Κρυπτογραφία & Πολυπλοκότητα
Σημειώσεις Παράδοσης

Επιμέλεια: Αντώνης Αντωνόπουλος

Παρασκευή, 20 Ιανουαρίου 2012

Άσκηση 1

Έστω p πρώτος και g γεννήτορας του $\mathbb{Z}_p^*$.

1. Αν δίνεται ότι $d|p-1$, να βρείτε (με αποδοτικό τρόπο) $b \in \mathbb{Z}_p^*$ τέτοιο ώστε $ord(b) = d$.

2. Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;

Λύση

1. Για το $\mathbb{Z}_p^* = \{1, 2, \ldots, 12\}$ ένας γεννήτορας είναι το $g = 2$. [1]
Γενικεύοντας αυτό το γεγονός, το στοιχείο που ψάχνουμε είναι το $b \equiv g^{\frac{p-1}{d}}$.
Αν είχαμε $d' < d$ τ.ω. $b^{d'} \equiv_p 1 \Rightarrow g^{d'(p-1)/d} \equiv_p 1 \Rightarrow ord(g) < p-1$ Άτοπο!

2. Η τάξη του g^t, $ord(g^t) = \frac{lcm(t,p-1)}{t}$
Θυμηθείτε ότι $ab = gcd(a,b) \cdot lcm(a,b) \Rightarrow \frac{a}{gcd(a,b)} = \frac{lcm(a,b)}{b}$, άρα $ord(g^t) = \frac{lcm(t,p-1)}{t} = \frac{p-1}{gcd(t,p-1)}$
Για να είναι ένα στοιχείο g^t τάξης d, πρέπει $d = \frac{p-1}{gcd(t,p-1)}$ (αν και μόνο αν), $\Rightarrow$

$$gcd(t, p-1) = \frac{p-1}{d}$$

Αυτό σημαίνει ότι $\frac{p-1}{d}|t$ και ότι είναι ο ΜΚΔ του t και του $p-1$ (εξ' ορισμού).

Έστω $c \in \mathbb{Z}_p^*$, $ord(c) = d$, και $c = g^t$. Τότε (από τα παραπάνω), το t είναι πολλαπλάσιο του $(p-1)/d$.

[1] $\mathbb{Z}_p^* = \{2 \equiv_{13} 2^1, 4, 8 \equiv_{13} 2^3, 3 \equiv_{13} 2^4, 6 \equiv_{13} 2^5, 12 \equiv_{13} 2^6, 11 \equiv_{13} 2^7, 9 \equiv_{13} 2^8, 5 \equiv_{13} 2^9, 10 \equiv_{13} 2^{10}, 7 \equiv_{13} 2^{11}, 1 \equiv_{13} 2^{12}\}$
$(2^3)^4 \equiv 1 (mod 13)$

Άρα, $\exists \lambda \in \mathbb{N} : c \equiv g^{\lambda \cdot \frac{p-1}{d}} \equiv b^{\lambda} \mod p \Rightarrow c \in < b >_p \ (= \{8, 12, 5, 1\})$ (δλδ στην υποομάδα που παράγεται από το b). Άρα, το πλήθος των στοιχείων τάξης d είναι το πολύ d:

$$\#(elements\ of\ \mathbb{Z}_p^*\ of\ order\ d) \leq d - 1$$

Στο $\mathbb{Z}_p^*$, πόσα στοιχεία είναι τάξης $p-1$; Οι αριθμοί που είναι σχετικά πρώτοι με το $p-1$, δηλαδή $\phi(p-1)$. Τότε, $ord(b^t) = \frac{lcm(t,d)}{t} = \frac{d}{gcd(t,d)}$. Άρα,

$$\#(elements\ of\ \mathbb{Z}_p^*\ of\ order\ d) = \phi(d)$$

Άσκηση 2

Θέλουμε ένα σύστημα συνεργατικής υπογραφής: χρειάζονται δύο για να παραχθεί η υπογραφή (συνυπογράφοντες), με σχήμα παρόμοιο με αυτό του RSA:
$sig(m) \equiv m^d \mod n$
$ver(m, s) \equiv 1 \Leftrightarrow s^e \mod n = m$
, όπου d το ιδιωτικό κλειδί, και (e, n) το δημόσιο.

1. Τι μπορεί να κάνει μια έμπιστη αρχή ώστε να δημιουργείται η ίδια υπογραφή με το παραπάνω σύστημα, αλλά *μόνο* με συνεργασία των δύο;

Λύση

1. Η έμπιστη αρχή (εφεξής Τ.Α.) υπολογίζει $d_1 + d_2 = d$ στέλνει στον Α το d_1 και στον Β το d_2. Τότε, ο Α υπολογίζει το $c_1 \equiv m^{d_1} \mod n$, ο Β το $c_2 \equiv m^{d_2} \mod n$, και η Τ.Α.: $c = c_1 c_2 \equiv m^{d_1+d_2} \mod n = m^d \mod n$.