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)

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

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 $\sigma_1=26$ and $\sigma_3=23$, 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

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

Name+Surname:_____ Univ. Code:_____

esame 4 feb. 2021

Q1) DIMOSTRA CHE PEDERSEN E' HOMOMORPHIC

SVOLGIMENTO

homo: sum of shares = share of the sum

$$comm(a+b, r+s) = g^{a+b} h^{r+s} = g^a \cdot g^b \cdot h^r \cdot h^s$$

$$= g^a \cdot h^r \cdot g^b \cdot h^s = comm(a,r) \cdot comm(b,s)$$

Q2) IN IBE, PubK = BOB, PrivK ?

SVOLGIMENTO

$S_K = h(Bob)^s$ cioè: $str_g \xrightarrow{h} EC\,pnt \rightarrow (EC\,pnt)^s = S_K$

Q3) ECDSA, $\langle S_K, P_K \rangle$ sono:

- $\langle [d], [d]P \rangle$ cioè (int, EC pnt)

Q4) SECRET SHARING SCHEME IDEALE SE:

- |share| = |secret| ✓
- ∀ party 1 share è SBAGLIATO, ermo vale per LSSS ✗

Q5) RSA COMMON MODULUS ATTACK:

SVOLGIMENTO

Alice: $M^{e_1} \bmod N = C_1$

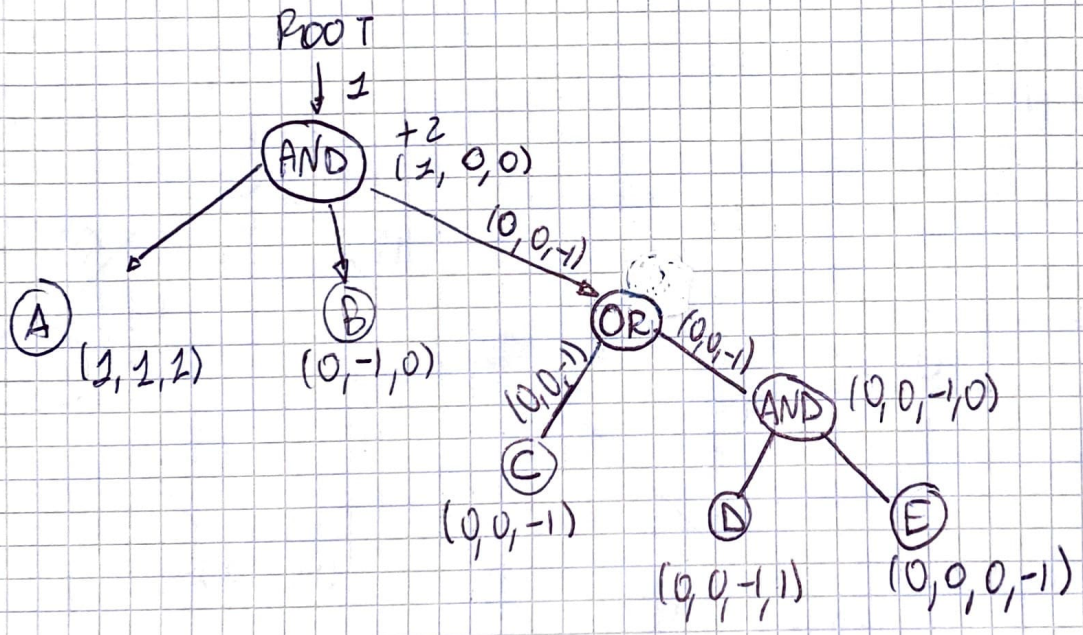
Bob: $M^{e_2} \bmod N = C_2$

, $\gcd(e_1, e_2) \rightarrow \exists\ r, s$:

$e_1 \cdot r + e_2 \cdot s \bmod \phi(N) \equiv 1 \rightsquigarrow C_1^{r} \cdot C_2^{s} = M^{e_1 \cdot r} \cdot M^{e_2 s} \bmod N$

