**Ens. : TEACHER NAME**
**EXAM NAME - MAN**
**DATE**
**Durée : XXX minutes**

1

# Student One

SCIPER : **111111**

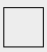
**Do not turn the page before the start of the exam. This document is double-sided, has 12 pages, the last ones possibly blank. Do not unstaple.**

- Place your student card on your table.
- **No other paper materials** are allowed to be used during the exam.
- Using a **calculator** or **any electronic device** is not permitted during the exam.
- For each question there is **exactly one** correct answer. We assign **negative points** to the **wrong answers** in such a way that a person that chooses uniformly at random over the possible options gains 0 points on average.
- Use a **black or dark blue ballpen** and clearly erase with **correction fluid** if necessary.
- Unless specified otherwise, all the entropies are in bits.

Respectez les consignes suivantes | Observe this guidelines | Beachten Sie bitte die unten stehenden Richtlinien

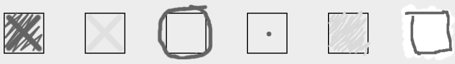
choisir une réponse | select an answer
Antwort auswählen

ne PAS choisir une réponse | NOT select an answer
NICHT Antwort auswählen



Corriger une réponse | Correct an answer
Antwort korrigieren

ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte



# First part: Source Coding

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

### Question 1

[6 points] Consider a source $S$ with some distribution $P_S$ over the alphabet $\mathcal{A} = \{a, b, c, d, e, f\}$. Bob designs an encoding map $\Gamma$ for a uniquely decodable code $\mathcal{C}$ over a code alphabet $\mathcal{D}$ of size $D$ with the following codeword lengths.

| | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|---|---|---|---|---|---|---|
| $l(\Gamma(\cdot))$ | 1 | 1 | 2 | 2 | 3 | 3 |

Answer the following true/false questions.

There exist a positive integer $D$ and a distribution $P_S$ over $\mathcal{A}$ such that the average codeword length of Bob's code is equal to $H_D(S)$.

☐ VRAI ☐ FAUX

The average codeword length of the code is necessarily greater than or equal to $H_D(S)$.

☐ VRAI ☐ FAUX

$D$ can be 2.

☐ VRAI ☐ FAUX

### Question 2

[4 points] You are given an i.i.d source with symbols taking value in the alphabet $\mathcal{A} = \{a, b, c, d\}$ and probabilities $\{1/8, 1/8, 1/4, 1/2\}$. Consider making blocks of length $n$ and constructing a Huffman code that assigns a binary codeword to each block of $n$ symbols. Choose the correct statement regarding the average codeword length per source symbol.

- ☐ None of the others.
- ☐ In going from $n$ to $n+1$, for some $n$ it stays constant and for some it strictly decreases.
- ☐ It is the same for all $n$.
- ☐ It strictly decreases as $n$ increases.

**Question 3**

[4 points] Let $X_1, X_2$ be two independent random variables taking values in $\{0, 1\}$ such that $P(X_1 = 0) = P(X_2 = 0) = 1/2$. Let $Y = X_1 + X_2 \bmod 2$. Answer the following true/false questions.

$H(X_1, X_2, Y) = H(X_1) + H(X_2) + H(Y)$ .

☐ VRAI ☐ FAUX

$H(Y, X_1) = H(Y) + H(X_1)$.

☐ VRAI ☐ FAUX

If I change the distribution of $X_1$ (while keeping the alphabet the same) I can obtain a new random variable $\hat{X}_1$ such that $H(\hat{X}_1) > H(X_2)$.

☐ VRAI ☐ FAUX

$H(X_1, X_2) = H(X_1) + H(X_2)$ .

☐ VRAI ☐ FAUX

**Question 4**

[4 points] Let $\mathcal{C}_1 = \{00, 01, 100, 101, 110, 111\}$ and $\mathcal{C}_2 = \{00, 01, 100, 101, 111\}$ be two source codes (We exclude the possibility of source symbols of zero probability.) Check the correct statement.

- ☐ $\mathcal{C}_1$ can be a Huffman code but not $\mathcal{C}_2$.
- ☐ Neither $\mathcal{C}_1$ nor $\mathcal{C}_2$ can be a Huffman code.
- ☐ Both codes can be Huffman codes.
- ☐ $\mathcal{C}_2$ can be a Huffman code but not $\mathcal{C}_1$.

