Pearls of Computer Science - Pearl 100 - 2021-22-Practice exam - 2

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

Generated on: Aug 26, 2021

Contents:

Pages:

Pearls of Computer Science - Pearl 100 - 2021-22-Practice exam - 2

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: 4

1 Please select the correct answer (among four choices) for each subquestion. There is only **one correct answer per subquestion**.

IMPORTANT:

1. For each correct answer you get 2 points.
2. Don't just guess; for each wrong answer, you get 1 point deducted for the question as a whole!
3. The minimum number of points in this question is 0 points; you cannot get negative points for the question as a whole.

2 pt. **a.** (a) Let `LLMIRAWJRRHPPWGOS` be a ciphertext produced by the Vigenère cipher using a key of length 5. Which of the following messages has the highest probability of being the underlying plaintext?

a. `ZEROISONEMINUSONE`

b. `FIVEISFOURPLUSONE`

c. `THREEISONEPLUSTWO`

d. `FIVEISANODDNUMBER`

2 pt. **b.** (b) Suppose that Alice encrypts the plaintext `11 01 11` using the One-Time-Pad. Assuming you don't know which key Alice used in the encryption, which of the following statements is correct?

a. The probability that `11 11 11` is the resulting ciphertext is 16.6667%.

b. The probability that `00 11 11` is the resulting ciphertext is 3.1250%.

c. The probability that `11 01 11` is the resulting ciphertext is 1.5625%.

d. The probability that `00 00 00` is the resulting ciphertext is 0%.

2 pt. **c.** (c) Which of the following statements about the different block cipher modes of operation is correct?

a. In the CBC mode, a transmission error in a single ciphertext block will affect the decryption of the block itself and *all* succeeding blocks.

b. In the CBC mode, a transmission error in a single ciphertext block will *only* affect the decryption of the immediately succeeding next block.

c. In the OFB mode, a transmission error in a single ciphertext block will *only* affect the decryption of the immediately succeeding next block.

d. In the OFB mode, a transmission error in a single ciphertext block will *only* affect the decryption of the block itself.

2 pt. **d.** (d) Which of the following statements is correct?

a. Encrypting the message `TWENTE` using the Vigenère cipher with the key `CAESAR` results in the same ciphertext as when encrypting this message using the CAESAR cipher.

b. In the ECB mode, the same plaintext blocks are encrypted into the exact same ciphertext blocks.

c. The Feistel cipher is a block cipher which encrypts plaintexts into ciphertexts whose lengths are strictly smaller than those of the underlying plaintexts.

d. In the One-Time-Pad, it is required that the length of the used secret key is strictly less than the length of the to-be-encrypted plaintext message.

2 pt. **e.** (e) Let $p = 37$ and $q = 53$ be primes, and $N = pq = 1961.$ What is the result of the computation: $3^{1872} + 3921 \bmod 1961?$

a. 0

b. 1

c. 2

d. 3

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.

2 pt. **a.** (a) Select *all* elements from the following list that are contained in $\mathbb{Z}_8^*$.

a. 0

b. 1

c. 2

d. 3

e. 4

f. 5

g. 6

h. 7

4 pt. **b.** (b) Which of the following numbers are valid, but too small to be secure, RSA moduli (i.e., generated as described in the lecture)?

a. 1

b. 1961

c. 37

d. 319

e. 2048

4 pt. **c.** (c) Let $(N, e) = (41449, 11)$ be an RSA public key. Which of the following statements are correct?

(*Note:* N is not small, so do *NOT* try to factor it! Moreover, you don't have to compute the RSA secret key *d* in this question.)

a. $\sigma = 41448$ is a valid RSA *signature* for the given public key (N, e) and it signs the message $m = 1$.

b. $c = 39401$ is a valid RSA *encryption* under the given public key (N, e) and it encrypts the plaintext message $m = 41447$.

c. $\sigma = 3$ is a valid RSA *signature* for the given public key (N, e) and it signs the message $m = 11351$.

d. $c = 177146$ is a valid RSA *encryption* under the given public key (N, e) and it encrypts the plaintext message $m = 3$.

e. $c = 0$ is a valid RSA *encryption* under the given public key (N, e) and it encrypts the plaintext message $m = 0$.

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

`10001`

Use the table below to *encrypt* this message in the **OFB**-mode by using the following 3-bit block cipher:

$E_k(b_2 b_1 b_0) = b_2 b_1 b_0 \oplus k$

with the bit-string k = `011` as secret key (note that $b_2 b_1 b_0$ denotes an arbitrary 3-bit plaintext message) and "shift"-parameter $r = 2$. As initialization vector for the OFB-mode, use the bit-string IV = `001`.

If desirable, you can use the "(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)

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.

4 Let *p = 53*, *q = 71*, and *N = pq = 3763*. Assume that we use *(N, e) = (3763, 11)* 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.)

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

NOTE: Don't just guess; you get 1 point deducted for selecting the wrong answer!

a. $1 = 3763 \cdot 1 - 11 \cdot 342$

b. $1 = 3763 \cdot 947 - 3640 \cdot 979$

c. $3 = 10920 \cdot (-1) + 33 \cdot 331$

d. $3 = 53 \cdot (-12) + 71 \cdot 9$

(c) What is the RSA secret key *d ≥ 0* that corresponds to the public key *(N, e) = (3763, 11)*?

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

This is the end of the practice exam.

Feel free to do the practice exam again in order to prepare yourself for the real exam.