$= M^{(e_1 \cdot r + e_2 \cdot s)} \bmod N = M^1 \bmod N = M \bmod N$

Q6) 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

E1) $y^2 \bmod 7 = x^3 + x + 1 \bmod 7$

• A) PUNTI $\in EC(Z_7)$

PROVO $(0,1) \rightarrow x^3 + x + 1 \big|_{x=0} = 1$, $\exists\ y : y^2 = 1$? SI, $y = 1$

$P = (0,1) \in EC(Z_7)$

▸ $2P = (0,1) + (0,1)$ $\quad P = Q$

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{1}{2} \bmod 7 = 4 = \lambda$$

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

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$x_3 = (16 - 0 - 0) \bmod 7 = 2$

$y_3 = 4(0 - 2) - 1 = -9 \bmod 7 = 5$

$2P = (2,5) \in EC(Z_7)$

▸ $3P = (2,5) + (0,1)$ $\quad P \neq Q$

$\lambda = \frac{1 - 5}{0 - 2} = \frac{4}{2} \bmod 7 = 4 \cdot 4 \bmod 7 = 2$

$x_3 = (2)^2 - 2 - 0 = 2$ $\qquad y_3 = 2(2 - 2) - 5 = -5 \bmod 7 = 2$

$3P = (2,2) \in EC(Z_7)$

▸ $4P = 3P + (0,1) = (2,2) + (0,1)$

$\lambda = \frac{1 - 2}{0 - 2} = \frac{1}{2} \bmod 7 = 4$

$x_3 = (4)^2 - 2 - 0 = 14 \bmod 7 = 0$; $y_3 = 4(2 - 0) - 2 = 6$

$4P = (0,6) \in EC(Z_7)$ $\rightsquigarrow$ $5P = (0,6) + (0,1) \rightsquigarrow \nexists$

$EC(Z_7) = \{ \mathcal{O}, (0,1), (2,5), (2,2), (0,6) \}$ $\quad |EC(Z_7)| = 5$

E2)

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

mod 101

$Y_A = 23$

$Y_B = 88$

$Y_C = 57$

A) trova segreto

SVOLGIMENTO

Lavoro con A, B, C

$c_1(1\ 1\ 0) + c_2(0\ 1\ -1) + c_3(0, 0, -1) = (1, 0, 0)$

$c_1 = 1 \quad c_2 = -1 \quad c_3 = 1$

$\rightarrow S = 23 - 88 + 57 \bmod 101 = 93$

info Hi $\{c_1(1\ 1\ 0) + \dots\} \begin{pmatrix} S \\ r_1 \\ r_2 \end{pmatrix} = (1\ 0\ 0) \begin{pmatrix} S \\ r_1 \\ r_2 \end{pmatrix} = S$ cioè

$c_1 \cdot Y_1 + c_2 \cdot Y_2 + c_3 \cdot Y_3 = S$ $\left(NB: c_1(1\ 1\ 0) \cdot \begin{pmatrix} S \\ r_1 \\ r_2 \end{pmatrix} = c_1 \cdot Y_1\right)$

B) $Y_A = 79 \quad Y_B = 20 \quad Y_D = 7$

$c_1(1\ 1\ 0) + c_2(0\ 1\ -1) + c_3(0\ 1\ 1) = (1\ 0\ 0)$

$c_1 = 1 \quad c_2 = -\frac{1}{2} \bmod 101 = -51 = c_3$

$S = [1(79) - 51(20 + 7)] \bmod 101 = 15 = 1$

E3) EL GAMAL, $g = 29$, $p = 83$

2) $g = 29$ è generator di $\mathbb{Z}_{83}^*$? USARE UN SOLO TEST

SVOLGIMENTO

se $g^{q = \frac{p-1}{2}} \bmod p \equiv 1 \rightsquigarrow g \in QR \rightarrow$ genera subgroup di cardinalità PRIME $\rightsquigarrow$ NON è generator.

$29^{41} \bmod 83 = 1$?

$29^{32+8+1} \bmod 83 = 1$?

