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]

Answer: by the extended GCD(17,11) → {r,s}={2,-3}

Hence

$M = 3^{-3} \times 17^{2} \bmod 35 = 12^{3} \times 17^{2} \bmod 35 = 12$

Q9 Consider the Elliptic curve $y^2 = x^3 + 2x - 1$ 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

O, {0,2}, {0,3}, {2,1},{2,4},{4,1},{4,4}

Order 7

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

[Answer: Secret = 14;
set of possible secrets: the 7 possible values which satisfy 19+10x mod 35 →
➔ {4, 9, 14, 19, 24, 29, 34}

esame 14 feb. 2020

Q1) $[259]P$, quante sum/doubles eseguo?

$259_{10} = 256 + 2 + 1 = 100000011_2$. Ho 9 bit e 3 '1'.

Eseguo $(9-1)$ double + $(3-1)$ sum $= 8 + 2 = 10$

Q2) LIMITAZIONE del TRIVIAL secret sharing scheme?

- implemento SOLO schemi (n,n), non (t,n) con $t<n$

Q3) in IBE, COSA SUCCEDE SE COMPROMETTO PKG?

- può trovare tutte le S_K degli utenti, poiché è PKG che le dà!

Q4) RSA signature, share $A = d-x-y$, share $B = x$, share $C = y$ devo fare sign di M, come procedo?

$$[H(m)]^{S_A} \cdot [H(m)]^{S_B} \cdot [H(m)]^{S_C} = [H(m)]^{d-x-y+x+y} = [H(m)]^{d}$$

Q5) COSA SUCCEDE se Alice fa $\begin{cases} s_1 = \dfrac{H(m_1)+dr}{k} \\ s_2 = \dfrac{H(m_2)+dr}{k} \end{cases}$?

- Possibile per un attaccante computare $S_K = d$

Q6) mod 100

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

$Y_A = 36$ $\quad Y_B = 51$ $\quad Y_D = 18$

$S = ?$

SVOLGIMENTO

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

$c_1 = 1 \quad c_2 = -1 \quad c_3 = -1$, cioè:

$$c_1(1\,1\,1)\begin{pmatrix} s \\ r_1 \\ r_2 \end{pmatrix} + c_2(0\,1\,0)\begin{pmatrix} s \\ r_1 \\ r_2 \end{pmatrix} + c_3(0\,0\,1)\begin{pmatrix} s \\ r_1 \\ r_2 \end{pmatrix} =$$

$c_1(Y_A) + c_2(Y_B) + c_3(Y_D) = S$

$(36 - 51 + 18) \bmod 100 = 3$

Q8) RSA: $e_1 = 11$, $e_2 = 17$, $N = 35$, $C_1 = 3$, $C_2 = 17$.

DECRIPTA CON COMMON MODULUS ATTACK.

SVOLGIMENTO

$$\begin{cases} M^{11} \bmod 35 = C_1 = 3 \\ M^{17} \bmod 35 = C_2 = 17 \end{cases} \rightsquigarrow \exists\, r, s : e_1 \cdot r + e_2 \cdot s \bmod \phi(N) = 1$$

applico Ext. Euc. Alg.

a	b	val	r
1	0	17	
0	1	11	1
1	-1	6	1
-1	2	5	1
2	-3	1	

$C_1^{-3} \cdot C_2^{2} \bmod 35 =$

$3^{-3} \cdot 17^2 \bmod 35 =$

$(12)^3 \cdot 17^2 \bmod 35 = \underline{12} = M$

INVERSO

Q10) $p = 35$ $(3,5)$ scheme

$P_1(1,18)$ $P_2(2,24)$ $P_5(5,19)$

a) $\lambda_1, \lambda_2, \lambda_5$

$\lambda_1 = \left(\frac{-2}{1-2} \cdot \frac{-5}{1-5}\right) \bmod 35 = \frac{10}{-1(-4)} = 10 \cdot 4^{-1} \bmod 35 = 90 \bmod 35 = 20$

