Solutions to Selected Problems

Guide to Internet Cryptography

Companion Material

February 7, 2026

Preface

This document provides solutions to selected problems from the book *Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*. The material is intended for educational use in courses and self-study.

Book website: https://link.springer.com/book/10.1007/978-3-031-19439-9

1 Chapter 7: Cellular Networks

Problem 7.1 GSM: Roaming

If A5 was *not* standardized: Which information would the foreign cellular network need to communicate with the mobile device of a roaming customer to be able to decrypt the radio signal at the base station?

Solution

It would need an implementation of the proprietary version of A5 and the key Kc.
Since there is no deployed, standardized method to communicate implementation details of algorithms between mobile devices and base stations, this would disable interoperability.

Problem 7.2 GSM: IMSI Catcher

Would the following countermeasure prevent the attack described in Figure 7.6? The key Kc is not directly used in A5-X, but only the key $k_X \leftarrow \mathsf{KDF}(Kc, \texttt{A5-X})$. Here `"A5-X"` is the ASCII string denoting version 1, 2, or 3 of A5.

Solution

Yes, because the IMSI Catcher would only learn the key k_2, which is different from the key k_3 needed to communicate with base station (AuC). Any good key derivation function will make it impossible to compute k_3 from k_2.

Problem 7.3 UMTS

In the protocol from Figure 7.8, the USIM does not send a challenge to HE. Which authentication protocol from chapter 4 would be best to describe the authentication of HE?

Solution

From the perspecktive of SN, the USIM is authenticated through a challenge-and-response protocol. Here RAND is the challenge, and RES is the response.
From the perspective of the USIM, the HE authenticates itself through a variant of a counter-based OTP protocol, where the counter is the sequence number SQN.