Ασκήσεις 2 (Συνθηματικοί) ΑΠΑΝΤΗΣΕΙΣ

1)

ⓐ $P_0 = 0,5$, $P_1 = 0,5$, $I_0 = \log_2 \frac{1}{P_0} = 1$, $I_1 = \log_2 \frac{1}{P_1} = 1$

$H_a = P_0 I_0 + P_1 I_1 = 1$

ⓑ $P_k = 0,9$, $I_k = \log_2 \frac{1}{P_k} = 0,152$, $P_3 = 0,1$, $I_3 = \log_2 \frac{1}{P_0} = 3,322$

$H_\beta = 0,9 \cdot 0,152 + 0,1 \cdot 3,322 = 0,1368 + 0,3322 = \underline{0,469}$

2) S^L

3) ~~(crossed out text)~~

Το μέγεθος L του password καθώς hec για how
έτερα γράμμα θα έχαμε S^{L+1} ενώ με ένα άλλα
γράμμα ότο S θα έχαμε $(S+1)^L$

από το runtime την επιτροπία

4) a)

1234	a123	15876
↓	↓	↓
5,8 bits	10,1 bits	7,7 bits

b)

password	Pass_Wrd	wejrnwek
↓	↓	
28,7 bits	37,5 bits	29,3 bits

σ)

fT4Q	XJQZ
12,5 bits	14 bits

5)

of the	or his
20,8 bits	19,6 bits

ε)

this is a test	wait ho way oh
48,8 bits	50,1 bits

-1-

5. Μπορώ λίαο τω τελευταιο μέρος ποιώρι νάτο πο νέρεω που δα εχε ινανικες λέξεις για μονο μινεες ωμερες στι ρπίλλοτα (έχτι ~~και~~ και κενα.) → αιο τυτολο επιν ανγνωση

6. Ενα ΡΙΝ με 4 τυχνία νομερα δα ηταν πιο δυσκολο να το μαντεψη κανεις απ'οτι ενα που σπιοσλει της ζευκσης όπω παρόμοια και με το pass-phrase, ενα τυχαιο δ' ηταν πλυ δυσκολότερο να μαντεψει από ~~μια~~ μια γνουννη φραξη.