Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal

Mid-Semester Examination February 2024

Course Code: CS851 **Course Name:** Network Security

Duration: 90 Minutes **Max. Marks:** 40

Note: Answer all questions.

Q1. There are three typical ways to use Nonces as challenges. Suppose N_a is a nonce generated by A. A and B share key K, and f() is a function (such as an increment). The three usages of Nonce are shown below. [2+2+2]

(i) A → B: N_a
B → A: $E_K(N_a)$

(ii) A → B: $E_K(N_a)$
B → A: N_a

(iii) A → B: $E_K(N_a)$
B → A: $E_K(f(N_a))$

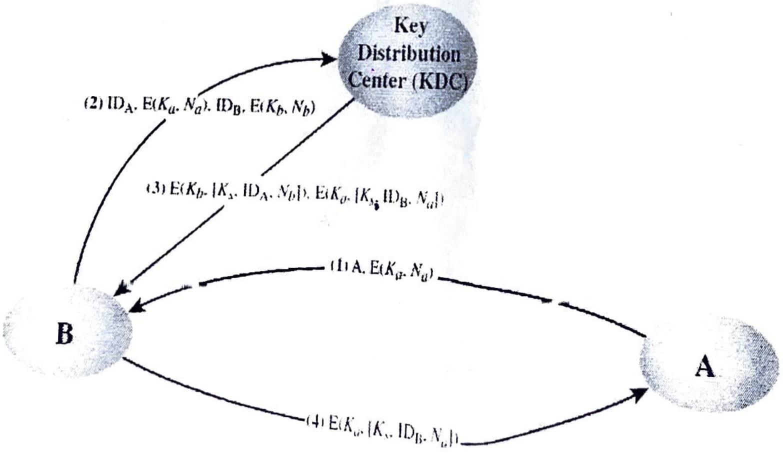
Describe situations for which each usage is appropriate.

Q2. (i) Design a lightweight protocol to enable secure online payment using the web client and server environment over the Internet. The proposed protocol must meet the following. [1.5×6]

- ➢ Provide Server Authentication
- ➢ Ensure Confidentiality and Integrity of payment-related data
- ➢ Provide Plain text access of payment-related data to the payment-approving bank only.
- ➢ Send payment approval intimation to the merchant and Gateway.
- ➢ Enforce the "Need-to-Know" security principle.
- ➢ Should use X.509 certificates

(ii) Compare the above-proposed protocol with SET (Secure Electronic Transaction) to show lightness. [5]

Q3. The following figure shows that one local area network vendor provides a key distribution facility.


Key Distribution Center (KDC)
(2) ID_A, $E(K_a, N_a)$, ID_B, $E(K_b, N_b)$
(3) $E(K_b, [K_s, ID_A, N_b])$, $E(K_a, [K_s, ID_B, N_a])$
(1) A, $E(K_a, N_a)$
B
A
(4) $E(K_a, [K_s, ID_B, N_a])$

(i) Explain the key distribution scheme. [5]

(ii) Highlights the advantages and disadvantages of the key distribution scheme. [2.5+2.5]

Q4. (i) What is Secure Socket Layer (SSL) Protocol, and explain how it can protect web traffic from confidentiality and integrity breaches. [5]

(ii) What is end-to-end encryption, and explain how it can be used to secure app-based chat. [5]
