LAPORAN HASIL ENKRIPSI & DEKRIPSI

Nama: Ryfaathir Rahman

NIM: 202410370110177

Kelas: Informatika E

PROSES ENKRIPSI EL GAMAL:

Blok 1 - ASCII: 82 (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 × 82 mod 2579

= 158096 mod 2579

= 777

Hasil Enkripsi Blok 1: ASCII (M) = 82, = 1410, = 777

Blok 2 - ASCII: 89 (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 × 89 mod 2579

= 9434 mod 2579

= 1697

Hasil Enkripsi Blok 2: ASCII (M) = 89, = 1109, = 1697

Blok 3 - ASCII: 70 (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 × 70 mod 2579

= 34230 mod 2579

= 703

Hasil Enkripsi Blok 3: ASCII (M) = 70, = 979, = 703

Blok 4 - ASCII: 65 (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 × 65 mod 2579

= 39130 mod 2579

= 445

Hasil Enkripsi Blok 4: ASCII (M) = 65, = 1700, = 445

Blok 5 - 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 5: ASCII (M) = 65, = 512, = 1366

Blok 6 - ASCII: 84 (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 × 84 mod 2579

= 50568 mod 2579

= 1567

Hasil Enkripsi Blok 6: ASCII (M) = 84, = 1700, = 1567

Blok 7 - ASCII: 72 (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 × 72 mod 2579

= 61848 mod 2579

= 2531

Hasil Enkripsi Blok 7: ASCII (M) = 72, = 1024, = 2531

Blok 8 - ASCII: 73 (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 × 73 mod 2579

= 31682 mod 2579

= 734

Hasil Enkripsi Blok 8: ASCII (M) = 73, = 2179, = 734

Blok 9 - ASCII: 82 (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 × 82 mod 2579

= 49364 mod 2579

= 363

Hasil Enkripsi Blok 9: ASCII (M) = 82, = 1700, = 363

Blok 10 - 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 10: ASCII (M) = 32, = 2554, = 912

Blok 11 - ASCII: 82 (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 × 82 mod 2579

= 5330 mod 2579

= 172

Hasil Enkripsi Blok 11: ASCII (M) = 82, = 8, = 172

Blok 12 - ASCII: 65 (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 × 65 mod 2579

= 71760 mod 2579

= 2127

Hasil Enkripsi Blok 12: ASCII (M) = 65, = 1820, = 2127

Blok 13 - ASCII: 72 (k = 1)

2^1 mod 2579 = 2

949^1 mod 2579 = 949

949^1 mod 2579 = 949

949^1 × 72 mod 2579

= 68328 mod 2579

= 1274

Hasil Enkripsi Blok 13: ASCII (M) = 72, = 2, = 1274

Blok 14 - ASCII: 77 (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 × 77 mod 2579

= 197120 mod 2579

= 1116

Hasil Enkripsi Blok 14: ASCII (M) = 77, = 190, = 1116

Blok 15 - ASCII: 65 (k = 44)

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 2^44 mod 2579:

2^44 mod 2579 = [2^32 mod 2579] × [2^8 mod 2579] × [2^4 mod 2579] mod 2579

= (1277 × 256 × 16) mod 2579

= 5230592 mod 2579

= 380

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 949^44 mod 2579:

949^44 mod 2579 = [949^32 mod 2579] × [949^8 mod 2579] × [949^4 mod 2579] mod 2579

= (34 × 678 × 2368) mod 2579

= 54587136 mod 2579

= 22

949^44 mod 2579 = 22

949^44 × 65 mod 2579

= 1430 mod 2579

= 1430

Hasil Enkripsi Blok 15: ASCII (M) = 65, = 380, = 1430

Blok 16 - ASCII: 78 (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 × 78 mod 2579

= 8268 mod 2579

= 531

Hasil Enkripsi Blok 16: ASCII (M) = 78, = 1109, = 531

ChipherText:

(1410, 777) (1109, 1697) (979, 703) (1700, 445) (512, 1366) (1700, 1567) (1024, 2531) (2179, 734)

(1700, 363) (2554, 912) (8, 172) (1820, 2127) (2, 1274) (190, 1116) (380, 1430) (1109, 531)

