Άσκηση 4 Dai16067 Κρυπτογραφία

1) A) 15 χ 29 mod 13 = 2 x 3 mod 13 =6 (mod 13) (ισχύει επιμεριστική ιδιότητα 15 mod 13 x 29 mod 13)

   B) 2 x 29 mod 13= 2x3 mod 13= 6 (mod 13)

   C) 2 x 3 mod 13=6 (mod 13)

   D) -11 x 3 mod 13= 2 x 3 mod 13 = 6 (mod 13).

2) Ισχύει ότι 5^{-1} x 5 =1 (mod n) άρα:

   - 5^{-1} mod 11 = 9 (mod 11)
   - 5^{-1} mod 12 = 5 (mod 12)
   - 5^{-1} mod 13 = 8 (mod 13)

3)
m=4:

gcd (0,4) =4gcd (0,4) =4

gcd (1,4) =1gcd (1,4) =1 Σχετικά πρώτος

gcd (2,4) =2gcd (2,4) =2

gcd (3,4) =1gcd (3,4) =1 Σχετικά πρώτος

Φ(4)=2 πρώτοι

m=5:

gcd(0,5)=5gcd(0,5)=5

gcd(1,5)=1gcd(1,5)=1 Σχετικά πρώτος

gcd(2,5)=1gcd(2,5)=1 Σχετικά πρώτος

gcd(3,5)=1gcd(3,5)=1 Σχετικά πρώτος

gcd(4,5)=1gcd(4,5)=1 Σχετικά πρώτος

Φ(5)= 4 πρώτοι

m=9:

gcd(0,9)=9gcd(0,9)=9

gcd(1,9)=1gcd(1,9)=1 Σχετικά πρώτος

gcd(2,9)=1gcd(2,9)=1 Σχετικά πρώτος

gcd(3,9)=3gcd(3,9)=3

gcd(4,9)=1gcd(4,9)=1 Σχετικά πρώτος

gcd(5,9)=1gcd(5,9)=1 Σχετικά πρώτος

gcd(6,9)=3gcd(6,9)=3

gcd(7,9)=1gcd(7,9)=1 Σχετικά πρώτος

gcd(8,9)=1gcd(8,9)=1 Σχετικά πρώτος

Φ(9)= 6 πρώτοι

m=26:

gcd(0,26)=26gcd(0,26)=26

gcd(1,26)=1gcd(1,26)=1 Σχετικά πρώτος

gcd(2,26)=2gcd(2,26)=2

gcd(3,26)=1gcd(3,26)=1 Σχετικά πρώτος

gcd(4,26)=2gcd(4,26)=2

gcd(5,26)=1gcd(5,26)=1 Σχετικά πρώτος

gcd(6,26)=2gcd(6,26)=2

gcd(7,26)=1gcd(7,26)=1 Σχετικά πρώτος

gcd(8,26)=2gcd(8,26)=2

gcd(9,26)=1gcd(9,26)=1 Σχετικά πρώτος

gcd(10,26)=2gcd(10,26)=2

gcd(11,26)=1gcd(11,26)=1 Σχετικά πρώτος

gcd(12,26)=2gcd(12,26)=2

gcd(13,26)=13gcd(13,26)=13

gcd(14,26)=2gcd(14,26)=2

gcd(15,26)=1gcd(15,26)=1 Σχετικά πρώτος

gcd(16,26)=2gcd(16,26)=2

gcd(17,26)=1gcd(17,26)=1 Σχετικά πρώτος

gcd(18,26)=2gcd(18,26)=2

gcd(19,26)=1gcd(19,26)=1 Σχετικά πρώτος

gcd(20,26)=2gcd(20,26)=2

gcd(21,26)=1gcd(21,26)=1 Σχετικά πρώτος

gcd(22,26)=2gcd(22,26)=2

gcd(23,26)=1gcd(23,26)=1 Σχετικά πρώτος

gcd(24,26)=2gcd(24,26)=2

gcd(25,26)=1gcd(25,26)=1 Σχετικά πρώτος

Φ(26)= 12 πρώτοι

4)

Α) έστω ότι ορίζουμε ένα k1 = (a1,b1) και k2 = (a2,b2) έχουμε οπότε $e_{k1}(x)$ = y= a1*x + b1 mod 26 , $e_{k2}(e_{k1}(x))$= y = a2(a1x+b1) +b2 mod 26= a1*a2*x +a2*b1+b2 mod 26 δηλαδή k3 = (a1a2 , a2b1+b2)mod 26 το οποίο σημαίνει ότι τα k1 και k2 είναι ισότιμα με το k3 άρα ένα affine cipher κάνει ακριβώς την ίδια δουλειά όσο και ο συνδυασμός των δυο.

Β) Για k1 = (3,5) και k2 = (11,7) και $e_{k3}(x)$= $e_{k2}(e_{k1}(x))$, k3 = (3 * 11 mod26 , 11 *5 +7 mod 26) = (7,10)

Γ) 1) παίρνουμε τα στοιχεία από το Β ερώτημα, οπότε έχουμε πάλι k1 = (3,5) kai k2 =(11,7) και το Κ είναι το 11^o γράμμα στην αλφάβητο (-1)=10 : e_{k1}= a1x+ b1= 3 * 10 + 5 (mod 26)= 9

e_{k2}= a2*e_1 +b2 (mod26) = 11 * 9 + 7 (mod26) = 2

2) e_{k3} = a2(a1x+b1) +b2 mod 26 = 11(3 * 10 + 5) + 7 (mod26) = 2 άρα ίδιο με το 1).

Δ) Όχι το πεδίο τιμών του κλειδιού (το σύνολο των κλειδιών) δεν μεγαλώνει με την διπλή κρυπτογράφηση από την στιγμή που όλα τα $e_{k2}(e_{k1}(x))$ μπορούν να υπολογιστούν όπως ένα απλό $e_k(x)$ δηλαδή μια μονή κρυπτογράφηση. Άρα μια πρωτόγονη επίθεση θα ήταν το ίδιο αποτελεσματική στην διπλή κρυπτογράφηση όσο και στην μονή καθώς ($k1 \in K$, $k2 \in K$) είναι ίσο με οποιοδήποτε ($k \in K$).