**Prof. M. Gastpar**

**Quiz 3 (Homeworks 5, 6 & 7)**

**Due on Moodle**

**on Monday, April 7, 2025, at 23:59.**

# Quiz 3

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] Answer the following True/False Questions

(a) $53^{654} \mod 17 = 1$

□ VRAI □ FAUX

(b) $252197 \mod 11 = 9$

□ VRAI □ FAUX

**Question 2**

[4 points] If we compute $\gcd(89, 65)$ via Euclid's extended algorithms, we produce a sequence of $(u, v)$ pairs, the last of which satisfies $\gcd(89, 65) = 89 \times u + 65 \times v$. Check the correct sequence.

□ $(1, 0)$, $(0, 1)$, $(1, -2)$, $(-2, 4)$, $(4, -7)$, $(-7, 20)$, $(20, -26)$.

□ $(1, 0)$, $(0, 1)$, $(1, -2)$, $(-2, 5)$, $(5, -7)$, $(-7, 19)$, $(19, -26)$.

**Question 3**

[8 points] Alice and Bob are studying cryptography for the first time. They each did a project and each got a score. The score is out of 30 points. They represent it with 5 bits, using the natural binary representation. They want to tell their project scores to their friend Charlie, using the one-time pad. Charlie has a single uniformly sampled binary string $K$ of length 5. He sends this *same* string to both Alice and Bob. Nobody else ever gets to know $K$.

Class policy dictates that students get a grade of 6 on the project if they score more than 27 points and a grade of 5.75 if they score more than 23 points.

Several people have partial information and try to infer Alice's and Bob's grades:

- David intercepts only Bob's transmission.
- Eve intercepts both Alice's and Bob's transmissions.
- Frank does not intercept anything, but he saw Bob very happy on finding his project score. So Frank knows that Bob received a grade of 6.

(a) David can tell if Bob got a grade of 6 on the project

□ VRAI □ FAUX

(b) Eve can tell for sure if Alice and/or Bob received full points.

□ VRAI □ FAUX

(c) Eve can tell who scored more points between Alice and Bob.

□ VRAI □ FAUX

(d) Frank can help Eve deduce if Alice got a grade of 5.75 or more.

□ VRAI □ FAUX

### Question 4

[3 points] Find $x$ such that $[10]_{56}x = [38]_{56}$.

□ 15

□ 28

□ 41

□ 49

### Question 5

[3 points] Find all solutions of $28x + [12]_{35} = [21]_{35}$ in the range $[0, 34]$. How many different solutions are there?

□ 1

□ 2

□ 3

□ 0