8 March 2022 – Computer & Network Security – PART 1

NAME:_____ SURNAME:_____ MATRICOLA CODE:_____

Q1 – A connectionless data transfer protocol uses nonces to prevent replay attacks: describe pros and cons of different types of nonces

Q2 – The password of a 50 years old person, is CccDDMMYY where Ccc are the first three letters (first letter = capital) of the name of the daughter, and DDMMYY is the date of birth of the daughter. What's the entropy of this password?

Q3 – Assume a random generation of 4 digit codes DDDD:

1) how many codes are approximately required to have a 50% collision probability?
2) and what's the collision probability when 30 codes are generated?

Q4 – Explain how the Anonymity Key in UMTS AKA is used to protect location privacy.

8 March 2022 – Computer & Network Security – PART 2

NAME:_____ SURNAME:_____ MATRICOLA CODE:_____

Q1: Using the Extended Euclidean Algorithm compute the modular inverse 11^{-1} mod 113

Q2: What is Forward Secrecy (FS)? Why RSA Key Transport does NOT provide FS? And how TLS1.3 guarantees FS?

Q3: An authentication request is of type:

USERNAME=Giuseppe; PASSWD=xxxx00\n

Where xxxx=CIRO or xxxx=MARA.

This request is then compressed, encrypted and then sent to a server. The attacker is now able to perform a single plaintext injection attack prior to compression (CRIME attack). Which string can the attacker inject to determine the password of Giuseppe?

Q4: Describe the truncation attack and the Close-Notify defense in TLS

8 March 2022 – Computer & Network Security – PART 3

NAME:_____ SURNAME:_____ MATRICOLA CODE:_____

Q1: Show, via either theory as well as a numerical example, a (2,3) Threshold El Gamal decryption. For the numerical example, use for the modulòar exponentiations the prime value p=59 and invent any other parameter (at your complete choice, as long as they are consistent with p).

Q2: Compute all the points of the Elliptic curve $y^2 = x^3 + x$ defined over the modular integer field Z_7.

Q3: Show how an adversary may compute the private key if you reuse the same nonce in an ECDSA signature.

Q4. Assume arithmetic modulus 101. A Linear secret sharing scheme involving 3 parties is described by the following access control matrix:

A:	1	1	0
B:	0	1	-1
C:	1	1	1

Assume that the following shares are revealed: A→11, B→22, C→33. What is the hidden secret?