ESD5 – Fall 2024
Problem Set 5

Department of Electronic Systems
Aalborg University

October 7, 2024

Problem 1

In encryption using block-cipher, what potential problem can occur when using Electronic Code Book? Using Cipher Block Chaining?

Problem 2

Assume that two parties know each other's public keys. If one message is sent from A to B, what can be verified? If two messages are exchanged, what can be verified?

Problem 3

With Diffie-Hellman key exchange, is it a man-in-the-middle attack possible? If possible, draw how this could be achieved.

Problem 4

Assume the following scenario: A and B both have the knowledge of a secret key K (e.g. pre-shared). They communicate over an insecure channel. Define a protocol (by writing down a message sequence chart) in which A and B use the pre-shared key K to mutually authenticate each other and to agree on a common session key (different from the long-term pre-shared key K). Try to keep the number of exchanged messages as low as possible.

Problem 5

Asymmetric encryption and symmetric encryption are both actively used to ensure security. While Asymmetric encryption leads to more security it comes with computational expensive algorithms for encryption and decryption. Meanwhile, symmetric keys provide less security but are less computationally expensive. Assuming A has a public/private key pair, where B can ask what the public key is through an unsecured channel, how could a middle ground between the computational cost and security be met?

(a) To further enhance security enhancing the authentication is critical. What kind of technology could A possess, and how would this make a Man-in-the-middle attack more difficult?