$29^1 \bmod 83 = \underline{29} \rightarrow 29^2 \bmod 83 = 11 \rightarrow 29^4 \bmod 83 = (11 \cdot 11) \bmod 83 = 38$

$29^8 \bmod 83 = (38 \cdot 38) \bmod 83 = \underline{33} \rightarrow 29^{16} \bmod 83 = (33 \cdot 33) \bmod 83 = 10$

$\rightarrow 29^{32} \bmod 83 = (10 \cdot 10) \bmod 83 = \underline{17}$

$\Rightarrow 29^{41} \bmod 83 = (29 \cdot 33 \cdot 17) \bmod 83 = (16269) \bmod 83 = 1$

$g = 29 \in QR \rightarrow$ NO gen.

3) $g = 29$, $p = 83$, $M = 37$, $SK = 7$, $PK = \underset{11}{g^s} = 4$, $r = 13$. ENC M

Per El Gamal ho $ENC(g^r, m \cdot h^r)$

$g^r = 29^{13} \bmod 83 = 29^{(8+4+1)} \bmod 83 = (33 \cdot 38 \cdot 29) \bmod 83$

$= (36366) \bmod 83 = 12 = g^r$

$(m \cdot \underset{(g^s)^r}{h^r}) = (37 \cdot 4^{13}) \bmod 83 = 51$ (Calcolo come prima!)

E3 parte 2)

$C_T = \{12, 51\}$, threshold decrypt $(t, n) = (2, 3)$, $P = 41$

$P_1 = (1, 26)$ $P_2 = (2, ?)$ $P_3 = (3, 23)$

- λ_1 e λ_3? i opero con loro 2)

$$\lambda_1 = \frac{-3}{1-3} = +\frac{3}{2} \bmod 41 = 3 \cdot 21 \bmod 41 = 63 \bmod 41 = 22$$

$$\lambda_3 = \frac{-1}{3-1} = -\frac{1}{2} \bmod 41 = -1 \cdot 21 \bmod 41 = 20 \bmod 41 = 20$$

- $S = \lambda_1 \cdot y_1 + \lambda_3 \cdot y_3 = (22 \cdot 26 + 20 \cdot 23) \bmod 41 = 7 = S$

- P_1 e P_3 non cooperano esplicitamente, come possono decriptare EL gamal (12, 51) dell'ex. precedente?

SVOLGIMENTO

$g^r = 12$, $m \cdot h^r = 51 = m \cdot (g^s)^r$

$P_1 : (g^r)^{\lambda_1 y_1} = (12)^{26 \cdot 22} \bmod 83 = 12^{572} \bmod 83$

$= 12^{512+32+16+8+4} \bmod 83$, trovo:

$12^2 \bmod 83 = 61$

$12^4 \bmod 83 = (61 \cdot 61) \bmod 83 = 69$

$12^8 \bmod 83 = 30$

$12^{16} \bmod 83 = 70$

$12^{32} \bmod 83 = 3$

$12^{64} \bmod 83 = 9$

$12^{128} \bmod 83 = 2$

$12^{256} \bmod 83 = 2$

$12^{512} \bmod 83 = 16$

$\rightarrow 12^{572} \bmod 83 = (69 \cdot 30 \cdot 70 \cdot 3 \cdot 16) \bmod 83 = 49$

analogamente $12^{\lambda_3 \cdot y_3} \bmod 83 = 28$

allora $m = \dfrac{m \cdot g^{sr}}{(g^{r})^{\lambda}}$

$(g^{r})^{\lambda} = (49 \cdot 28) \bmod 83 = 44$, voglio l'inverso!

$44^{-1} \bmod 83 = ?$ uso ext. eucl. Alg

EQUAZIONE: $83 \cdot a + 44 \cdot b = 1$

a	b	vol	r
1	0	83	
0	1	44	1
1	-1	39	1
-1	2	5	7
8	-15	4	1
-9	17	1	

$44 \cdot 17 \bmod 83 = 1$

CONCLUSIONE

$m = \dfrac{(m \cdot g^{sr})}{(g^{r})^{\lambda}} = 51 \cdot 17 \bmod 83 = 37 = M$ ✓