Network Security – prof. Giuseppe Bianchi – 3rd term exam, 4 February 2021

Name+Surname:____ Univ. Code:__________________

Q1 Prove that a Pedersen Commitment is homomorphic

Q2 How is the private key SK of an user named "bob" constructed in the Boneh-Franklin's Identity Based Encryption scheme? (notation: s, g^s = PKG key pair, H() = hash function which maps a string into an EC point)

- ○ a) SK = g^H(bob)
- ○ b) SK = H(bob)^s
- ○ c) SK = bob^s
- ○ d) SK= g^s H(bob)

Q3 In ECDSA, the key pair (private key, public key) is…

- ○ a) A pair of EC points
- ○ b) A pair of modular integers
- ○ c) the private key is a modular integer whereas the public key is an EC point
- ○ d) the private key is an EC point whereas the public key is a modular integer

Q4 A Secret Sharing scheme is ideal if…

- ○ a) Each party receives exactly one share
- ○ b) The total number of participating parties n is equal to the minimum number of parties t which can reconstruct the secret
- ○ c) the size of each share is an integer value
- ○ d) none of the above answers

Q5 Describe the RSA common modulus attack

Q6 Determine the access control matrix that implements the policy: P = **A** AND **B** AND (**C** OR (**D** AND **E**))

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

(solution obviously not unique!)

Network Security – prof. Giuseppe Bianchi – 3rd term exam, 4 February 2021

Name+Surname:____ Univ. Code:__________________

E1 Consider the Elliptic curve $y^2 = x^3 + x + 1$ defined over the modular integer field Z_7.

A. find all the points $EC(Z_7)$

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

B. State what is the order of the corresponding group

C. Compute [3](2,2)
[HELP: possibly useful mnemonic hints reported here on the right; MUST-DO: show step-by-step detailed computations]

points: 0, (0,1), (0,6), (2,2), (2,5)
order: 5
[3](2,2) = (0,6) → should be computed as follows:
(2,2) + (2,2) = (0,1)
(2,2) + (0,1) = (0,6)

Name+Surname:____ Univ. Code:__________________

E2 Assume arithmetic modulus 101. A Linear secret sharing scheme involving 4 parties is described by the following access control matrix:

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

A. Assume that the following shares are revealed:

A → 23
B → 88
C → 57

What is the secret? (explain how you arrived to the result, otherwise the answer is not considered valid)

93 = 23-88+57

B. *[optional, extra]* Assume that the following shares are revealed:

A → 79
B → 20
D → 7

What is the secret? (explain how you arrived to the result, otherwise the answer is not considered valid)

Per ricostruire il vettore (1,0,0) è necessario fare la seguente operazione:
A-(B+D)/2 ma attenzione che l'aritmetica è modulare!! Pertanto ½ = 51 mod 101 e quindi
Segreto = 79-27 x 51 mod 101=15

Network Security – prof. Giuseppe Bianchi – 3rd term exam, 4 February 2021

Name+Surname:____ Univ. Code:__________________

E3 – part 1 – El Gamal Encryption, g=29, p=83:

1. Reviewed El Gamal encryption

Ciphertext = {g^r, m h^r}

2. Assume operations are modulo p=83: is g=29 a generator of the Z^*_{83} multiplicative group? [you must respond to this question by performing a single "test"! Trying all possible values in the range is not considered a valid answer]

It suffices to compute g^(p-1)/2, since 29^41 mod 83 = 1, g is NOT a generator.

3. Using g=29 and p=83, encrypt message M=37 for an user whose private key is sk=7 and whose public key is pk=4 – if you need an ephemeral value, use r=13.

Ciphertext = {g^r, m pk^r} → using r=13, pk=4, M=37 → ciphertext = {12,51}

E3 – part 2 – Threshold El Gamal Decryption.

If you have not solved the previous part, solve the exercise by usig as ciphertext the pair {41,25} *[note: on purpose different from the solution of the previous exercise!]*

The ciphertext produced at the end of the previous part is now sent for threshold description to a (2,3) group. The group has been built by sharing the secret key via a (2,3) Shamir Secret Sharing scheme, prime modulus 41.

The three participating parties P_1, P_2, P_3, use standard x-coordinates x_i = {1,2,3}.

The message is received by parties P1 and P3 which have, shares σ_1=26 and σ_3=23, respectively

- compute the Lagrange interpolation coefficients for parties 1 and 3;

q=41; x1=1; x3=3;
lambda1 = Mod [-x3 * PowerMod[x1-x3,-1,q],q] = 22
lambda3 = Mod [-x1* PowerMod[x3-x1,-1,q],q] = 20

- Assuming that P1 and P3 directly exchange their shares, reconstruct the original secret key

s1=26; s3=23;
Mod[s1*lambda1+s3*lambda3,q] = 22x26+20x23 mod 41 = 7

- Assuming, instead, that P1 and P3 do NOT explicitly exchange their shares: show how P1 and P3 can still cooperate to decrypt the previous El Gamal encrypted message (and numerically compute the result, showing the step-by-step operations).

start from {g^r, m*h^r} = {12,51}.
P1 computes 12^s1^lambda1 mod 83 = 49;
P3 computes 12^s2^lambda2 mod 83 = 28;
Now multiply the two terms and compute the modular inverse → (49*28)^(-1) = 17
And decrypt the message as 17*51 mod 83 = 37

Name+Surname:______________________________________ Univ. Code:__________________