PART 1

Exercise 1.1

Consider a Vigenère cipher with key-length equal to 4. Given the ciphertext AFYWX what of the plaintexts CLASS, HOUSE, HORSE, TABLE, ZEBRA could possibly be the correct decryption? Justify your answer.

Exercise 1.2

Consider the following protocol that authenticates *Alice* (A) to *Bob* (B):

$$A \rightarrow B : E_K(t_A)$$

where t_A must be a valid, recent timestamp and K is a long-term key shared between A and B.

1. Show an attack that allows a malicious user to impersonate B with A without necessarily breaking key K;
2. Illustrate a modification of the protocol that fixes the previous problem and show how the attack is prevented.

Exercise 1.3

A questionnaire requires users to pick among the following choices: *good*, *ok*, *bad*, *awful*. The `username` is sent to the server in the clear. The choice, instead, is encoded as an ASCII string (each character is one byte), padded with zeros up to 16 bytes and encrypted using AES:

$$\texttt{username}, E_K(\texttt{padded\_choice})$$

At the end of the questionnaire, the overall number of different choices is published. For example, 120 *good*, 80 *ok*, 74 *bad*, 6 *awful*.

1. Describe an attack that allows a malicious user to discover who voted what (without breaking AES of course);
2. Illustrate a modification of the encryption scheme that prevents the attack.

PART 2

Exercise 2.1

Write a fragment of C code with an overflow vulnerability. Discuss possible consequences of the overflow and show how to fix the code so to prevent the attack.

Exercise 2.2

A network attacker injects into page

```
http://mysite.com/index.html
```

requested by Alice, a reference to

```
https://mybank.com/payment.php?account=r1x&amount=10000
```

Discuss why this is dangerous and how the attack could be prevented.

Exercise 2.3

A web site does not properly filter user input when checking login credentials. Explain why giving as input

```
' OR ''='
```

might allow an attacker to circumvent the credential check and impersonate a user. Give an example of query that is subject to the attack.