**Question 5**

[3 points] Consider the i.i.d. source $S_1S_2S_3\dots$ where for all $i$, $S_i$ models a loaded dice with distribution $P(S_i = 6) = 5/6$ and $P(S_i = x) = 1/30$ for $x \in \{1, 2, 3, 4, 5\}$. Answer the following true/false questions.

$H(S_n|S_{n-1}) \neq H(S_n)$ .

☐ VRAI ☐ FAUX

$\lim_{n\to\infty} H(S_n) = \log_2(6)$.

☐ VRAI ☐ FAUX

The source is regular.

☐ VRAI ☐ FAUX

$H(S_n, S_{n+1}) = H(S_n) + H(S_{n+1})$.

☐ VRAI ☐ FAUX

The source is stationary.

☐ VRAI ☐ FAUX

$H(S_n) = H(S_{n-1})$.

☐ VRAI ☐ FAUX

**Question 6**

[5 points] A bag contains the letters of LETSPLAY. Someone picks at random 4 letters from the bag without revealing the outcome to you. Subsequently you pick one letter at random among the remaining 4 letters. What is the entropy (in bits) of the random variable that models your choice? Check the correct answer.

- ☐ $\log_2(7)$.
- ☐ $\frac{11}{4}$.
- ☐ 2.
- ☐ $\log_2(8)$.

**Question 7**

[5 points] Let $0 \le \alpha \le 1$ be an unknown constant. Let $X$ be a random variable taking values in $\mathcal{X} = \{0, 1, 2\}$ with probability $p_X(0) = p_X(1) = \alpha$ and $p_X(2) = 1 - 2\alpha$. Let $Y$ be a random variable defined as follows

$$Y = \begin{cases} 1, & \text{if } X = 2 \\ 0, & \text{if } X \neq 2 \end{cases}.$$

You also know that $H(X|Y) = \frac{1}{2}$. Choose the correct value of $\alpha$.

- ☐ 1.
- ☐ $\frac{1}{2}$.
- ☐ $\frac{1}{4}$.
- ☐ $\frac{1}{8}$.

## Second part: Cryptography and Number Theory

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

### Question 8

[5 points] If we compute $\gcd(70, 51)$ via Euclid's extended algorithms, we produce a sequence of $(u, v)$ pairs, the last of which satisfies $\gcd(70, 51) = 70 \times u + 51 \times v$. Check the correct sequence.

- ☐ $(1, 0)$, $(0, 1)$, $(1, -2)$, $(-2, 3)$, $(3, -8)$, $(-8, 11)$.
- ☐ $(1, 0)$, $(0, 1)$, $(1, -2)$, $(-2, 5)$, $(5, -8)$, $(-8, 11)$.

### Question 9:

[6 points] Answer the following true/false questions.

$(\mathbb{Z}/8\mathbb{Z}^\star, \cdot)$ is isomorphic to $(\mathbb{Z}/k\mathbb{Z}, +)$ for some $k$.

☐ VRAI ☐ FAUX

$(\mathbb{Z}/9\mathbb{Z}, +)$ is isomorphic to $((\mathbb{Z}/3\mathbb{Z})^2, +)$.

☐ VRAI ☐ FAUX

$(\mathbb{Z}/6\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}, +)$ is isomorphic to $((\mathbb{Z}/2\mathbb{Z})^2, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$.

☐ VRAI ☐ FAUX

### Question 10

[4 points] How many integers $n$ between 1 and 2021 satisfy $10^n \equiv 1 \mod 11$? Check the correct answer.

- ☐ 1010.
- ☐ 183.
- ☐ 505.
- ☐ 990.

**Question 11:**

[6 points] Answer the following true/false questions.

$[3^{10}2^{5}14]_{19}$ has a multiplicative inverse.

☐ VRAI ☐ FAUX

$[60]_{15}$ has a multiplicative inverse.

☐ VRAI ☐ FAUX

$[126]_{147}$ has a multiplicative inverse.

☐ VRAI ☐ FAUX

$[169]_{9}$ has a multiplicative inverse.

☐ VRAI ☐ FAUX

**Question 12**

[6 points] Consider the Diffie-Hellman secret-key-exchange algorithm performed in the cyclic group $(\mathbb{Z}/11\mathbb{Z}^{\star}, \cdot)$. Let $g = 2$ be the chosen group generator. Suppose that Alice's secret number is $a = 5$ and Bob's is $b = 3$. Which common key $k$ does the algorithm lead to? Check the correct answer.

- ☐ $k = 10$.
- ☐ $k = 7$.
- ☐ $k = 9$.
- ☐ $k = 2$.

