Third assignment

Cryptography, ITC8240

December 2021

1 Important notices:

- If you have any questions regarding the tasks, please do not hesitate to contact me.
- This assignment is voluntary. You will get 0.5 point to your final mark if you solve 65% of the tasks, and 1.0 point if you solve 90% of the task.
- **Provide an explicit explanation to your solutions**. Providing answers to the task with no explanation will give you 0 points.
- Your solution should be in the PDF format. You may either scan a handwritten solution or type your solution (Word, TXT, LaTeX, etc.) and export it into PDF.
- For submitting your solution in a LaTeX, you get up to 4 bonus points.
- You may write the programming code to solve any task. However, you have to explain explicitly the code logic in your submission and how it helped you solving the task. Providing the code with no explanations will give you 0 points for the task. You must submit your code either in the appendix of your submission or to a public repository (GitHub, Bitbucket, Gitlab).
- **Bruteforce is not a solution!**
- Using online tools or/and someone's else code to solve the tasks is prohibited. If you are suspected of this, then you will receive 0 for the task.

- Plagiarism is prohibited. If you are suspected of this, then you will receive 0 for the task and will be reported to the Dean's office.
- This assignment is due 26th of December, 23:59. No late submissions are allowed.

2 Assignment tasks

2.1 Task 1 (12 points) - Groups and Number theory

- Is $(\mathbb{Q}, +)$ (*Rationals under addition*) a group? Motivate your answer.
- Is $(\mathbb{Z}_{33} \setminus \{0\}, *)$ (*Integers modulo 33 excluding 0 under multiplication*) a group ? Motivate your answer.
- Write down a definition of homomorphism. Show a homomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{R}^+, *)$.
- Estonian boatswain is trying to sell corsair Alice a sailboat, however without revealing the age of the sailboat. From several sailors Alice found that one year ago, its age was a multiple of 4, in 3 years its age will be a multiple of 7, and in 5 years multiple of 11. Help Alice to deduce the age of the sailboat. **Do not skip calculations in this solution!!!**
- Calculate the order of 7 in $(U_{15}^*, *)$ (set of units)
- Calculate Euler's totient function for number 55440.
- Calculate $(-14)^{42} \mod 1181$. **Provide intermediate calculations**

2.2 Task 2 (7 points) - Probability theory

- The box contains 3 white balls and 2 black ones. One ball is drawn from the box, and then the second. Event B - the appearance of a white ball at the first draw. Event A - the appearance of a white ball on the second draw. Find $P(A|B)$ and $P(A|\overline{B})$

- Among the 30 cryptography exam variants, there are 7 "lucky". Two students take turns taking one variant (the first student takes each of the variant with the same probability, the second - equally likely any of the remaining ones). Find the probability that the second student took the "lucky" variant. Write your answer as a fraction $\frac{X}{Y}$.
- Cryptography students is solving multiple choice task. There are n options. If cryptography student knows a solution, they choose the right option. If they do not - they randomly choose the answer with probability $\frac{1}{n}$. What is the probability, that student knows a solution for a task, under a condition that they chose the right option? (**Hint**: a) treat probability of student knowing the answer as parameter b) Bayes formula

