

Homework 1 – Prerequisites Test

Cryptography and Security 2022

Name:		
COIDED		
SCIPER: .		

- ♦ This document contains 3 independent exercises.
- ♦ Do NOT open this document until the beginning of the exam.
- ♦ Duration: **105 minutes** (one hour and forty-five minutes).
- ♦ This is a closed book exam. No extra sheet is allowed.
- Allowed Material: blue or black pen (avoid pencils), eraser. Except for a basic pocket calculator or a non-connected clock, any other kind of electronic device is forbidden.
- ♦ Food and water are allowed but should not disturb the exam when consumed.
- Blank pages are provided at the end of the exam and can be used as scrap paper or to report answers. If needed, additional scrap paper will be provided.
- Only answers directly written on the exam sheet will be corrected.
- ⋄ Each answer must be written in English in the dedicated box. If the answer is put at the end, clearly indicate which exercise it refers to. In particular, properly separate scrap text from answers to be corrected.
- ♦ Non-trivial statements must be **cleanly and formally justified**.
- ♦ Questions about the (technical) content of the exam will not be answered.
- ♦ Prepare the CAMPIRO card or an official ID paper for the identity check.

THIS PACE INTERVITOR ALLEY LETTERS PACE INTERVITOR AND A STATE OF THE PACE OF

Exercise 1 Probability

Given a discrete random variable X, we recall the definition of entropy H(X)

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x)$$

And the associated notion of joint entropy H(X,Y) and conditional entropy H(X|Y)

$$H(X,Y) = -\sum_{x \in X} \sum_{y \in Y} p(x,y) \log_2 p(x,y)$$

$$H(X|Y) = -\sum_{x \in X} \sum_{y \in Y} p(x, y) \log_2 p(x|y)$$

Question 1.1

Show the following *chain rule* for entropy.

$$H(X,Y) = H(Y) + H(X|Y)$$

Question 1.2

Consider the following symmetric encryption system: We consider a plaintext space $\mathcal{M} = \{m_1, m_2, m_3\}$, key space $\mathcal{K} = \{k_1, k_2, k_3\}$ and a ciphertext space $\mathcal{C} = \{1, 2, 3, 4, 5\}$. We denote by P, C, K the random variables for the plaintext, ciphertext and keys respectively. The encryption is given by the following matrix:

$$\begin{pmatrix} m_1 & m_2 & m_3 \\ k_1 & 2 & 1 & 4 \\ k_2 & 1 & 5 & 3 \\ k_3 & 2 & 4 & 5 \end{pmatrix}.$$

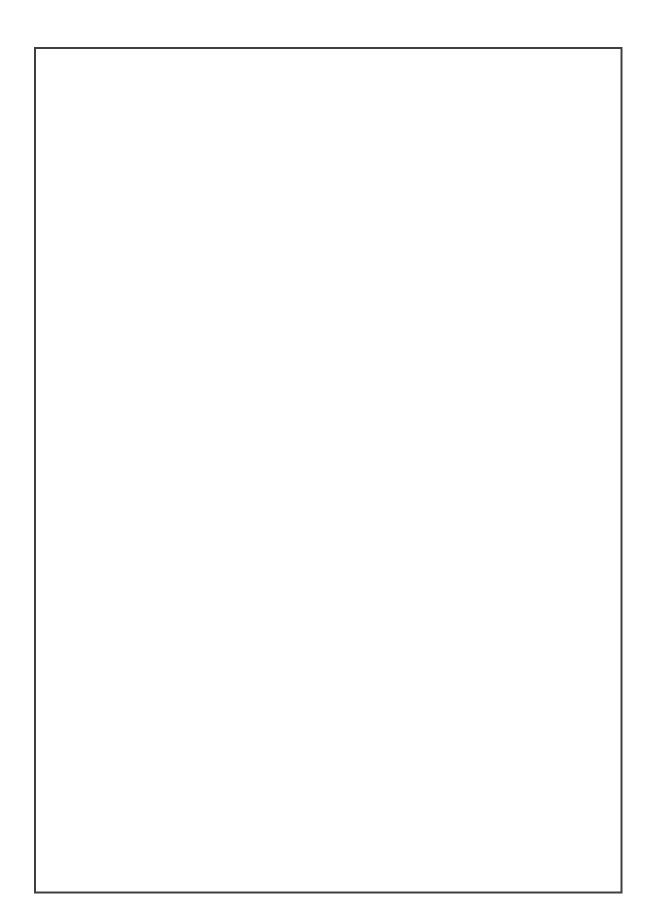
This means that e.g. the encryption of m_1 with k_1 is 2.

