Network Security – prof. Giuseppe Bianchi – 3rd term exam, 14 February 2020

Name+Surname:_____ Univ. Code:_____

Q1 Let P be an EC point. What is the minimum number of EC sums/doubles necessary to compute [259]P?

- **a)** 8
- **b)** 10
- **c)** 11
- **d)** 12
- **e)** 258
- **f)** 259

Q2 What is the main limitation of a trivial secret sharing scheme?

- **a)** Unlike the Shamir scheme, it is not ideal
- **b)** Unlike the Shamir scheme, it is not unconditionally secure but only computationally secure
- **c)** It permits only to implement (t,n) schemes with t strictly lower than n
- d) It permits only to implement (n,n) schemes and not (t,n) schemes with t<n

Q3 In the Boneh-Franklin's Identity Based Encryption scheme, what happens if an attacker compromises the PKG?

- **a)** Nothing, as there is no PKG in such scheme
- **b)** It becomes impossible to decrypt a previously encrypted data
- **c)** the attacker may find all private keys for all users
- d) the attacker may revoke all users' public keys

Q4 Three parties A, B, C setup a group (3,3) RSA signature, i.e. a message is correctly signed if all three parties contribute to the signature with their shares of the private key d. Being x and y random values (in the appropriate range), shares are:

Share_A = d-x-y
Share_B = x
Share_C = y

Assuming that a message M needs to be signed, schematically describe the specific modular operations and exchange of messages that such a (3,3) RSA signature requires.

Name+Surname:_____ Univ. Code:_____

Q5 What may happen if Alice digitally signs two different messages M1 and M2,with ECDSA using the same nonce r (r = x-coordinate(kP) mod n)?

- ○ **a)** The attacker can compute Alice's Private key
- ○ **b)** The attacker can forge a signature for any linear combination of M1 and M2
- ○ **c)** The attacker can decrypt both M1 and M2
- ○ **d)** The attacker can perform an expansion attack on one of the two messages

Q6 Assume arithmetic modulus 100. A Linear secret sharing scheme involving 4 parties is described by the following access control matrix:

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

Assume that the following shares are revealed:

A → 36
B → 51
D → 18

What is the secret?

a) 3 **b)** 5 **c)** 31 **d)** 33 e) 67 **f)** 69 **g)** 95 **h)** 97 **i)** another result = _____

Q7 Describe the threshold El Gamal decryption, and specifically explain why the private key is never revealed in the reconstruction.

Name+Surname:_____ Univ. Code:_____

Q8 A same message M is RSA-encrypted using two different public keys e1 = 11 and e2 = 17, but same RSA modulus n=35. The two resulting ciphertexts are: c1=3 and c2=17. Decrypt the message applying the Common Modulus Attack (show the detailed computations required).
[Just in case you might need to rapidly compute inverses mod 35, see table associated to exercise Q10]

Q9 Consider the Elliptic curve $y^2 = x3 + 2x - 1$ defined over the modular integer field Z_5. A) find all the points $EC(Z_5)$ and B) specify what is the order of the corresponding group

Network Security – prof. Giuseppe Bianchi – 3rd term exam, 14 February 2020

Name+Surname:_____ Univ. Code:_____

Q10 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 P5 aim at reconstructing the secret.

a) compute the Lagrange Interpolation coefficients for parties 1,2,5;

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

P1 → 18
P2 → 24
P5 → 19

c) Prove that the system is NOT unconditionally secure, by showing that the knowledge of the two shares P1 and P5 leak information about the secret – specifically, after knowing shares P1 and P5 which would be the only possible remaining secret values?

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