# Solutions to Selected Problems

Guide to Internet Cryptography

Companion Material

February 12, 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 13: SSH

### Problem 13.1 SSH key management

How would you display the X.509 certificate validation result in a CLI window? Which digital identity of the server should the certificate contain?

### Solution

X.509 certificates are *not* used in SSH, although a few SSH projects support them. Using a PKI is simply not necessary in most SSH use cases.
If a PKI was used, the result of the X.509 validation could be displayed as a text string: "The signature presented by the sever is valid, and was verified against a valid certificate chain. The server name in the leave certificate is `ssh.example.com`"
Domain names are be easier to remember than IP addresses, so they should be preferred.

### Problem 13.2 SSH-1

Why must the two RSA moduli be of different lengths? What would be the minimum length difference if PKCS#1 encoding is used for the inner ciphertext?

### Solution

Let $n_1 < n_2$. As it is already mentioned in the question, the result of the first RSA-PKCS#1 encryption (of bytelength $|n_1|_8$) must be encoded agains with PKCS#1 before it is encrypted a second time. The minimal padding for this would consist of the bytes 0x00 and 0x02 as the prefix, at least eight non-zeri padding bytes, and the delimiter byte 0x00. So we must add at least 11 bytes, which results in

$$|n_1|_8 + 11 \leq |n_2|_8$$

### Problem 13.3 SSH 2.0 Handshake

Which basic protocols introduced in chapter 4 are contained in SSH 2.0?

### Solution

One DHKE, and two signature/verify protocols.

### Problem 13.4 SSH 2.0 BPP

Normally, encryption *protects* the confidentiality of data. So why is it better to *not* encrypt the length field in the BPP?

### Solution

Because as [3] shows, if we put another ciphertext in the place of the encrypted length field, the decryption can be used as an oracle to determine an unknown plaintext value. SSH now supports many additional ciphers, which either don't encrypt the length field, or encrypt it with a different key.

### Problem 13.5 SSH 2.0 BPP

Suppose we would modify the length field in BPP as follows: We use 8 bytes instead of 4 and double the length indication therein. If the SSH recipient first checks if the two length indications match: What would be the probability that the attack by Albrecht et al. still works?

### Solution

Assuming that the plaintext is pseudorandom, the probability that the second half of a plaintext is identical to the first half is $2^{-32}$.