Prof. M. Gastpar

Quiz 4 (Homeworks 7, 8 & 9)

Due on Moodle

on Monday, April 28, 2024, at 23:59.

Quiz 4

SCIPER : **111111**

- This quiz is to be solved individually.
- Try not to use any of the course materials other than the formula collection on a first attempt.
- Once you are done, enter your answers into Moodle. Moodle will give you feedback. You can update your answers as many times as you want before the deadline.
- For each question there is **exactly one** correct answer. We assign **negative points** to the **wrong answers** in such a way that a person who chooses a wrong answer loses **25 %** of the points given for that question.

Question 1

[2 points] Consider the group $(\mathbb{Z}/207\mathbb{Z}^*, \cdot)$. Find how many elements are in the group.

- ☐ 128
- ☐ 100
- ☐ 127
- ☐ 132

Question 2

[3 points] Passing on secrets: Alice has posted her RSA credentials as (m, e), with m the modulus and e the encoding exponent. As required by RSA, she keeps her decoding exponent d preciously secret. Bob has a message t_1, RSA-encrypts it using (m, e_1) and passes the resulting cryptogram c_1 on to Carlos. Carlos has a message t_2, RSA-encrypts it using (m, e_2) to obtain the cryptogram c_2. Then, Carlos multiplies the two cryptograms, $(c_1 \cdot c_2) \mod m$, and passes this to Alice. Alice applies her regular RSA decryption to $(c_1 \cdot c_2) \mod m$. Under what condition is the result of this decryption exactly equal to the product $(t_1 \cdot t_2) \mod m$?

- ☐ If d is prime and $(e_1 + e_2) \mod m = 1$.
- ☐ If for some integer ℓ, we have $e_1 e_2 d = \ell\phi(m) + 1$, where $\phi(\cdot)$ denotes Euler's totient function.
- ☐ If $e_1 + e_2 = e$.
- ☐ If $e_1 = e_2 = e$.

Question 3

[6 points] *Note: This is an* **open** *question. In the real exam, we will grade your arguments. Here for the quiz, we do not have the capacity to do this. Therefore, you will merely enter your final answer into a multiple choice grid on Moodle. However, do make sure to carefully look at the solution and compare to your answer. How many points would you have given yourself?*

Consider the source $S_1, S_2, \ldots$ such that S_1 is uniformly distributed on $\mathbb{Z}/10\mathbb{Z}^*$, and for every $n \geq 1$, S_{n+1} is distributed uniformly on $\mathbb{Z}/(S_n + 1)\mathbb{Z}^*$. Answer the following questions.

(a) (3 pts) Calculate the marginal distribution of S_2.

(b) (1 pt) Is the source stationary? Fully justify your answer

(c) (2 pts) Show that $H(S_n|S_1, \ldots, S_{n-1}) \leq \big(p_{S_{n-1}}(3) + p_{S_{n-1}}(5)\big) \log 2 + \big(p_{S_{n-1}}(7) + p_{S_{n-1}}(9)\big) \log 4$.

(d) *[Difficult, and not graded on the Moodle interface]* Show that the probabilities in the right hand side of the above inequality converge to zero as n increases.

Question 4

[6 points] Consider an RSA encryption where the (p, q) are determined as $(67, 53)$. Check if the following encoding and decoding exponent pairs are valid.

(a) $(e, d) = (123, 79)$ are valid exponents.

☐ VRAI ☐ FAUX

(b) $(e, d) = (631, 223)$ are valid exponents.

☐ VRAI ☐ FAUX

(c) $(e, d) = (319, 23)$ are valid exponents.

☐ VRAI ☐ FAUX

Question 5

[3 Points] How many $x \in \{0, 1, 2, \ldots, 34\}$ satisfy the equation $x^2 - 5x + 4 \mod 35 = 0$?

☐ 2
☐ 1
☐ 0
☐ 4