$\lambda_2 = \frac{-1}{2-1} \cdot \frac{-5}{2-5} \bmod 35 = \frac{5}{-3} = -5 \cdot 12 \bmod 35 = 10 \bmod 35 = 10$

$\lambda_5 = \left(\frac{-1}{5-1} \cdot \frac{-2}{5-2}\right) \bmod 35 = \frac{2}{4 \cdot 3} \bmod 35 = 2 \cdot 3 \bmod 35 = 6$

b) $s = \sum_{1,2,5} y_i \cdot \lambda_i = (20 \cdot 18 + 10 \cdot 24 + 6 \cdot 19) \bmod 35 = 14$

c) PROVA che NON è UNCONDITIONALLY SECURE, con P_1 e P_5 (share)

$\begin{cases} \lambda_1 = 20 \\ y_1 = 18 \end{cases}$ $\begin{cases} \lambda_2 = 10 \\ y_2 = ? = X \end{cases}$ $\begin{cases} \lambda_5 = 6 \\ y_5 = 19 \end{cases}$

$s = (20 \cdot 18 + 10X + 6 \cdot 19) \bmod 35 = 19 + 10D$, sostituisco

$D = 0 \rightarrow s = 19$ / $D = 1 \rightarrow s = 29$ / ... / $D = 3 \rightarrow s = 14$ / ... / $D = 7 \rightarrow s = 19$

Q9) $y^2 \bmod 5 = x^3 + 2x - 1 \bmod 5$

svolgimento

- $x=0 \rightsquigarrow x^3+2x-1 \Big|_{x=0} \bmod 5 = -1 \bmod 5 = 4 \bmod 5 = y^2 \to y=2$

$P = (0,2) \in E(Z_5)$, $\emptyset \in E(Z_5)$

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

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

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

- $2P = \overset{x_1\ y_1}{(0,2)} + \overset{x_2\ y_2}{(0,2)}$

$\lambda = \dfrac{0+2}{4} \bmod 5 = 2 \cdot 4 \bmod 5 = 3$

$x_3 = 9 - 0 - 0 \bmod 5 = 4$

$y_3 = 3(0-4) - 2 \bmod 5 = -14 \bmod 5 = 1 \to 2P = (4,1)$

- $3P = \overset{x_1\ y_1}{(4,1)} + \overset{x_2\ y_2}{(0,2)}$

$\lambda = \dfrac{2-1}{0-4} = +\dfrac{1}{-4} \bmod 5 = -4 \bmod 5 = 1$

$x_3 = 1 - 4 - 0 \bmod 5 = 2$, $y_3 = 1(4-2) - 1 \bmod 5 = 2$

$\hookrightarrow 3P = (2,1)$

- $4P = \overset{x_1\ y_1}{(2,1)} + \overset{x_2\ y_2}{(0,2)}$

$\lambda = \dfrac{2-1}{0-2} = \dfrac{-1}{2} \bmod 5 = -3 \bmod 5 = 2$

$x_3 = 4 - 2 - 0 = 2$ $y_3 = 2(2-2) - 1 \bmod 5 = 4 \to 4P = (2,4)$

- $5P = \overset{x_1\ y_1}{(2,4)} + \overset{x_2\ y_2}{(0,2)}$

$\lambda = \dfrac{2-4}{0-2} = \dfrac{-2}{-2} = 2 \cdot 3 \bmod 5 = 1$

$x_3 = 1 - 2 - 0 \bmod 5 = 4$ $y_3 = [1(2-4) - 4] \bmod 5 = 4 \to 5P = (4,4)$

- $6P = \overset{x_1\ y_1}{(4,4)} + \overset{x_2\ y_2}{(0,2)}$

$\lambda = \dfrac{2-4}{0-4} = \dfrac{+2}{+4} \bmod 5 = 3$, $x_3 = 0$, $y_3 = 3(4-0) - 4 \bmod 5 = 3 \to 6P = (0,3)$