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 operations necessary to compute [63]P? And more specifically which are these operations?

$63_{10} = 32+16+8+4+2+1 = 111111_2 \rightarrow$ 6 bit, 6 '1'

Computo allora 10 operazioni:

5 double (1 ∀ bit) e 5 sum (1 ∀ bit='1')

	double	result
1	P	P
1	2P	$\rightarrow$ 3P
1	4P	$\rightarrow$ 7P
1	8P	$\rightarrow$ 15P
1	16P	$\rightarrow$ 31P
1	32P	$\rightarrow$ 63P

Q2 - Consider both commitments introduced in our classes (Feldman and Pedersen), and assume they "commit" a value x. Under which (eventually different) assumptions they can be considered secure?

Feldman	Pedersen	
○	○	**a)** no specific assumptions
○	●	**b)** must use a large prime p in the modular exponentiations ($C_0 = g^s$ leak)
○	○	**c)** require that the committed value x is drawn from a large space
●	○	**d)** both large prime p and x drawn from large space

$\rightarrow 1 < x < p-1$ per perfect Bind,

$\rightarrow$ voglio x in ampio spazio $\rightarrow$ P ampio

Q3 - A strong prime p is defined as:

- ○ **a)** a prime number p much larger than usual
- ○ **b)** a prime p such as 2p+1 = q is also prime
- ⊠ **c)** a prime p such as p = 2q+1 and q is also prime
- ○ **d)** a prime p such as the Euler ϕ(p) is also prime

Q4 - Describe the Boneh-Franklin Identity Based Encryption scheme, specifying in particular, i) how a message is encrypted, ii) how a message is decrypted, and iii) what is the private key used by the receiver.

Name+Surname:____ Univ. Code:__________________

Q5 - Consider an RSA digital signature based on a (2,2) secret sharing, and assume all following operations are based on modulo n, with n being the RSA parameter. The tag $H(m)^d$ is reconstructed by:

- ○ **a)** Summing the tags constructed using the two shares
- ⊗ **b)** Multiplying the tags constructed using the two shares
- ○ **c)** Interpolating the tags constructed using the two shares using Lagrange coefficients
- ○ **d)** Using a special approach proposed by Shoup.

Q6 - Assume arithmetic modulus 100. A Linear secret sharing scheme involving 3 parties is described by the following access control matrix:

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

$1(1\,1\,0) - 1(0\,1\,1) - 1(0\,0\,{-1}) = (1\,0\,0)$ ✓

$[1(51) - 1(63) - 1(11)] \bmod 100 = 77 = S$

Assume that the following shares are revealed:

A → 51
B → 63
D → 11

What is the secret?

a) 1 **b)** 3 **c)** 23 **d)** 25 e) 75 ~~**f)**~~ 77 **g)** 97 **h)** 99 **i)** another result = __________

Q7 - A same message M is RSA-encrypted using two different public keys e1 = 5 and e2 = 7, but same RSA modulus n=143. The two resulting ciphertexts are: c1=23 and c2=4. Decrypt the message applying the Common Modulus Attack (show the detailed computations required).

Just in case you need to rapidly compute inverses modulus 143, here a few ones:
$x = \{4,5,7,17,20,23,29,92\} \rightarrow x^{-1} \bmod 143 = \{36,86,41,101,93,56,74,14\}$

$$\begin{cases} M^5 \bmod 143 = 23 \bmod 143 \\ M^7 \bmod 143 = 4 \bmod 143 \end{cases}$$

CMA:

find r, s $\quad 7 \cdot r + 5 \cdot s = 1$

a	b	val	r
1	0	7	
0	1	5	1
1	-1	2	2
-2	3	1	fine

$7(-2) + 5(3) = 1$

$23^3 \cdot 4^{-2} \bmod 143 =$

$23^3 \cdot 36^2 \bmod 143 = 108 = M$

Name+Surname:______________________________________ Univ. Code:__________________

