X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Foundations of Cryptography (course)

Announcements (announcements) **About the Course (https://swayam.gov.in/nd1_noc20_cs02/preview)**

Ask a Question (forum) Progress (student/home) Mentor (student/mentor)

Unit 2 - Course Overview, Symmetric-key Encryption, Historical Ciphers, Perfect Security and Its Limitations

Register for Certification exam (https://nptelaprilexam.swayam.gov.in/)

Course outline

How does an NPTEL online course work?

Course Overview, Symmetric-key Encryption, Historical Ciphers, Perfect Security and Its Limitations

- Introduction (unit?unit=27&lesson=28)
- Symmetric-key Encryption (unit?unit=27&lesson=29)
- Historical Ciphers and their

Week 1 Assessment

The due date for submitting this assignment has passed. **Due on 2020-02-12, 23:59 IST.**

Assignment submitted on 2020-02-12, 23:49 IST

Assignment for Week1

1) Advanced application(s) of cryptography include(s) which of the following (select all options that apply) : ***1 point***

☑ Bitcoin Technology
☑ Zero-knowledge Proof
□ Secure cloud computation
□ None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
Bitcoin Technology
Zero-knowledge Proof
Secure cloud computation

2) Example of a perfectly secure encryption scheme is: ***1 point***

○ Vigenère Cipher
● Vernam Cipher
○ Affine Cipher
○ Playfair Cipher

Cryptanalysis (unit?unit=27&lesson=30)

○ Perfect Security (unit?unit=27&lesson=31)

○ Limitations of Perfect Security (unit?unit=27&lesson=32)

● **Quiz : Week 1 Assessment (assessment?name=25)**

Computational Security, Semantic Security and Pseudorandom Generators (PRGs)

Stream Ciphers, Provably-secure Instantiation of PRG, Practical Instantiation of PRG, CPA-security and Pseudo-random Functions (PRFs)

Weekly Feedback forms

Yes, the answer is correct.
Score: 1

Accepted Answers:
Vernam Cipher

3) Which of the following statement(s) is/are necessarily correct? ***1 point***

1. Any encryption scheme with key length greater than message length is a perfectly-secure scheme.
2. Given the one-time pad scheme, the scheme is no longer perfectly-secure if on any subsequent invocation of the key generation algorithm, an earlier key gets re-generated.

● 1 only
○ 2 only
○ Both 1 and 2
○ Neither 1 nor 2

No, the answer is incorrect.
Score: 0

Accepted Answers:
Neither 1 nor 2

4) You are given an encryption scheme that is CPA Secure. Then which of following statement is/are correct? ***1 point***

□ We are not sure whether the scheme is COA secure.
☑ We are not sure whether the scheme is necessarily both COA secure and KPA secure.
□ We are guaranteed that the scheme is both COA secure and KPA secure.
□ We are guaranteed that the scheme is CCA secure.

No, the answer is incorrect.
Score: 0

Accepted Answers:
We are guaranteed that the scheme is both COA secure and KPA secure.

5) A scheme is called perfectly-secure, if in the perfect indistinguishability experiment, the adversary can win the game (where we say the outcome of the experiment = 1) with probability exactly equal to : ***1 point***

○ 1
● 0
○ 0.5
○ 0.75

No, the answer is incorrect.
Score: 0

Accepted Answers:
0.5

6) Which of the following statement(s) is/are incorrect for a symmetric-key encryption scheme? ***1 point***

1. A symmetric-key encryption scheme consists of only two algorithms – encryption and decryption
2. The decryption algorithm should always be a deterministic algorithm
3. The encryption algorithm can either be a randomized or deterministic algorithm

□ 1 only
□ 2 only
□ 3 only
☑ All of 1, 2, 3

No, the answer is incorrect.
Score: 0

Accepted Answers:
1 only

7) A malicious adversary is best modeled in which of the following adversarial models? ***1 point***

○ CPA
○ KPA
○ COA
● CCA

Yes, the answer is correct.
Score: 1

Accepted Answers:
CCA

8) Consider an instance of shift cipher with the probability distribution over the message space as follows: P[M=a] = 0.3, P[M=b] = 0.3, P[M=c] = 0.4. What is the probability that the ciphertext is ‘D’? ***1 point***

○ 1/26
○ 1/13
○ 3/26
● None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
1/26

9) Refer Numerical Example II from Lecture 04. ***1 point***
Define *x* as the probability that plaintext is *d*, given that the ciphertext is *2*. Then the value of *(7x + 10)* = ?

○ 17
● 15
○ 16
○ None of the given options

No, the answer is incorrect.
Score: 0

Accepted Answers:
16

10)Assume you are given a 300 character encrypted message, encrypted in Vigenère cryptosystem, in which you know the plaintext word CRYPTOGRAPHY occurs exactly two times, and we know that the ciphertext sequence TICRMQUIRTJR is the encryption of CRYPTOGRAPHY. The first occurrence starts at character position 10 and second at character position 241 (we start counting from 1). What is the length of the key used for encryption ? ***1 point***

○ 7
● 8
○ 9
○ 10

No, the answer is incorrect.
Score: 0

Accepted Answers:

7