Άσκηση 8 Dai16067 Κρυπτογραφία

Μιχούλης Γεώργιος

1)

a)

Z_5*

a |1 2 3 4

ord(a)| 1 4 4 2

b) Z_7*

a |1 2 3 4 5 6

ord(a)| 1 3 6 3 6 2

c) Z_{13}*

a| 1 2 3 4 5 6 7 8 9 10 11 12

ord(a) |1 12 3 6 4 12 12 4 3 6 12 2

2) $A = k_{pub,\,A} = g^{a} \bmod p$ $B = k_{pub,B} = g^{b} \bmod p$ $k_{AB} = g^{ab} \bmod p$

1. $K_{pubA} = 8$, $K_{pubB} = 32$, $K_{AB} = 78$
2. $K_{pubA} = 137$, $K_{pubB} = 84$, $K_{AB} = 90$
3. $K_{pubA} = 394$, $K_{pubB} = 313$, $K_{AB} = 206$

4)

Υπολογισμός του β: β = α d mod p.

Κρυπτογράφηση : (kE,y) = (α i mod p,x · β i mod p).

Αποκρυπτογράφηση του x = y(k d E) −1 mod p.

1. (kE, y) = (29,296), x = 33
2. (kE,y) = (125,301), x = 33
3. (kE,y) = (80,174), x = 248
4. (kE,y) = (320,139), x = 248

5) Το pub κλειδί του BOB είναι $k_{pub,B}$= (p, g, B) =(31,3,18)

(B = g^d mod p ⇔ $\log_g B = \log_g g^d$ ⇔ d=2,6)

$K_{e,1}$=6=3^i mod31

K_M=18^i mod p

• υπολογίζει εφήμερο κλειδί kE = g^{i} mod p

• υπολογίζει κλειδί ‘‘μάσκας’’ kM = β^{i} mod p

• κρυπτογραφεί μήνυμα c=m *k_M mod p

X1=17 kai ID bob x1=21 => c=m*Km mod p => Km=20

Με τον αντίστροφο του κλειδιού ρ=31 , αποκρυπτογραφούμε το c2 μιας και ο BOB χρησιμοποιεί το ίδιο ιδιωτικό κλειδί για την κρυπτογράφηση. Οπότε K_M^{-1}=14   m2=c2* K_M^{-1} mod p=9