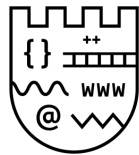


Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

---

## Εργασία στο μάθημα της Κρυπτογραφίας

---

Όνομα 1 ΑΕΜ:

Όνομα 2 ΑΕΜ:

18 Φεβρουαρίου 2020

---

## Περιεχόμενα

Περίληψη	1
Θέμα 1	2
Θέμα 2	3

## Περίληψη

.....

---

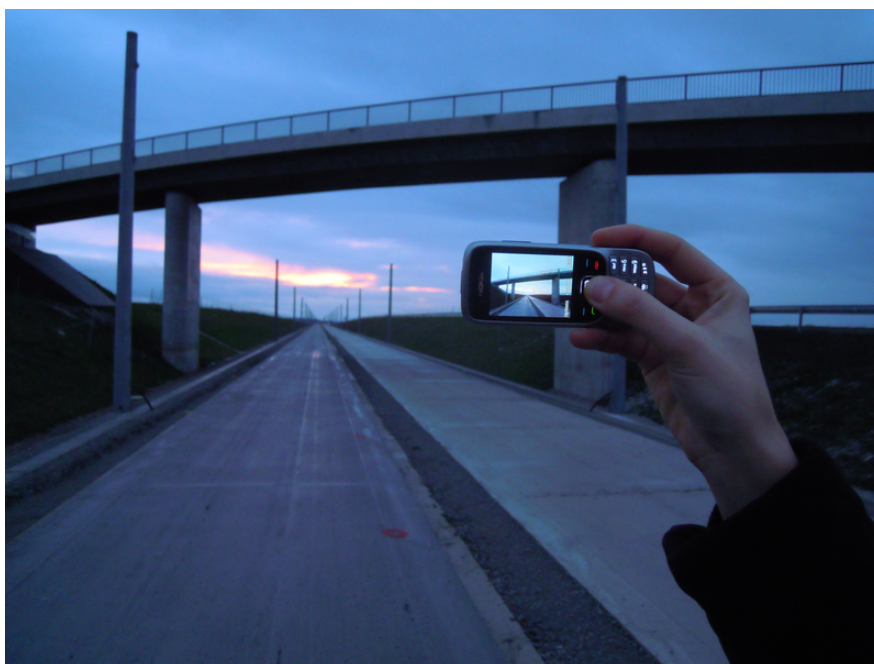
## Θέμα 1

(i). Παράδειγμα ενός πίνακα,

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
20	21	22	23	24	25	0

Παράδειγμα πως εισαγουμε μια φωτογραφια,



---

(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*

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

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

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

*and*

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

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

---

```

1 from itertools import imap
2
3 def KSA(key):
4     S = range(256)
5     j = 0
6     for i in range(256):
7         j = (j + S[i] + key[i % len(key)]) % 256
8         S[i], S[j] = S[j], S[i]
9     return S

```

Παράδειγμα ενός πίνακα της γραμμικής άλγεβρας,

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Παράδειγματα μαθηματικών όρων,

$$x \equiv 9 \pmod{17}$$

$$x \equiv 9 \pmod{12}$$

$$x^2 + y^2$$

$$\gcd(x, y) = d$$

---

$$x^n + y^n = z^n \tag{0.4}$$

Το θεώρημα του Fermat λέει ότι δεν υπάρχουν μη τετριμμένες ακέραιες λύσεις στην εξίσωση (0.4) για  $n \geq 3$ . Αποδείχτηκε από τον Andrew Wiles και δημοσιεύτηκε στο περιοδικό Annals of Mathematics.