Computer & Network Security, 9CFUs – prof. Giuseppe Bianchi – 3rd midterm exam, 2 Feb 2022

Surname_____________________Name:_________________ Univ. Code:_________________

Q1 Describe the Joux's three-party Diffie-Hellman protocol

Q2 What is the (min) order of the following multiplicative groups defined by the chosen parameters p and g:
[hint: 593, 1187, 3559 primes, with 1187 = 2 x 593 + 1 and 3559=593 x 2 x 3+1 → with the exception of (2), no need to do any modular exponentiation! – NOTE: EXPLAIN YOUR ANSWER otherwise answer is not valid]

1) g^x mod p, with g=1186, p=1187

2) g^x mod p, with g=7, p=1187

3) g^x mod p, with g=9, p=1187

4) g^x mod p, with g=64, p=3599

Surname____________________Name:________________ Univ. Code:________________

Q3 Describe the Pedersen Verifiable Secret sharing

Q4 Being e: GxG→Gt a bilinear map, and g a generator of G, simplify the expression:

$e(g^a g^b, g^c g^d) / e(g^{ac}, g^{bd})$

Computer & Network Security, 9CFUs – prof. Giuseppe Bianchi – 3rd midterm exam, 2 Feb 2022

Surname_____________________Name:_________________ Univ. Code:_________________

E1. Consider the Elliptic curve $y^2 = x^3 - 2x - 3$ defined over the modular integer field Z_5.

A. find all the points $EC(Z_5)$ and state what is the order of the corresponding group

$$P = (x_1, y_1)$$
$$Q = (x_2, y_2)$$
$$R = P + Q = (x_3, y_3)$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

B. Compute [4](1,1)

[HELP: possibly useful mnemonic hints reported here on the right;
MUST-DO: show step-by-step detailed computations; try to minimize the number of EC additions]

Surname_____________________Name:_________________ Univ. Code:_________________

E2 – Secret Sharing and Threshold RSA. A group of four parties forms a (3,4) secret sharing scheme. Using ordinary arithmetic (no moduli) parties P_i={1,2,3,4} are dealt with shares σ_i of a key SK, which is the private key of an RSA scheme with modulus n=91 and public key PK=5.

A. Using shares σ_1=34, σ_2=41, σ_4=61, reconstruct the secret key SK and verify that it is the correct one for the considered RSA public key PK;

B. If the attacker only knows shares σ_1 and σ_4, and does not yet know share σ_2, what's his/her advantage in terms of chances to guess the secret key versus a pure random guess? *[ignore here the further info that SK is an RSA secret key]*

C. Using the Shoup construction, show step by step how the three parties P1, P2 and P4 can distributely compute a threshold RSA signature for the message m=15, and verify that the result is correct by directly computing the signature using the SK value computed before.
[NOTE: if you prefer, to simplify computation instead of using the full L! you can use the minimum value that permits to make all lambda coefficients integer] [HINT: 15^{-1} mod 91 =85]