November 15, 2022, Midterm 1, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Describe the Merkle-Damgard Iterative construction for a Hash function, highlighting the required properties for the basic component(s)

Q2: What are the main properties that differentiate a cryptographically secure PRNG from a between classical PRNG

Q3 (on encryption vs integrity): A plaintext encrypted with a stream cipher carries, as fourth plaintext byte, the port number 80 (in hex: 0x50). The attacker wants to turn this port number into port 25 (hex: 0x19). The attacker sees the following ciphertext (hex notation, 4th byte being underlined):

CT = A3 B2 CC **77** 9A

How should the attacker modify the above message to perform such port number change?

Q4 (on TOTP): An attacker has physical access, for an entire day, to a Smart Phone of a Tor Vergata professor. The smart phone has a "signature app" installed, which implements a TOTP used to generate secure codes for the registration of exam grades. The attacker further knows the Professor's password of Delphi (the system where exams are recorded), and knows the future day in which the registration will take place.

1. Can the attacker change his grade? If yes, then how, specifically? (note: the secret key used to generate the TOTP is not accessible)

2. Would HOTP improve security of the exam registration process, or would further reduce security, or would it make no difference?

Q5 (**On Linear Congruential Generators**): Define the main equation for a Linear Congruential Generator, and discuss, without describing all the necessary mathematical details, what is the general strategy for attacking an LCG in a scenario where we don't know any of the parameter. Then, suppose the following numbers were generated through an LCG with parameters c=444447 (module) and a=1337 (multiplier):

9823, 244430, 134407

Is it possible to discover the value of the additive parameter b? How would you do it? What if instead we only had the first number?