Q8 - A Shamir Secret Sharing scheme uses a non-prime modulus p=55 (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 P_1, P_3 and P_5 aim at reconstructing the secret.

a) compute the Lagrange Interpolation coefficients for parties 1,3,5;

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

$P_1 \rightarrow 46$
$P_3 \rightarrow 51$
$P_5 \rightarrow 2$

c) Prove that the system is NOT unconditionally secure, by showing that the knowledge of the two shares P_3 and P_5 leak information about the secret – specifically, after knowing shares P_3 and P_5 which would be the only possible remaining secret values?

x	1/x mod 55
1	1
2	28
3	37
4	14
6	46
7	8
8	7
9	49
12	23
13	17
14	4
16	31
17	13
18	52
19	29
21	21
23	12
24	39
26	36
27	53
28	2
29	19
31	16
32	43
34	34
36	26
37	3
38	42
39	24
41	51
42	38
43	32
46	6
47	48
48	47
49	9
51	41
52	18
53	27
54	54

a) $\lambda_1 = \frac{-3}{1-3} \cdot \frac{-5}{1-5} = \frac{15}{-2\cdot(-4)} = \frac{15}{8} \bmod 55 = 15\cdot 7 \bmod 55 = 50$

$\lambda_3 = \frac{-1}{3-1} \cdot \frac{-5}{3-5} = \frac{5}{2(-2)} = -5\cdot 14 \bmod 55 = 40$

$\lambda_5 = \frac{-1}{5-1} \cdot \frac{-3}{5-3} = \frac{3}{4\cdot 2} = 3\cdot 7 \bmod 55 = 21$

b) $[50\cdot 46 + 40\cdot 51 + 21\cdot 2] \bmod 55 = 4382 \bmod 55 = 37 = S$

c) $[50\cdot X + 40\cdot 51 + 21\cdot 2] \bmod 55 = (47+50D) \bmod 55$

$D=0$ $S=47$
$D=1$ $S=42$
SALTO DI 'S'

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

Name+Surname:______________________________________ Univ. Code:_________________

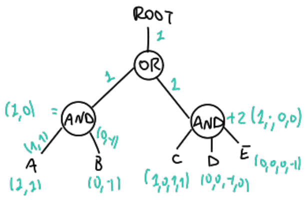
Q9 - Prove that **<u>any</u>** linear secret sharing scheme is homomorphic with respect to the sum operation.

$$\begin{cases} A x_a = Y_a & x_a = (s_a, a_1, \dots) & Y_a = (share1a, \dots) \\ A x_B = Y_B & x_B = (s_b, b_1, \dots) & Y_B = (share1b, \dots) \end{cases}$$

$$Y_a + Y_b = A(x_a + x_B) = A(s_a+s_b, a_1+b_1, \dots)$$

Q10 – 1) Determine the access control matrix that implements the policy: $\pi = (A \cap B) \cup (C \cap D \cap E)$, and then 2) turn it into a linear secret sharing scheme, by computing the shares to assigned to the 5 parties (use modulus 100, share secret S=10, inventiyour own random values if/when necessary)

1) (A and B) OR (C and D and E)



$$\begin{array}{c|cccc} A & 1 & 1 & 0 & 0 \\ B & 0 & -1 & 0 & 0 \\ C & 1 & 0 & 1 & 1 \\ D & 0 & 0 & -1 & 0 \\ E & 0 & 0 & 0 & -1 \end{array}$$

2)

$$\underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}}_{5 \cdot 4} \cdot \underbrace{\begin{bmatrix} 10 \\ 3 \\ 7 \\ 4 \end{bmatrix}}_{4 \cdot 1} = \begin{bmatrix} 30 \mod 55 \\ -3 \mod 55 = 52 \\ 10+7+4 = 21 \\ -7 \mod 55 = 48 \\ -4 \mod 55 = 51 \end{bmatrix}$$