Even-Numbered Problem Solutions to *Understanding Cryptography* From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms by Christof Paar- Jan Pelzl - Tim Guneysu

Mustapha EL BOUAZAOUI.
mustaphaelbouazaoui@gmail.com

July 23, 2025

Abstract

While trying to recall a bit of cryptography to prepare for interviews. I find the masterpiece of lectures by Mr. christophe Paar in youtube. From then, I find out the book and while trying to solve some problems from it, I find out there's book only for odd-numbered problems. I find it intriguing and interesting as if the writer want someone to do the other part. And as far as I am aware, none has done the other part. So, I decided to be the one who gonna do the other one and publish them and try to add bunch of code in python as an example for those ciphers.
keywords: Mathematics, cryptography, problems, solutions.

Contents

Chapter 1 Introduction to Cryptography and Data Security

1.1 See code 1.1.py.

1.2

We know we are dealing with a shift cipher. Hence, we can perform letter frequency analysis to guess k: the number of positions by which the most frequent letter (usually "e" in English) has been shifted. After deciphering, we found:
"If we all unite, we will cause the rivers to stain the great waters with their blood" — Tecumseh in his speech to the Osages.
See 1.2.py for the code used.

1.3

There's a small mistake in the solution, as the ASIC costs \$50, not \$100.

1.4

1. For each letter, there are 128 possible characters. Since we have 8 letters, the size of the key space is 128^8.
2. Each letter uses 7 bits, so the key length is $7 \times 8 = 56$ bits.
3. Similarly, if only lowercase letters are used, the size of the key space is 26^8.
4. Representing 26 letters requires $\frac{\log 26}{\log 2} \approx 4.7$ bits, which rounds up to 5 bits per character. Hence, the key length is $5 \times 8 = 40$ bits.
5. (a) For 7-bit characters, we need $\frac{128}{7} \approx 18.3$, so we need at least 19-character passwords.
   (b) For 26 lowercase letters, we need $\frac{128}{5} = 25.6$, so we need 26-character passwords.

1.5 *Hint:* Use the identity $p^n - 1 = (p-1)\left(\sum_{i=0}^{n-1} p^i\right)$. Straightforward calculation.

1.6

Attacker	Can read?	Can alter?	Why?
Hacker between Alice and base station A	No	No	Sees only y_1 and does not have k_1.
Mobile operator on A	Yes	Yes	Controls base station A and knows k_1 and k_2.
National law enforcement agency	Yes	Yes	Same reason as (b) or (e), once access is obtained.
An intelligence agency of a foreign country	No	No	Only sees y_2.
Mobile operator on B	Yes	Yes	Same reason as (b).
Hacker between Bob and base station B	No	No	Only sees y_3 and does not know k_3.

- None can read or alter the message, since they only see c, which only Alice and Bob can decrypt using their mutual key k_{AB}.

1.7 Easy.

1.8

- $5 \times 8 = 40 \equiv 1 \mod 13$
- $5 \times 3 = 15 \equiv 1 \mod 7$
- $3 \times 2 \times 5^{-1} = 6 \times 3 = -3 \equiv 4 \mod 7$

1.9 Straightforward.

1.10

- $5 \times 9 = 45 \equiv 1 \mod 11$
- $5 \times 5 = 25 \equiv 1 \mod 12$
- $5^{-1} \equiv 8 \mod 13$

Hence, the multiplicative inverse of a number (if it exists) depends on the ring we are working in (e.g., $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, etc.).

1.11 Straightforward calculation.

1.12

- $\phi(4) = 2$
- $\phi(5) = 4$
- $\phi(9) = 6$
- $\phi(26) = 12$

1.13

Chapter 2 Stream cipher