Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ, ΜΠ)

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 3/12/2022

Άσκηση 1.

1. Έστω $a, b, c \in \mathbb{N}$, όπου $gcd(a, b) = 1$ και $gcd(a, c) = 1$. Να δείξετε ότι $gcd(a, b \cdot c) = 1$.
2. Έστω $a, b \in \mathbb{N}$, όπου $gcd(a, b) = 1$. Να δείξετε ότι $gcd(a^n, b^n) = 1$, $\forall n \in \mathbb{N}$.
3. Έστω $a, b \in \mathbb{N}$. Να δείξετε ότι $gcd(a^n, b^n) = (gcd(a, b))^n$, $\forall n \in \mathbb{N}$.

Άσκηση 2.

1. Να αποδείξετε ότι $2 \mid \phi(n)$, $\forall n \geq 3$
2. Έστω $n \geq 1, n \in \mathbb{N}$ αναλύεται σε γινόμενο k περιττών πρώτων αριθμών. Να αποδείξετε ότι $2^k \mid \phi(n)$.

Άσκηση 3.

1. Αποδείξτε ότι p πρώτος αριθμός αν και μόνο αν $(p-1)! \equiv -1 \pmod{p}$.
2. Έστω p πρώτος αριθμός και a ακέραιος. Να δείξετε ότι $a^p(p-1)! + a \equiv 0 \pmod{p}$

Άσκηση 4. Έστω $\mathbb{G}$ ομάδα περιττής τάξης. Να δείξετε ότι αν $a, b \in \mathbb{G}$ τέτοια ώστε $a^2 = b^2$ τότε $a = b$

Άσκηση 5.
(α) Να δείξετε ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι επίσης κυκλική.
(β) Πόσες υποομάδες έχει η ομάδα $U(\mathbb{Z}_{4872961})$;

Άσκηση 6. Υλοποιήστε τον έλεγχο πρώτων αριθμών Fermat σε πρόγραμμα (απαιτείται να υποστηρίζονται πράξεις μεγάλων αριθμών, χιλιάδων ψηφίων). Εφαρμόστε τον για να ελέγξετε τους παρακάτω αριθμούς:
$67280421310721, 1701411834604692317316873037158841057 21, 2^{2281} - 1, 2^{9941} - 1, 2^{19939} - 1$

Άσκηση 7. Ο τελεστής $\uparrow\uparrow$ ορίζεται ως εξής:
$\alpha \uparrow\uparrow (n+1) = \alpha^{\alpha \uparrow\uparrow n}$ με $\alpha \uparrow\uparrow 1 = \alpha$.
Για παράδειγμα $3 \uparrow\uparrow 4 = 3^{3^{3^3}} = 3^{3^{27}} = 3^{7625597484987}$
Να φτιάξετε ένα κομψό και αποδοτικό πρόγραμμα, προτιμώμενα σε γλώσσα C ή Python, το οποίο να υπολογίζει τα τελευταία 17 ψηφία του αριθμού $1707 \uparrow\uparrow 1783$.
Σημείωση: ο ζητούμενος υπολογισμός μπορεί να γίνει σε χρόνο λιγότερο από 3 sec σε υπολογιστή 'κανονικών' προδιαγραφών χρησιμοποιώντας μεταβλητές τύπου long (ακέραιους 64-bit).

Άσκηση 8. Έστω $\mathbb{Z}_p^*$ με p πρώτο και g ένας γεννήτορας, p, g γνωστά.

1. Αν d ένας ακέραιος που διαιρεί το $p-1$, βρείτε με αποδοτικό τρόπο ένα στοιχείο b του $\mathbb{Z}_p^*$ τάξης d (δηλαδή d ο μικρότερος ακέραιος με $b^d \equiv 1 \pmod p$)
2. Πόσα στοιχεία τάξης d υπάρχουν μέσα στο $\mathbb{Z}_p^*$;
3. Πόσους γεννήτορες έχει η κυκλική υποομάδα που παράγει ένα στοιχείο b τάξης d;
4. Πόσες κυκλικές υποομάδες τάξης d υπάρχουν στο $\mathbb{Z}_p^*$;
5. Αν μας δώσουν ένα στοιχείο h, την τάξη του d και ένα τυχαίο στοιχείο a, πώς μπορούμε να δούμε αν το a ανήκει στην υποομάδα που παράγει το h σε πολυωνυμικό χρόνο;

Άσκηση 9.

1. Ένα DES κλειδί k είναι ασθενές αν DES_k είναι ενέλιξη (involution). Βρείτε 4 ασθενή κλειδιά του DES.

   Παρατήρηση: Για ένα πεπερασμένο σύνολο S, μια 1-1 και επί συνάρτηση $f : S \to S$ είναι ενέλιξη αν $f(f(x)) = x, \forall x \in S$.

2. Ένα DES κλειδί k είναι ημιασθενές αν δεν είναι ασθενές και υπάρχει κλειδί k' ώστε:

   $$\mathsf{DES}_k^{-1} = \mathsf{DES}_k'$$

   Βρείτε 4 ημιασθενή κλειδιά DES.

