Università di Padova - Scuola di Scienze
Esame di Cybersecurity and Cryptography

Lauree Cybersec-Mat-Algant-Inf-Ict-IngInf January 21st, 2022 (primo appello, a.a. 2021-2022)

Name: _____

ID number: _____ Master: _____

PER LA COMMISSIONE D'ESAME

1E	2E	3E	Totale
10	10	10	30

Written exam

Question 1. Describe the general settings of the AES cryptosystem. Then describe its enciphering function (pseudocode, state, functions S, SR, MC, E). Explain how the AES-deciphering function works.
(**Italian**: Si descrivano le caratteristiche generali del crittosistema AES. Si descriva poi la sua funzione di cifratura (pseudocodice, stato, funzioni S, SR, MC, E). Si spieghi poi come funziona la funzione di decifratura di AES.

Question 2. Describe the algorithm and estimate the computational complexity of the Pollard ρ factoring method (Floyd iteration included).
(**Italian:** Si descriva l'algoritmo di fattorizzazione ρ di Pollard e si calcoli la sua complessità computazionale (variante di Floyd inclusa).)

Question 3. (3.a) Describe the general scheme of the DES deciphering function.
(**Italian:** Si descriva lo schema generale della funzione di decifratura del DES.)

(3.b) Prove that any affine block cipher can be attacked with a "known-plaintext" strategy.
(**Italian**: Si dimostri che un cifrario a pacchetto affine può essere violato con una attacco di tipo "known-plaintext".)

Total time: 120 minutes

