Cryptography Pearl 100 - 2021-2022 - Practice Exam 1

Course: B-CS-MOD01-1A-202001022 B-CS Pearls of Computer Science Core 202001022

Contents: Pages:

Generated on: Aug 26, 2021

Cryptography Pearl 100 - 2021-2022 - Practice Exam 1

Course: B-CS-MOD01-1A-202001022 B-CS Pearls of Computer Science Core 202001022

This is a practice exam. Please use it to learn for the real exam.

- You may use 1 A4 sheet (both sides) with your own notes for this practice exam, as well as the calculator as provided in the digital exam (Remindo).
- Your own calculators, laptops, mobile phones, books etc. are not allowed.
- In order to simulate the real exam, it is recommended that you try to finish this practice exam within 60 minutes.

1 Please select the correct answer for each subquestion. There is only **one correct answer per subquestion**.

1 pt. **a.** (a) Is the RSA cryptosystem perfectly secure?

a. NO

b. YES

1 pt. **b.** (b) Assume that the ciphertext QGBTM was created using the Vigenère cipher with the key BC. What is the underlying plaintext?

a. SIGHT

b. OFFER

c. PEARL

d. REACH

1 pt. **c.** (c) Let *(N, e) = (23711, 7)* be an RSA public key. Note that *N* is not small, so do NOT try to factor it. Furthermore, let *c = 23583* mod *N* be an RSA encryption under the given public key *(N, e)*.

You can assume that *c* is an encryption of the following messages, but which of them does *c* really encrypt?

a. 1

b. 2

c. 23709

d. 23710

1 pt. **d.** (d) What is the result of the computation $12^{3386092} - 88 \bmod 13$?

a. 0

b. 1

c. 2

d. 3

e. 4

1 pt. **e.** (e) Let *N = 15* be a product of two distinct primes and let *e = 2*. Can we use *(N, e) = (15, 2)* as a public key in the RSA cryptosystem (i.e., can *(N, e)* be a valid public key output of the RSA key generation)?

a. NO

b. YES

2 The following questions can have more than one correct answer. To get full points, you need to select *all* correct answers. You get points deducted for each selected wrong answer.

3 pt. **a.** (a) Select *all* elements from the following list that are contained in $\mathbb{Z}_{14}^*$.

a. 0

b. 1

c. 2

d. 3

e. 4

f. 5

g. 6

h. 7

i. 8

j. 9

k. 10

l. 11

m. 12

n. 13

6 pt. **b.** (b) Let $(N, e) = (119, 5)$ be an RSA public key. Which of the following statements are correct?

a. $c = 120$ is a valid RSA *encryption* under the given public key (N, e) and it encrypts the plaintext message $m = 1$.

b. $\sigma = 6$ is a valid RSA *signature* for the given public key (N, e) and it signs the message $m = 41$.

c. $\sigma = 1$ is a valid RSA *signature* for the given public key (N, e) and it signs the message $m = 1$.

d. $c = 32$ is a valid RSA *encryption* under the given public key (N, e) and it encrypts the plaintext message $m = 2$.

3 2 pt. Compute value $x \in \mathbb{Z}$ such that $11 \cdot x \bmod 22 = 1$. If there is no such value x , then type in NO as your solution.

$x =$ .....

4 2 pt. Assume that 31 parties want to securely communicate by using secret-key encryption. This implies that they first have to exchange a unique secret key between any two of them. How many secret keys have to be exchanged in total?

The number of secret keys to be exchanged in total = ...

5 Consider the following plaintext message (a 13-bit string):

`1011000101101`

Use the table below to *encrypt* this message in the **CBC**-mode by using the following 4-bit block cipher:

$E_k(b_3b_2b_1b_0) = b_3b_2b_1b_0 \oplus k$

with the bit-string k = `0010` as secret key (note that $b_3b_2b_1b_0$ denotes an arbitrary 4-bit plaintext message). As initialization vector for the CBC-mode, use the bit-string IV = `1110`.

If desirable, you can use "optional"-cells for intermediate results (they won't give you any points though).