**Question 13:**

[7 points] Consider an RSA encryption scheme with parameters $m = 55$, $e = 3$ and $k = \phi(m)$. Answer the following true/false questions.

Both $d = 27$ and $d = 67$ are valid decryption exponents.

☐ VRAI ☐ FAUX

The encryption of $t = 18$ is $c = 4$.

☐ VRAI ☐ FAUX

## Third part: Coding Theory

For each question, mark the box corresponding to the correct answer. Each multiple choice question has **exactly one** correct answer.

**Question 14:**

[6 points] A generator matrix $G$ for a binary $(6, 3)$ linear code maps the information vectors $m_1 = (1, 0, 1)$ and $m_2 = (1, 1, 1)$ into the codewords $c_1 = (1, 1, 0, 0, 0, 1)$ and $c_2 = (1, 0, 0, 0, 1, 0)$ respectively. Answer the following true/false questions.

$G$ is in systematic form.

☐ VRAI ☐ FAUX

The second row of $G$ is $(0, 1, 0, 0, 1, 1)$.

☐ VRAI ☐ FAUX

$d_{\min} = 3$.

☐ VRAI ☐ FAUX

**Question 15**

[2 points] What is the minimum distance of a linear block code over $\mathbb{F}_7$ that has

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 6 \\ 0 & 1 & 0 & 0 & 6 & 6 \\ 0 & 0 & 1 & 0 & 6 & 3 \end{pmatrix}$$

as the parity check matrix? Check the correct answer.

- ☐ 5.
- ☐ 4.
- ☐ 1.
- ☐ 3.
- ☐ 2.
- ☐ 0.

**Question 16**

[5 points] How many $x \in \mathbb{Z}/23\mathbb{Z}$ satisfy the equation $0 = 1 - x + x^2 - x^3 + .... - x^{21} + x^{22} - x^{23}$, when all operations are with respect to the field $(\mathbb{Z}/23\mathbb{Z}, +, \cdot)$? Check the correct answer.

- ☐ 2.
- ☐ 23.
- ☐ 22.
- ☐ 0.
- ☐ 1.

**Question 17**

[4 points] Consider a $(k+1, k)$ block code that to a binary sequence $x_1, \ldots, x_k$ associates the codeword $x_1, \ldots, x_k, x_{k+1}$, where $x_{k+1} = x_1 + \ldots + x_k \bmod 2$. This code can detect all the errors of odd weight.

☐ VRAI ☐ FAUX

**Question 18**

[6 points] Let $E$ be a subspace of $\mathbb{F}_7^4$ which consists of elements $\vec{x} = (x_1, x_2, x_3, x_4)$ satisfying,

$$\begin{aligned} x_1 + 6x_2 + 3x_3 + 4x_4 &= 0 \\ 3x_1 + 6x_2 + x_3 + 3x_4 &= 0 \\ 5x_1 + 2x_2 + x_3 + 3x_4 &= 0 \end{aligned}$$

What is the dimension of $E$? Check the correct answer.

- ☐ 3.
- ☐ 1.
- ☐ 2.
- ☐ 4.
- ☐ 0.

**Question 19**

[4 points] Consider an $(n, k)$ RS code. If you delete up to $n-k$ columns of the generator matrix, the result is still an RS code (for some choice of parameters).

☐ VRAI ☐ FAUX

**Question 20**

[3 points] Consider a communication system consisting of a binary block code, an error channel, and a minimum-distance decoder. Check the correct statement about the minimum-distance decoder.

- ☐ None of the others can be stated with certainty due to missing information.
- ☐ It always minimizes the error probability.
- ☐ It minimizes the error probability if the channel is a binary symmetric channel.
- ☐ It minimizes the error probability if the channel is a binary symmetric channel with crossover (flip) probability smaller than 1/2.

**Question 21:**

[2 points] Consider a standard-array-based decoder. Answer the following true/false questions.

The syndrome of a specific coset depends on the choice of the coset leader.

☐ VRAI ☐ FAUX

For the same input, the decoder output depends on the choice of the coset leader.

☐ VRAI ☐ FAUX

**Question 22**

[3 points] Consider a $(7,4)$ Reed-Solomon code $\mathcal{C}$ over $\mathbb{F}_q$. Let $\vec{x} \neq \vec{y}$ be two different information vectors. The corresponding codewords $c(\vec{x})$ and $c(\vec{y})$ match in at most:

- ☐ 3 places.
- ☐ 2 places.
- ☐ 0 places.
- ☐ None of the others is correct.