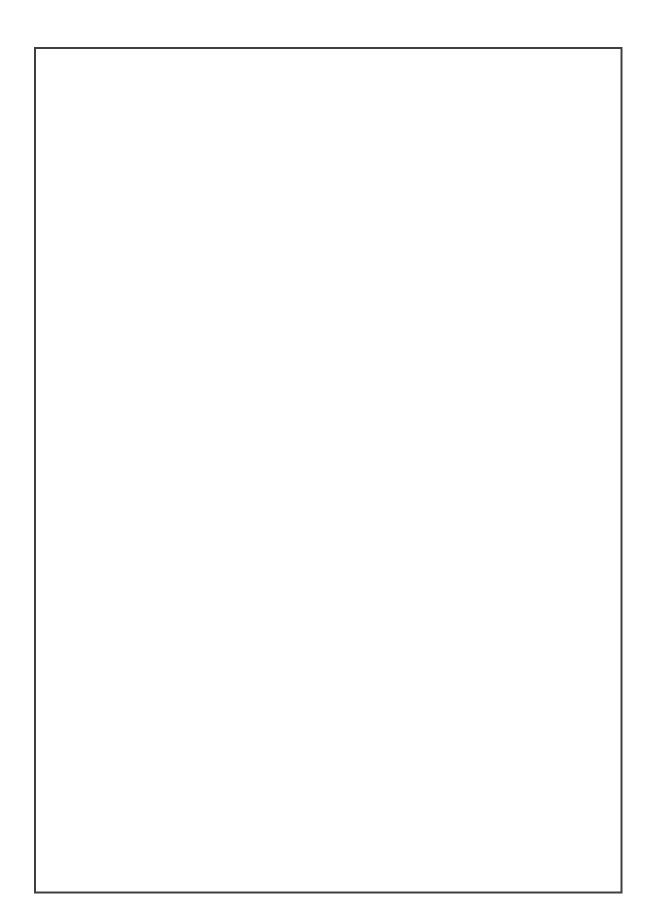
Additionally we suppose that the keys are equiprobable, and that the plaintexts appear with the following probabilities:

$$p(m_1) = \frac{1}{2}, \quad p(m_2) = \frac{3}{20}, \quad p(m_3) = \frac{7}{20}.$$

Compute the following entropies, justify your computations when necessary and simplify all the expressions as much as possible :

- 1. H(P)
- 2. H(K)
- H(C)
- 4. H(P|C)





Question 1.3 What do you think of this cryptosystem? Do you think it is secure? Give one concrete example/justification.

Exercise 2 Arithmetic

Question 2.1				
Let $a=247338$ and $b=139776$. Using Euclid's Algorithm, compute $\gcd(a,b)$.				

\sim		\sim	\sim
(Ji	uestion	2	2

Let $(F_n)_{n\geq 0}$ be the Fibonacci sequence, starting from $F_0=0$ and $F_1=1$ and recursively defined by $F_{n+2}=F_n+F_{n+1}$ for $n\geq 0$.

Question 2.2a	Prove that $gcd(F_n, F_{n-1}) = 1$ for all $n \ge 1$.

Question 2.2b	Prove that $F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$ for all $n, m \ge 0$.

Question 2.2c	Let $m, n \geq 1$. Prove that if m divides n , then F_m divides F_n .

