National Technical University of Athens
School of Electrical and Computer Engineering

Computational Cryptography

(ECE, SEMFE, ALMA, AMS)

2nd Exercise Set

Deadline: 3/12/2022

Question 1.

1. Let $a, b, c \in \mathbb{N}$, where $gcd(a, b) = 1$ and $gcd(a, c) = 1$. Prove that $gcd(a, b \cdot c) = 1$.
2. Let $a, b \in \mathbb{N}$, where $gcd(a, b) = 1$. Prove that $gcd(a^n, b^n) = 1$, $\forall n \in \mathbb{N}$.
3. Let $a, b \in \mathbb{N}$. Prove that $gcd(a^n, b^n) = (gcd(a, b))^n$, $\forall n \in \mathbb{N}$.

Question 2.

1. Prove that $2 \mid \phi(n)$, $\forall n \geq 3$
2. Let $n \geq 1, n \in \mathbb{N}$ and assume that n has k distinct odd prime factors. Prove that $2^k \mid \phi(n)$.

Question 3.

1. Prove that p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.
2. Let p be a prime and a integer. Prove that $a^p(p-1)! + a \equiv 0 \pmod{p}$

Question 4. Let $\mathbb{G}$ be a group of odd order. Prove that if $a, b \in \mathbb{G}$ such that $a^2 = b^2$ then $a = b$.

Question 5.

1. Prove that every subgroup of a cyclic group is cyclic.
2. How many subgroups does the group $U(\mathbb{Z}_{4872961})$ have?

Question 6. Implement the Fermat's primality test into program (it should support operations of large numbers, with thousands of digits).
Run the code to test the following numbers:
$67280421310721, 1701411834604692317316873037158841057 21, 2^{2281} - 1, 2^{9941} - 1, 2^{19939} - 1$

Question 7. The operator $\uparrow\uparrow$ is defined as follows:
$\alpha \uparrow\uparrow (n+1) = \alpha^{\alpha\uparrow\uparrow n}$, where $\alpha \uparrow\uparrow 1 = \alpha$.
For example $3 \uparrow\uparrow 4 = 3^{3^{3^3}} = 3^{3^{27}} = 3^{7625597484987}$
Implement an elegant and efficient program, preferably in language C or Python, that calculates the last 17 digits of the number $1707 \uparrow\uparrow 1783$.
Note: the requested calculation can be done in time less than 3 sec in a "normal" computer using variables of type long (integers 64-bit).

Question 8. Let $\mathbb{Z}_p^*$ where p is prime and g a generator, p, g are known.

1. If d is an integer that divides p–1, find efficiently an element b of $\mathbb{Z}_p^*$ of order d (d is the smaller integer such that $b^d \equiv 1 \pmod p$)
2. How many elements of order d are there in $\mathbb{Z}_p^*$?
3. How many generators has the cyclic subgroup that is produced by an element b of order d?
4. How many cyclic subgroups of order d are there in $\mathbb{Z}_p^*$;
5. If we are given an element h, its order d and a random element a, how can we check whether a belongs to the subgroup that is produced by h in polynomial time?

Question 9.

1. A DES key k is weak if DES_k is an involution. Exhibit 4 weak keys for DES.
   Note: For a finite set S, a 1-1 and onto function $f : S \to S$ is an involution if $f(f(x)) = x, \forall x \in S$.
2. A DES key k is semi-weak if it is not weak and there exists a key k' such that:
   $$\mathsf{DES}_k^{-1} = \mathsf{DES}_{k'}$$
   Exhibit 4 semi-weak keys for DES.

Question 10. The two-key 3DES encrypts a 64-bit message m in the following manner:

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

k_1, k_2 are strings of size 56 bits each.

1. What is the average number of encryptions/decryptions of a 'naive' exhaustive search?

2. We are given a box that encrypts a message according to the above manner. If 0 is the message containing only zeros, we can build a table that contains the standard DES **decryption** of 0 under all 2^{56} keys. Then we use a CPA attack we can build a second table containing the box encryptions for every element of the first table. Given these two tables, one can find both k_1, k_2 used by the encryption box. Describe how.

Question 11. Consider the encryption of an n block message $x = x_1||\dots||x_n$ by a cryptosystem E in CBC mode and $y = y_1||\dots||y_n$ the corresponding ciphertext.

1. Show that we can extract information in case of collision (i.e. if $y_i = y_j$ για $i \neq j$).
2. What is the probability of getting a collision when the block size of E is 64 bits?
3. For which n does this attack become useful?

Bonus Question.
The game of thrones

Once upon a time in a region far, far away, in the kingdom of King's Landing, there lived King Joffrey the Usurper with his people. They were $2^{19}-1$ people in total and each one of them had a mortal enemy, apart from the Imp that everyone liked.

Each one of them had a personal knife (all the knives are pairwise different) and each one of them had injured with some knife each one of the rest. Then finally everyone was injured by all the knives (specifically, the knife of each person was used by someone to injure him)

The Imp, whom every person injured with some knife, had a knife that everyone used to injure himself. Also, the Imp injured every person with the knife of the mortal enemy of this person, and since he didn't have a mortal enemy he injured himshelf.

For every triplet of people, the person that injured the third using the knife of the person that injured the second with the knife of the first, is the same person that used the knife of the first to injure the person that injured the third with the knife of the second.

1. If the Dragonmother was the one that injured John Snow with the knife of King Joffrey the Usurper, who injured King Joffrey the Usurper with the knife of John Snow?
2. If we know that the Dragonmother and King Joffrey the Usurper are mortal enemies, who injured the Dragonmother with her knife?

☠ Who used the knife of the person that injured John Snow with his personal knife to injure the one that injured King Joffrey the Usurper with his own knife?

Best of Luck !