Cryptography Pearl 100 - 2021-2022 - Practice Exam 1

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

Generated on: Aug 26, 2021

Contents: Pages:

Cryptography Pearl 100 - 2021-2022 - Practice Exam 1

Course: 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.

Number of questions: 6

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. `OFFER`

b. `REACH`

c. `PEARL`

d. `SIGHT`

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. YES

b. NO

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

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

3 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.
2 pt.

$x =$ .....

4 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?
2 pt.

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

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

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

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

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