ΘΕΜΑΤΑ ΠΡΟΟΔΟΥ 4/6/2024
ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διάρκεια 1 ώρα και 20 λεπτά

Θέμα 1

ΥΠΟΧΡΕΩΤΙΚΟ

Α Έστω ότι κρυπτογραφείτε με OTP το μήνυμα: m="GK" (σε ASCII). Τα κλειδιά K και μηνύματα M είναι σύνολα K, M $\in (0,1)^7$, δηλαδή $|k|=|m|=7$. Αν από όλα τα διαθέσιμα κλειδιά χρησιμοποιήσετε το: $K = 5^{32} \bmod 19$, τότε ποιό είναι το cipher; (1,5)

Β Κρυπτογραφήστε το μήνυμα m= ΠΡΟΟΔΟΣ με κλειδί:

$$Key = \begin{cases} \text{ΗΜΕΡΑ, αν Α.Μ. είναι ζυγός} \\ \text{ΝΥΧΤΑ, αν Α.Μ. είναι περιττός.} \end{cases}$$

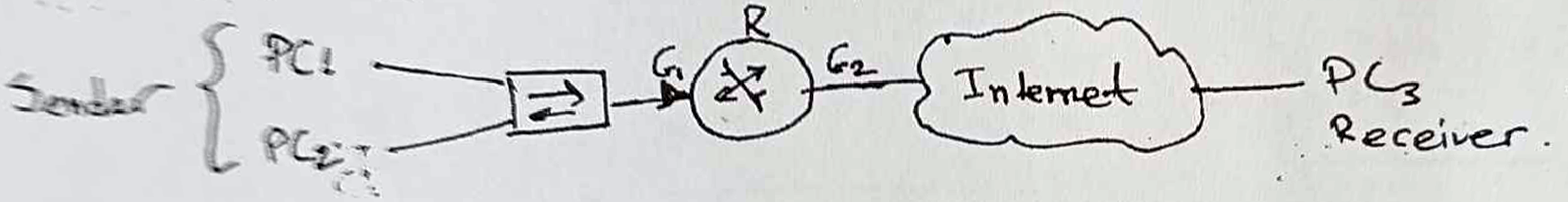
κάνετε χρήση Ελληνικά γράμματα στο Z_{24} (2)

Γ Σας δίνεται το cipher, c="LW" που έχει προκύψει από κρυπτογράφηση μηνύματος με τον ομοπαραλληλικό αλγόριθμο Affine και κλειδί K=(3,10), στο Αγγλικό αλφάβητο Z_{26}. Ποιό είναι το μήνυμα m; (1,5)

Θέμα 2

ΕΠΙΛΟΓΗΣ

Α Έστω (2) χρήστες, ο (S)ender και ο (R)eceiver, οι οποίοι ανήκουν στο ίδιο τοπικό δίκτυο.



Ο PC1 έχει IP: 192.168.1.43/24 και ο PC2 έχει IP: 192.168.1.Ε.

μία ACL έχει ρυθμιστεί στο interface G1 ως:

```
access list 1 permit 192.168.1.1 0.0.0.254
access list 1 deny any
```

Το δημόσιο κλειδί το PC1 είναι: $(n,e_1)=(119,5)$ και του PC2 είναι: $(n,e_2)=(119,7)$. Και οι δύο κρυπτογραφούν το μήνυμα $m=$"K" (στο ASCII), όμως λόγω της ACL, μόνο ένα κρυπτογράφημα περνά από τον Router. Ζητείται:

1) Ποιό περνά και γιατί;
2) Ποιό είναι το cipher που φτάνει στον Receiver;
3) Ποιό το ιδιωτικό κλειδί (d) του receiver;

(25)

* * *

B Ο A στέλνει στον B το δημόσιο κλειδί RSA $(n,e)=$ $=(43,7)$. Αν $m=27$, να υπολογιστεί η ψηφιακή υπογραφή RSA που πρέπει να σταλεί

(25)

* * *

Θέμα 3 Σύμφωνα με τη σχέση $P=K^{-1}\cdot C \bmod 26$ ΕΠΙΛΟΓΗΣ

προτείνετε το μήνυμα (αποκρυπτογράφηση) του cipher $C=$ "SYICHOLER" (Αγγλικά γράμματα στο Z_{26}).

Ποιό είναι το μήνυμα κατά αλγορίθμου HILL, εάν το κλειδί είναι: K= ALPHABET; (γράψτε 3x3 πίνακα κλειδί ως $K=\begin{pmatrix} A & L & P \\ H & A & B \\ E & T & A \end{pmatrix}$)

(5)

* * *

Καλή Επιτυχία!