- p "μεγάλος" πρώτος αριθμός
- g πρωτεύουσα ρίζα mod p
- Θα έχετε και πρώτο με p ίσχυει $g^k = a \pmod p$

i) Επιλέγουμε ακέραιο x $(1 < x < p-1)$

ii) Υπολογίζουμε το y.

$$y = g^x \bmod p$$

x: Ιδιωτικό κλειδί
y: Δημόσιο κλειδί, στέλνει το (p, g, y)

iii) Κρυπτογράφηση (μυνήματος M)

$$C_1 = g^k \bmod p$$
$$C_2 = M y^k \bmod p$$

Επομένως $C(C_1, C_2)$

iv) Αποκρυπτογράφηση

$$C_1^x = (g^k)^x \bmod p = (g^x)^k \bmod p = y^k \bmod p$$

$$C_2 / (C_1^x) \bmod p = M$$