Άσκηση 10. Η κρυπτογράφηση διπλού κλειδιού με το 3DES για ένα μήνυμα m 64-bit γίνεται ως εξής:

$$c = \mathsf{DES}_{k_1}(\mathsf{DES}_{k_2}^{-1}(\mathsf{DES}_{k_1}(m)))$$

Τα k_1, k_2 έχουν μέγεθος 56 bits.

1. Ποιο είναι το μέσο πλήθος κρυπτογραφήσεων/αποκρυπτογραφήσεων της απλής εξαντλητικής αναζήτησης;

2. Έστω μια συσκευή που κρυπτογραφεί ένα μήνυμα με τον παραπάνω τρόπο την οποία και χρησιμοποιούμε για την κρυπτογράφηση μηνυμάτων της επιλογής μας. Αν 0 είναι το μήνυμα που αποτελείται μόνο από μηδενικά, μπορούμε να κατασκευάσουμε έναν πίνακα που περιέχει την κρυπτογράφηση κατά DES του 0 με τα 2^{56} κλειδιά. Στη συνέχεια χρησιμοποιώντας μια επίθεση CPA μπορούμε να κατασκευάσουμε ένα δεύτερο πίνακα με τις κρυπτογραφήσεις από την συσκευή μας για κάθε στοιχείο του πρώτου πίνακα. Με βάση τους παραπάνω πίνακες μπορούν να βρεθούν τα k_1, k_2 που χρησιμοποιεί η συσκευή. Περιγράψτε πώς.

Άσκηση 11. Έστω η κρυπτογράφηση ενός μηνύματος n block $x = x_1||\dots||x_n$ από ένα κρυπτοσύστημα E σε λειτουργία CBC και $y = y_1||\dots||y_n$ το αντίστοιχο κρυπτοκείμενο.

1. Δείξτε ότι μπορούμε να εξάγουμε πληροφορία σε περίπτωση σύγκρουσης (δηλ. $y_i = y_j$ για $i \neq j$).

2. Ποια η πιθανότητα σύγκρουσης για μπλοκ μεγέθους 64 bits;

3. Για ποια τιμή του n η επίθεση είναι χρήσιμη;

Bonus Άσκηση.
Το παιχνίδι του σιδεροθρόνου

Πριν από πολλά χρόνια, στον μακρινό τόπο της Βασιλοπροσγείωσης, ζούσε ο Τζοφραίος ο Αντιπαθητικός με τους υπηκόους του. Συνολικά ήταν $2^{19}-1$ άνθρωποι και όλοι τους είχαν από ένα θανάσιμο εχθρό, εκτός από τον Καλικάτζαρο που τον συμπαθούσαν όλοι.

Κάθε ένας από αυτούς είχε ένα προσωπικό μαχαίρι (όλα τα μαχαίρια ήταν διαφορετικά μεταξύ τους) και κάθε ένας από αυτούς είχε τραυματίσει με κάποιο μαχαίρι κάθε έναν από τους υπόλοιπους.Έτσι τελικά όλοι τους τραυματίστηκαν από όλα τα μαχαίρια (ειδικότερα, το μαχαίρι κάθε ανθρώπου χρησιμοποιήθηκε από κάποιον για να τον τραυματίσει).

Ο Καλικάτζαρος, τον οποίο κάθε άτομο τραυμάτισε με κάποιο μαχαίρι, είχε ένα μαχαίρι που ο καθένας χρησιμοποίησε για να τραυματίσει τον εαυτό του. Επίσης, ο Καλικάτζαρος τραυμάτισε κάθε άνθρωπο με το μαχαίρι του θανάσιμου εχθρού του ανθρώπου αυτού και μιας και ο ίδιος δεν είχε θανάσιμο εχθρό, αυτοτραυματίστηκε με το ίδιο του το μαχαίρι.

Για κάθε τριάδα ανθρώπων, ο άνθρωπος που τραυμάτισε τον τρίτο χρησιμοποιώντας το μαχαίρι αυτού που τραυμάτισε τον δεύτερο με το μαχαίρι του πρώτου, είναι ο ίδιος άνθρωπος που χρησιμοποίησε το μαχαίρι του πρώτου για να τραυματίσει αυτόν που τραυμάτισε τον τρίτο με το μαχαίρι του δεύτερου.

1. Αν η Δρακομάνα ήταν αυτή που τραυμάτισε τον Γιάννη τον Χιονιά με το μαχαίρι του Τζοφραίου του Αντιπαθητικού, ποιος τραυμάτισε τον Τζοφραίο τον Αντιπαθητικό με το μαχαίρι του Γιάννη του Χιονιά;

2. Αν ξέρουμε ότι η Δρακομάνα και ο Τζοφραίος ο Αντιπαθητικός είναι θανάσιμοι εχθροί, ποιος τραυμάτισε την Δρακομάνα, με το μαχαίρι της;

- Ποιος χρησιμοποίησε το μαχαίρι αυτού που τραυμάτισε τον Γιάννη τον Χιονιά με το ίδιο του το μαχαίρι, για να τραυματίσει αυτόν που τραυμάτισε τον Τζοφραίο τον Αντιπαθητικό με το ίδιο του το μαχαίρι;

Σύντομες οδηγίες: (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*.