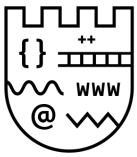
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Εργασία στο μάθημα της Κρυπτογραφίας

Όνομα 1 ΑΕΜ:

Όνομα 2 ΑΕΜ:

18 Φεβρουαρίου 2020

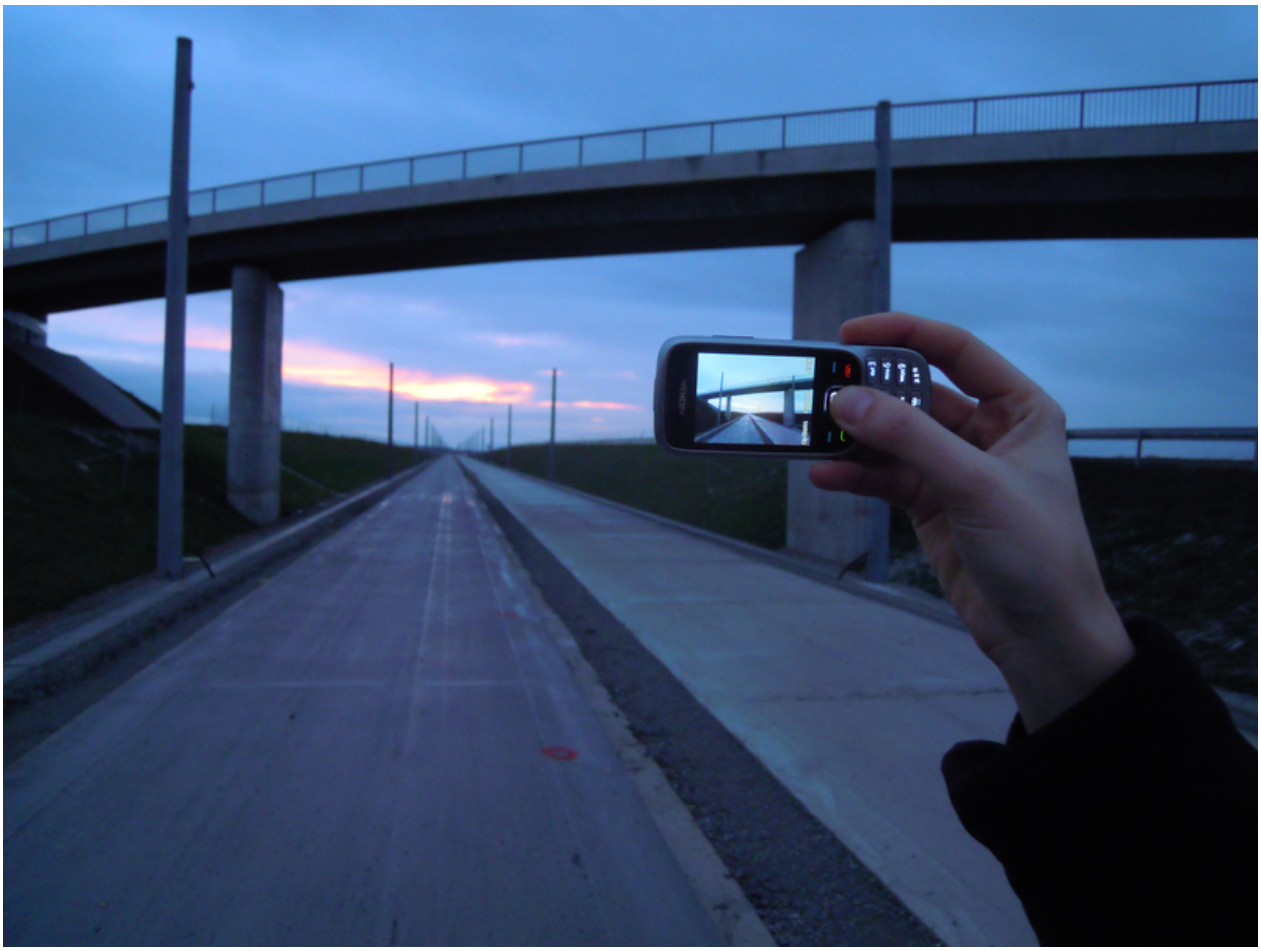
Περιεχόμενα

Περίληψη

.....

Θέμα 1

(i). ....



(**ii.**) Για την υλοποίηση του One Time Pad ...

Παρακάτω φαίνεται και η υλοποίηση.

.....

Θέμα 2

Auxiliary results

Proposition 0.1 *Let n, q and A_j be positive integers with A_j such that*

$$A_j \in I_j = \left(\frac{q^{j/(n+1)+f_q(n)}}{2}, \frac{q^{j/(n+1)+f_q(n)}}{1.5}\right), \tag{0.1}$$

with $1 \leq j \leq n$. The sequence $f_q(n) : \mathbb{N} \to (0, 1)$ is such that,

$$f_q(n) + \frac{n}{n+1} < 1 \tag{0.2}$$

and

$$\frac{q^{1+2f(n)}}{1.5} < q - \frac{1}{2}q^{n/(n+1)+f_q(n)}. \tag{0.3}$$

With L we denote the full rank lattice of rank $n+1$ generated by the vectors $\mathbf{b}_0 = (-1, A_1, \ldots, A_n)$, $\mathbf{b}_j = (0, 0, \ldots, q, \ldots, 0)$, where q is in the position $j+1$ for $j = 1, \ldots, n$. Then, for all non-zero $\mathbf{v} \in L$ we have

$$\|\mathbf{v}\| > \frac{q^{n/(n+1)+f_q(n)}}{2}.$$

Θέμα 3

Παράδειγμα κώδικα σε tex

```
from itertools import imap

def KSA(key):
```

```
  S = range(256)
  j = 0
  for i in range(256):
    j = (j + S[i] + key[i % len(key)]) % 256
    S[i], S[j] = S[j], S[i]
  return S
```