Sample Question1

Consider the following pseudo-WEP protocol. The key is 4 bits and the IV is 2 bits. The IV is appended to the end of the key when generating the keystream. Suppose that the shared secret key is 1010. The keystreams for the four possible inputs are as follows:

101000: 00101011010101010011011010100100 . . .

101001: 10100110110010101101001001011101 . . .

101010: 00011010001111000101001010011111 . . .

101011: 11111010000000001010101000101111 . . .

Suppose all messages are 8-bits long. Suppose the ICV (integrity check) is 4-bits long, and is calculated by XOR-ing the first 4 bits of data with the last 4 bits of data. Suppose the pseudo-WEP packet consists of three fields: first the IV field, then the message field, and last the ICV field, with some of these fields encrypted.

We want to send the message m = 10100000 using the IV = 11 and using WEP. What will be the values in the three WEP fields?

Sample Question1 - Solution

Answer:
Since IV = 11, the key stream is 111110100000 …….

Given, m = 10100000
Hence, ICV = 1010 XOR 0000 = 1010
The three fields will be:

IV: 11
Encrypted message: 10100000 XOR 11111010 = 01011010
Encrypted ICV: 1010 XOR 0000 = 1010 (remember the key bits from 9-12 above are all 0000.
•

Sample Question-2

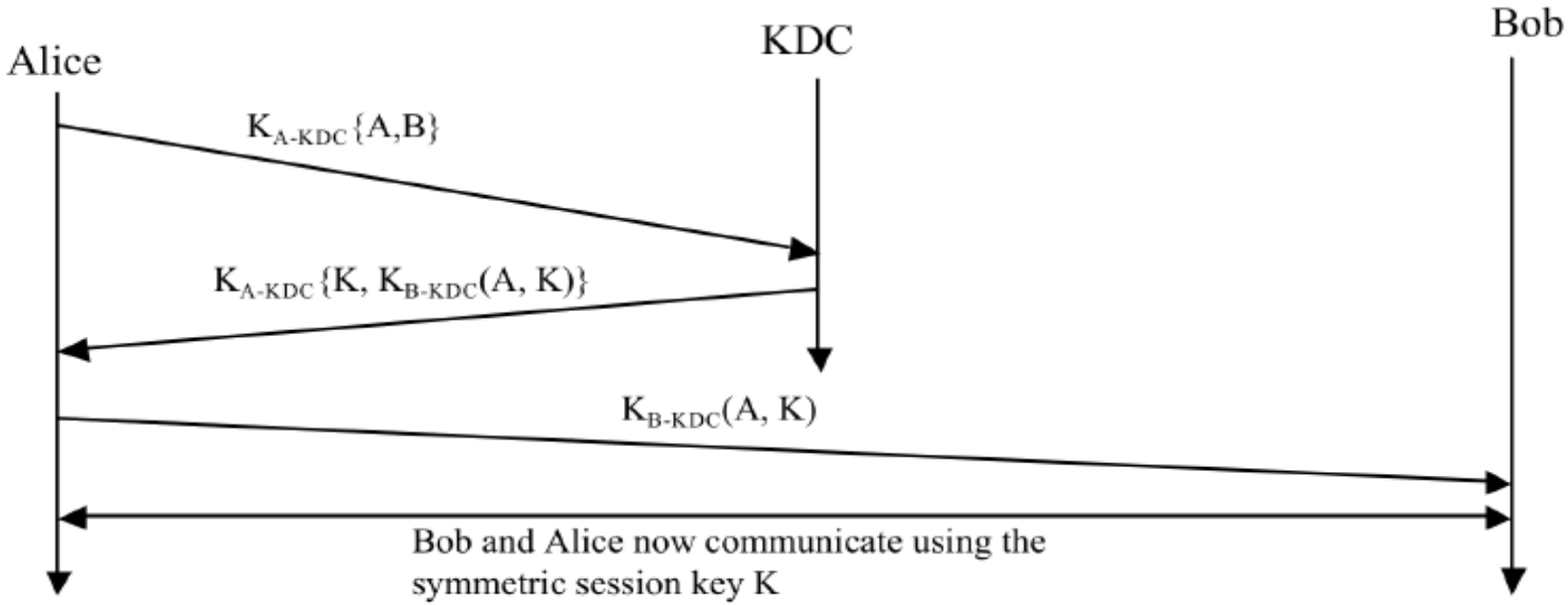
Suppose Alice wants to communicate with Bob using Symmetric Key Cryptograpy using a session key Ks. In this question we use a Key Distribution Centre in place of Public Key Cryptography. KDC shares a unique secret symmetric key with each registered user. For Alice and Bob, denote these keys by $K_{A\text{-}KDC}$ and $K_{B\text{-}KDC.}$ Design a scheme that uses the KDC to distribute the session key: A message from Alice to the KDC; A message from KDC to Alice; and finally a message from Alice to Bob. The first message is $K_{A\text{-}KDC}$ (A,B). Using the notation $K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$, S, A, and B answer the following questions:

A) What is the second message?

B) What is the third message?

(Exam question may be longer a bit more complex)

Sample Question-2 Solution



First message; Request a session key with Bob from KDC
Second Message: KDC to Alice, sends Key as well as the key encrypted with Bob's shared key with KDC for Bob to verify that it is from a legitimate source.
Third Message: Alice sends this encrypted key to Bob (saying that use this key for session With A (Alice)

Correction: Curly braces should Be parenthesis in first message

Sample Question 3

- Suppose Bob initiates a TCP connection to Trudy who is pretending to be Alice. During the handshake, Trudy sends Bob Alice's certificate. In what step of the SSL handshake algorithm will Bob discover that he is not communicating with Alice?

Sample Question 3 - Solution

Answer:

After the client will generate a pre-master secret (PMS), it will encrypt it with Alice's public key, and then send the encrypted PMS to Trudy. Trudy will not be able to decrypt the PMS, since she does not have Alice's private key. Thus Trudy will not be able to determine the shared authentication key. She may instead guess one by choosing a random key. During the last step of the handshake, she sends to Bob a MAC of all the handshake messages, using the guessed authentication key. When Bob receives the MAC, the MAC test will fail, and Bob will end the TCP connection.

Thank You

- And good luck with final exams.