2.3 Task 2 (8 points) - RSA

- Show that RSA is not IND-CCA2. The IND–CPA game is defined as follows

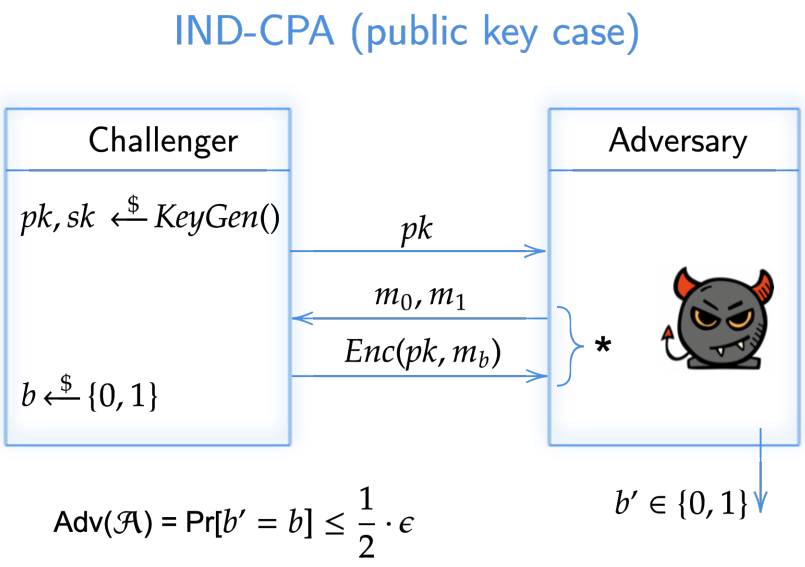

Figure 1: IND-CCA2 Game

- Imagine the following modification to the RSA encryption scheme. In-

stead of generating p and q as a distinct prime numbers, we set $q = p$ (i.e. modulus $n = p^2$). All other steps remain the same. Please, explain, is the security of the scheme affected by this change? If yes, please provide an attack.

2.4 Task 3 (6 points) - ElGamal encryption

1. Consider the ElGamal cryptosystems with a public key (p, q, y) and a private key x. Encrypt the message $m = 15131$ using parameters $p = 199999, q = 23793, x = 894, r = 723$. Decrypt the ciphertext $c = (299, 457)$ using parameters $p = 503, q = 2, x = 42$.

2. Assume there is an jewellery auction happening, both Alice and Eve want to buy precious diamond earrings. The rules of the auction are the following:

   - Each bidder places a bid.
   - The highest bidder gets the first slot, the second-highest, the second slot and so on.
   - The highest bidder pays the price bid by the second-highest bidder.

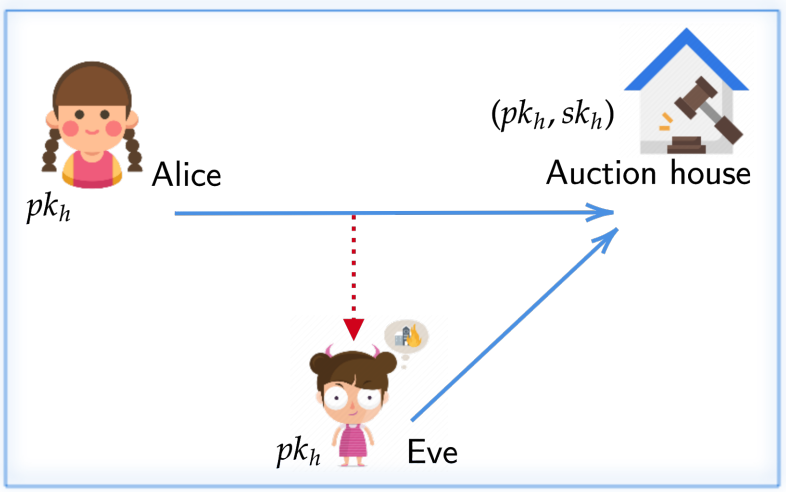

Figure 2: Auction setup

Eve found out that the bids are sent to the auction house in encrypted form, using ElGamal encryption. Additionally, Eve can eavesdrop on communication between Alice and auction house. Explain, how can Eve win the auction using homomorphic properties of ElGamal.

2.5 Task 4 (9 points) - Hash functions and signatures

Part 1. Let p be a prime number and let g be a generator of $\mathbb{Z}_p^*$. Suppose we have the following function: $f : \mathbb{Z} \to \mathbb{Z}_p^*$, where $f(x) = g^x \mod p$. Is f collision resistant? Please, explain your answer.

Part 2. Assume Alice uses some signature algorithm S with a hash function H that is **not** collision resistant. That is, to sign a message m Alice first computes $H(m)$ and then uses some secret key to sign $H(m)$. Explain, how malicious Carl can trick Alice into signing a fraudulent document.