mod 2579

= 217

1820^1024 mod 2579 = [1820^512 mod 2579] × [1820^512 mod 2579] mod 2579

= (217 × 217) mod 2579

= 47089 mod 2579

= 667

Menghitung hasil akhir 1820^1813 mod 2579:

1820^1813 mod 2579 = [1820^1024 mod 2579] × [1820^512 mod 2579] × [1820^256 mod 2579] × [1820^16 mod 2579] × [1820^4 mod 2579] × [1820^1 mod 2579] mod 2579

= (667 × 217 × 931 × 2314 × 856 × 1820) mod 2579

= 485784614579001920 mod 2579

= 1432

Perhitungan: M = (1432 × 2109) mod 2579

= 3020088 mod 2579

= 79

Hasil Dekripsi Blok 24: y = 1432, M = 79

Blok 25 - Dekripsi dengan = 8, = 2491

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 × 2491) mod 2579

= 3063930 mod 2579

= 78

Hasil Dekripsi Blok 25: y = 1230, M = 78

Blok 26 - Dekripsi dengan = 1502, = 319

1502^1 mod 2579 = 1502

1502^2 mod 2579 = [1502^1 mod 2579] × [1502^1 mod 2579] mod 2579

= (1502 × 1502) mod 2579

= 2256004 mod 2579

= 1958

1502^4 mod 2579 = [1502^2 mod 2579] × [1502^2 mod 2579] mod 2579

= (1958 × 1958) mod 2579

= 3833764 mod 2579

= 1370

1502^8 mod 2579 = [1502^4 mod 2579] × [1502^4 mod 2579] mod 2579

= (1370 × 1370) mod 2579

= 1876900 mod 2579

= 1967

1502^16 mod 2579 = [1502^8 mod 2579] × [1502^8 mod 2579] mod 2579

= (1967 × 1967) mod 2579

= 3869089 mod 2579

= 589

1502^32 mod 2579 = [1502^16 mod 2579] × [1502^16 mod 2579] mod 2579

= (589 × 589) mod 2579

= 346921 mod 2579

= 1335

1502^64 mod 2579 = [1502^32 mod 2579] × [1502^32 mod 2579] mod 2579

= (1335 × 1335) mod 2579

= 1782225 mod 2579

= 136

1502^128 mod 2579 = [1502^64 mod 2579] × [1502^64 mod 2579] mod 2579

= (136 × 136) mod 2579

= 18496 mod 2579

= 443

1502^256 mod 2579 = [1502^128 mod 2579] × [1502^128 mod 2579] mod 2579

= (443 × 443) mod 2579

= 196249 mod 2579

= 245

1502^512 mod 2579 = [1502^256 mod 2579] × [1502^256 mod 2579] mod 2579

= (245 × 245) mod 2579

= 60025 mod 2579

= 708

1502^1024 mod 2579 = [1502^512 mod 2579] × [1502^512 mod 2579] mod 2579

= (708 × 708) mod 2579

= 501264 mod 2579

= 938

Menghitung hasil akhir 1502^1813 mod 2579:

1502^1813 mod 2579 = [1502^1024 mod 2579] × [1502^512 mod 2579] × [1502^256 mod 2579] × [1502^16 mod 2579] × [1502^4 mod 2579] × [1502^1 mod 2579] mod 2579

= (938 × 708 × 245 × 589 × 1370 × 1502) mod 2579

= 197200483330552800 mod 2579

= 647

Perhitungan: M = (647 × 319) mod 2579

= 206393 mod 2579

= 73

Hasil Dekripsi Blok 26: y = 647, M = 73