Computer & Network Security – prof. Giuseppe Bianchi – 3rd midterm, February 2, 2023

Name+Surname:______________________________________ Univ. Code:__________________

Q1. Determine whether the following statements are true or false or Not-applicable/meaningless (i.e. the sentence is badly formulated or refers to something impossible/wrong).

In ECDSA, for providing IND-CPA (semantic) security, the nonce used must be always fresh	V	F	N/A
In ECIES, for providing IND-CPA (semantic) security, the nonce used must be always fresh	V	F	N/A
In El Gamal, for providing IND-CPA security, the nonce used must be always fresh	V	F	N/A
ECDSA security relies on the hardness of the factorization problem over elliptic curves	V	F	N/A
The order of an elliptic curve group built on Zp with p prime is either p or a multiple of p	V	F	N/A
In a (4,4) secret sharing scheme using arithmetic modulo n, n must be a prime number	V	F	N/A
The Shamir secret sharing is unconditionally secure	V	F	N/A
A verifiable secret sharing using the Pedersen Commitment is unconditionally secure	V	F	N/A
The Pedersen Commitment is perfectly hiding	V	F	N/A
Unlike Shamir, a trivial secret sharing scheme cannot be ideal	V	F	N/A

Q2. Part 1: Describe the Boneh-Franklin's Identity Based Encryption scheme

Part 2: Show how the user private key can be computed via a PKG system distributed among two parties so that neither party is able, alone, to know the users' private keys.

Name+Surname:_______________________________________ Univ. Code:__________________

Q3. Let P be an EC point. What is the minimum number of EC sums/doubles necessary to compute [193]P?

193 in binary is: 1100.0001
Then, 7 doubles and 2 additions = 8.

Q4 Assume arithmetic modulus 100. A Linear secret sharing scheme involving 4 parties is described by the following access control matrix:

A:	1	1	0	0
B:	0	1	1	0
C:	0	0	1	1
D:	0	0	0	1

Assume that the following shares are revealed: A → 15, B → 27, C → 33, D→41
What is the secret?

A-B+C-D = 80.

Q5. Consider the Elliptic curve EC(Z_7): $y^2 = x^3 + x$ defined over the modular integer field Z_7.

A. Verify that (0,0) is a point of the curve, and (*without any computation*) determine (0,0)+(0,0).

B. find all the remaining points of the curve.

(0,0) + (0,0) = 0 (y=0 implies that the "intercept" is at infinity, hence no need to do any computation of course – besides, computation would anyway give 0/0…)
[COMMON MISTAKE: 0 is NOT (0,0) → (0,0) is a "normal" point in the curve… the point at infinitiy is a supplementary one!]

All points: (0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5), <u>and</u> 0

Name+Surname:_________________________________ Univ. Code:_______________

Q6. A Shamir Secret Sharing scheme uses a non-prime modulus p=35 (if you need modular inverses see table on the right). Of the 5 participating parties $P_1,\ldots,P_5$, with respective x coordinates $x_i = \{1,2,3,4,5\}$, parties P1, P2 and P4 aim at reconstructing the secret.

a) compute the Lagrange Interpolation coefficients for parties 1, 2, 4.

b) Reconstruct the secret, assuming that the shares are:

P1 → 33
P2 → 4
P4 → 21

c) Does the knowledge of the two shares P1 and P2 leak information about the secret?

x	1/x mod 35
1	1
2	18
3	12
4	9
6	6
8	22
9	4
11	16
12	3
13	27
16	11
17	33
18	2
19	24
22	8
23	32
24	19
26	31
27	13
29	29
31	26
32	23
33	17
34	34

a) Lambda 1/2/4 = {26,33,12}

b) secret = 17

c) Unlike what we could expect, in this SPECIFIC CASE we are still ok! Indeed, if share 4 is not known (call it D), then the secret is given by the expression

$$S = 33 \times 26 + 4 \times 33 + D \times 12 \mod 35 = 10 + 12\,D \mod 35$$

But since 12 is (luckily) still coprime with 35, for any value of D in the range (0,34) we have a different value of S!

(you can also see this via brute force:

Mod[10+12 Range[0,34] →

{10,22,34,11,23,0,12,24,1,13,25,2,14,26,3,15,27,4,16,28,5,17,29,6,18,30,7,19,31,8,20,32,9,21,33}

Computer & Network Security – prof. Giuseppe Bianchi – 3rd midterm, February 2, 2023

Name+Surname:______________________________________ Univ. Code:_________________

Q7 An RSA system has the following parameters: modulo n=253, public key e=3. Assume we are NOT able neither to factorize n nor gather or compute the corresponding private key d. Despite this, we wish to compute the RSA signature 19^d mod n for message m=19.

1) Show how this is possible if we know that $19^{5d} = 10$ mod n, and
2) numerically compute the signature.

[here a few modular inverses with might (might not) be useful: $\{3, 5, 10, 19, 100\}^{-1}$ mod n → {169,152,76,40,210}]

Remember Shoup's lecture and just apply Common modulus attack using (all what follows is mod n)

$M_1 \rightarrow 19^{5d} = 10$

$M_2 \rightarrow 19^{ed} = 19^{3d} = 19$

Since ExtendedGCD[5,3] = {-1,2} we just need to compute

$19^d = M_1^{-1} \times M_2^2 = 76 \times 108 = 112$

You can check that this is correct by explicitly computing the signature using d=147