Metoda e memories së veçantë

$c \equiv b^e \ mod \ m$

Alogoritmi

1° C = 1, e' = 0

2° Rrisim e' për 1

3° Vendosim C = (b * c) (mod m).

4° nëse e' <= e, kalo te hapi 2, përndryshe C është përgjigjja.

p.sh:

Nëse b=4, e=13, m=497

e' = 1, C = (1 * 4) mod 497= 4 mod 497 = 4

e' = 2, C = (4 * 4) mod 497 = 16 mod 497 = 16

e' = 3, C = (16 * 4) mod 497 = 64 mod 497 = 64

e' = 4, C = (64 * 4) mod497= 256 mod 497=256

e' = 5, C = (256 * 4) mod 4917 = 1024 mod 497 = 30

e' = 6; C = (30 * 4) mod 497 = 120 mod 497 = 120

---

e' = 13, C = (484.4) mod 497 = 1936 mod 497=445