PROSES DEKRIPSI EL GAMAL

Blok 1 - Dekripsi dengan = 1410, = 777

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 × 777) mod 2579

= 80031 mod 2579

= 82

Hasil Dekripsi Blok 1: y = 103, M = 82

Blok 2 - Dekripsi dengan = 1109, = 1697

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 × 1697) mod 2579

= 123881 mod 2579

= 89

Hasil Dekripsi Blok 2: y = 73, M = 89

Blok 3 - Dekripsi dengan = 979, = 703

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 × 703) mod 2579

= 771191 mod 2579

= 70

Hasil Dekripsi Blok 3: y = 1097, M = 70

Blok 4 - Dekripsi dengan = 1700, = 445

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 × 445) mod 2579

= 657710 mod 2579

= 65

Hasil Dekripsi Blok 4: y = 1478, M = 65

Blok 5 - 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

= 1082959772079144960 mod 2579

= 2445

Perhitungan: M = (2445 × 1366) mod 2579

= 3339870 mod 2579

= 65

Hasil Dekripsi Blok 5: y = 2445, M = 65

Blok 6 - Dekripsi dengan = 1700, = 1567

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

= 3033220997573312000 mod 2579

= 1478

Perhitungan: M = (1478 × 1567) mod 2579

= 2316026 mod 2579

= 84

Hasil Dekripsi Blok 6: y = 1478, M = 84

Blok 7 - Dekripsi dengan = 1024, = 2531

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 × 2531) mod 2579

= 3259928 mod 2579

= 72

Hasil Dekripsi Blok 7: y = 1288, M = 72

Blok 8 - Dekripsi dengan = 2179, = 734

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 × 734) mod 2579

= 833090 mod 2579

= 73

Hasil Dekripsi Blok 8: y = 1135, M = 73

Blok 9 - Dekripsi dengan = 1700, = 363

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

= 3033220997573312000 mod 2579

= 1478

Perhitungan: M = (1478 × 363) mod 2579

= 536514 mod 2579

= 82

Hasil Dekripsi Blok 9: y = 1478, M = 82

Blok 10 - 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 10: y = 362, M = 32

Blok 11 - Dekripsi dengan = 8, = 172

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 × 172) mod 2579

= 211560 mod 2579

= 82

Hasil Dekripsi Blok 11: y = 1230, M = 82

Blok 12 - Dekripsi dengan = 1820, = 2127

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 × 2127) mod 2579

= 3045864 mod 2579

= 65

Hasil Dekripsi Blok 12: y = 1432, M = 65

Blok 13 - Dekripsi dengan = 2, = 1274

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 × 1274) mod 2579

= 2537808 mod 2579

= 72

Hasil Dekripsi Blok 13: y = 1992, M = 72

Blok 14 - Dekripsi dengan = 190, = 1116

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 × 1116) mod 2579

= 2272176 mod 2579

= 77

Hasil Dekripsi Blok 14: y = 2036, M = 77

Blok 15 - Dekripsi dengan = 380, = 1430

380^1 mod 2579 = 380

380^2 mod 2579 = [380^1 mod 2579] × [380^1 mod 2579] mod 2579

= (380 × 380) mod 2579

= 144400 mod 2579

= 2555

380^4 mod 2579 = [380^2 mod 2579] × [380^2 mod 2579] mod 2579

= (2555 × 2555) mod 2579

= 6528025 mod 2579

= 576

380^8 mod 2579 = [380^4 mod 2579] × [380^4 mod 2579] mod 2579

= (576 × 576) mod 2579

= 331776 mod 2579

= 1664

380^16 mod 2579 = [380^8 mod 2579] × [380^8 mod 2579] mod 2579

= (1664 × 1664) mod 2579

= 2768896 mod 2579

= 1629

380^32 mod 2579 = [380^16 mod 2579] × [380^16 mod 2579] mod 2579

= (1629 × 1629) mod 2579

= 2653641 mod 2579

= 2429

380^64 mod 2579 = [380^32 mod 2579] × [380^32 mod 2579] mod 2579

= (2429 × 2429) mod 2579

= 5900041 mod 2579

= 1868

380^128 mod 2579 = [380^64 mod 2579] × [380^64 mod 2579] mod 2579

= (1868 × 1868) mod 2579

= 3489424 mod 2579

= 37

380^256 mod 2579 = [380^128 mod 2579] × [380^128 mod 2579] mod 2579

= (37 × 37) mod 2579

= 1369 mod 2579

= 1369

380^512 mod 2579 = [380^256 mod 2579] × [380^256 mod 2579] mod 2579

= (1369 × 1369) mod 2579

= 1874161 mod 2579

= 1807

380^1024 mod 2579 = [380^512 mod 2579] × [380^512 mod 2579] mod 2579

= (1807 × 1807) mod 2579

= 3265249 mod 2579

= 235

Menghitung hasil akhir 380^1813 mod 2579:

380^1813 mod 2579 = [380^1024 mod 2579] × [380^512 mod 2579] × [380^256 mod 2579] × [380^16 mod 2579] × [380^4 mod 2579] × [380^1 mod 2579] mod 2579

= (235 × 1807 × 1369 × 1629 × 576 × 380) mod 2579

= 207279631224057600 mod 2579

= 1524

Perhitungan: M = (1524 × 1430) mod 2579

= 2179320 mod 2579

= 65

Hasil Dekripsi Blok 15: y = 1524, M = 65

Blok 16 - Dekripsi dengan = 1109, = 531

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 × 531) mod 2579

= 38763 mod 2579

= 78

Hasil Dekripsi Blok 16: y = 73, M = 78