**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ**

**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**ΜΑΘΗΜΑ: ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ, 2022-2023**

**ΔΙΔΑΣΚΟΝΤΕΣ: Γ. Στεργιόπουλος**

**1η Σειρά Ασκήσεων**

**Προθεσμία Παράδοσης: 21/12/2023**

**Συμμετοχή στην βαθμολογία: 15%**

## Άσκηση 1 [ 2 μονάδες]

### *Task 1.1*

Υπολογίστε τους ακόλουθους ΜΚΔ με χρήση του αλγορίθμου του Ευκλίδη.

(a) gcd(291,252).

(b) gcd(16261,85652).

### *Task 1.2*

Βρείτε ο ΜΚΔ των 621 και 483. Στη συνέχεια, βρείτε μια λύση των 621m + 483n = k, όπου k είναι ο ΜΚΔ των 621 και 483.

### *Task 1.3*

Υπολογίστε το $3^{64}$ modulo 67 χρησιμοποιώντας τον αλγόριθμο επαναλαμβανόμενων τετραγώνων.

## Άσκηση 2 [ 4 μονάδες]

### *Task 2.1*

Χρησιμοποιήστε ένα affine cipher για να κρυπτογραφήσετε το μήνυμα "hello" με το ζεύγος κλειδιών (7, 2). Χρησιμοποιήστε τον affine cipher για να αποκρυπτογραφήσετε το κρυπτογραφημένο κείμενο.

### *Task 2.2*

Η Eve έχει αναχαιτίσει το κρυπτογράφημα «UVACLYFZLJBYL». Δείξτε πώς μπορεί να χρησιμοποιήσει μια επίθεση ωμής βίας (brute force) για να σπάσει το κρυφό με τυφλές δοκιμές.

### *Task 2.3*

Η Eve έχει αναχαιτίσει το παρακάτω κρυπτογράφημα. Χρησιμοποιώντας μια στατιστική επίθεση για την αγγλική γλώσσα, βρείτε το απλό κείμενο.

“XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVXLQSVILYVVCFIJSVI XLIWIPPIVVIGIMZIWQSVISJJIVW”

## Άσκηση 3 [ 4 μονάδες]

### *Task 3.1*

Λύστε τις ταυτόχρονες συνέπειες $x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$.

### *Task 3.2*

Επιλεγμένη επίθεση Plaintext στο Affine Cipher. Σκεφτείτε ένα κρυπτογράφο:

$e(x) = a*x+b \bmod 26$ , με a, b αγνώστους.

1. Εκτελέστε μια επιλεγμένη επίθεση απλού κειμένου χρησιμοποιώντας το "hahaha". Το κρυπτοκείμενο είναι "NONONO".
2. Προσδιορίστε τη λειτουργία κρυπτογράφησης.