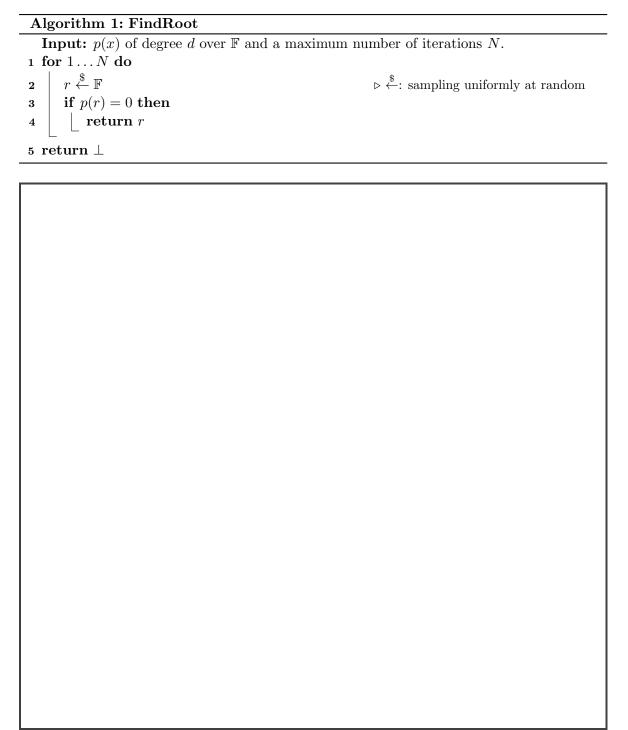
Question 2.2d Prove that $gcd(F_m, F_n) = F_{gcd(m,n)}$ for all $n, m \ge 1$.					
Hint: Show that simultaneously.					r subscripts
I					

Question 2.2e	Let $m, n \geq 1$. Deduce that if F_m divides F_n , then m divides n .

Exercise 3 Algorithms

Question 3.1 Random root finding

Given a polynomial p of degree d (i.e. deg(p) = d) defined over a finite field \mathbb{F} and a maximum number of iterations N. Algorithm 1 tries to find a root of this polynomial. Compute the expected number of iterations of this algorithm.



Question 3.2 Asymptotic Notation
Definition 1 $(O(.))$. Assume that $f(n)$ and $g(n)$ are two functions. We write $f(n) = O(g(n))$ if and only if there exist constants $N > 0$ and $C > 0$ such that for all $n \ge N$, $ f(n) \le C g(n) $
Definition 2 $(\Omega(.))$. Assume that $f(n)$ and $g(n)$ are two functions. We write $f(n) = \Omega(g(n))$ if and only if there exist constants $N > 0$ and $C > 0$ such that for all $n \ge N$, $ f(n) \ge C g(n) $
Definition 3 $(o(.))$. Assume that $f(n)$ and $g(n)$ are two functions. We write $f(n) = o(g(n))$ if and only if for all $C > 0$ there exists a constant $N > 0$ such that for all $n \ge N$, $ f(n) < C g(n) $
Definition 4 $(\omega(.))$. Assume that $f(n)$ and $g(n)$ are two functions. We write $f(n) = \omega(g(n))$ if and only if for all $C > 0$ there exists a constant $N > 0$ such that for all $n \ge N$, $ f(n) > C g(n) $
Question 3.2a Show that $3n^3 - 5n + 16 = \Omega(n^3)$.

Question 3.2b $g(n) = \Omega(f(n))$.	Let $f(n)$ and g	(n) be positive for	unctions. Show t	that $f(n) = O(g(n))$)) implies

2. $f = \Omega(g)$	
3. f = o(g)	
$4. \ g = \omega(f)$	

If $f(n) = n^2 \log(n)$ and $g(n) = n^3$. Which of the following statements are

Question 3.2c true? List all.

1. f = O(g)

THIS PACE INTERVITOR ALLEY LETTERS PACE INTERVITOR AND A STATE OF THE PACE OF