Block nr. j	**Plaintext block m_j**	**a.** .....(0 pt.) (optional - no points)	**b.** .....(0 pt.) (optional - no points)	**Ciphertext block c_j**
j = 1	**c.** ..(0 pt.) (fill in)	**d.** .....(0 pt.) (optional - no points)	**e.** .....(0 pt.) (optional - no points)	**f.** ...(2 pt.) (fill in)
j = 2	**g.** ..(0 pt.) (fill in)	**h.** .....(0 pt.) (optional - no points)	**i.** .....(0 pt.) (optional - no points)	**j.** ...(2 pt.) (fill in)
j = 3	**k.** ..(0 pt.) (fill in)	**l.** .....(0 pt.) (optional - no points)	**m.** .....(0 pt.) (optional - no points)	**n.** ..(2 pt.) (fill in)
j = 4	**o.** .....(0 pt.) (fill in)	**p.** .....(0 pt.) (optional - no points)	**q.** .....(0 pt.) (optional - no points)	**r.** .....(2 pt.) (fill in)

NOTE: Make sure that you only type in (sequences of) 0's and 1's! Any other format will be ignored and regarded as a wrong answer.

Hint. You need to use "padding" to solve this assignment successfully.

6 Let *p = 7*, *q = 13*, and *N = pq = 91*. Assume that we use *(N, e) = (91, 29)* as the public key in the RSA encryption scheme.

(a) What is Euler's totient function *φ* evaluated on *N*?

φ(N) = **a.** .....(2 pt.)

1 pt. **b.** (b) Which of the following equations can be used to deduce a value x such that $e \cdot x \bmod \varphi(N) = 1$?

a. $-1 = 7 \cdot (-2) + 13 \cdot 1$

b. $1 = 91 \cdot 19 - 72 \cdot 24$

c. $1 = (-7) \cdot 91 + 22 \cdot 29$

d. $1 = 5 \cdot 29 + (-2) \cdot 72$

(c) What is the RSA secret key *d ≥ 0* that corresponds to the public key *(N, e) = (91, 29)*?

d = **c.** .....(2 pt.)

Correction model

1. 5 pt.
- a. A
- b. C
- c. C
- d. E
- e. A

2. 9 pt.
- a.
  - -0.5 pt. A
  - 0.5 pt. B
  - -0.5 pt. C
  - 0.5 pt. D
  - -0.5 pt. E
  - 0.5 pt. F
  - -0.5 pt. G
  - -0.5 pt. H
  - -0.5 pt. I
  - 0.5 pt. J
  - -0.5 pt. K
  - 0.5 pt. L
  - -0.5 pt. M
  - 0.5 pt. N
  - Bonus: 0 pt.
- b.
  - -1 pt. A
  - 2 pt. B
  - 2 pt. C
  - 2 pt. D
  - Bonus: 0 pt.

3. 2 pt.
2 pt. NO

4. 2 pt.
2 pt. 465

5. 8 pt.
- a. 0 pt.
- b. 0 pt.
- c. 0 pt. 1011
- d. 0 pt.
- e. 0 pt.
- f. 2 pt. 0111
- g. 0 pt. 0001
- h. 0 pt.
- i. 0 pt.
- j. 2 pt. 0100
- k. 0 pt. 0110
- l. 0 pt.
- m. 0 pt.
- n. 2 pt. 0000
- o. 0 pt. 1100
- p. 0 pt.
- q. 0 pt.
- r. 2 pt. 1110

6. 5 pt.
- a. 2 pt. 72
- b. D
- c. 2 pt. 5

Caesura

Points scored	Grade
31	10
30	9.7
29	9.4
28	9.0
27	8.7
26	8.4
25	8.1
24	7.7
23	7.4
22	7.1
21	6.8
20	6.5
19	6.1
18	5.8
17	5.5
16	5.2
15	5.0
14	4.7
13	4.4
12	4.2
11	3.9
10	3.6
9	3.4
8	3.1
7	2.8
6	2.6
5	2.3
4	2.1
3	1.8
2	1.5
1	1.3
0	1.0

Question identifiers

These identifiers can be used to track the exact origin of the question. Use these identifiers together with the identifier of this document when sending in comments about the questions, so that your comment can be connected precisely with the question you are referring to.

Document identifier: 3372-7894

Question number	Question identifier	Version identifier
1	36897	a19f47ab-e181-cd7f-8aba-eff782a007c3
2	15424	ff0cd04d-4236-0920-6862-f236f0d55209
3	15427	e75e39df-933b-bb40-8955-c37e94b6140e
4	15430	88250423-4679-8ca3-e818-4cbb72863566
5	15433	e732f8d1-ad3b-eeda-5c4d-76f5f5776468
6	36902	82e82a1d-3b5e-e3b1-f05b-aff046acc28d