PART 1

Exercise 1.1

Give a formal definition of *digital signature scheme* and show an example of implementation through RSA and hash functions. Discuss which cryptographic properties of the hash functions are required in order to prevent forgery attacks.

Exercise 1.2

Consider the following protocol that authenticates A to B:

$$A \quad \rightarrow \quad B \quad : \; B, Sign_A(B)$$

1. Show a replay attack that allows an intruder to impersonate A with B;
2. Illustrate a nonce-based modification of the protocol that fixes the previous problem and show how the attack is prevented.

Exercise 1.3

Consider a shift cipher in which each letter of the plaintext is encrypted under a fresh key, picked at random. Given the ciphertext FHRR, what is the probability that the plaintext is, respectively, WOOD or TREE? Justify your answer.

PART 2

Exercise 2.1

Consider the following fragments of assembly code (Intel syntax):

```
   0x0804851d <+0>:  push   ebp
   0x0804851e <+1>:  mov    ebp,esp
   0x08048520 <+3>:  sub    esp,0x68
   0x08048523 <+6>:  mov    eax,gs:0x14
   0x08048529 <+12>: mov    DWORD PTR [ebp-0xc],eax

   ... (omitted code) ...

   0x08048565 <+72>: mov    edx,DWORD PTR [ebp-0xc]
   0x08048568 <+75>: xor    edx,DWORD PTR gs:0x14
   0x0804856f <+82>: je     0x8048576 <read_name+89>
   0x08048571 <+84>: call   0x80483c0 <__stack_chk_fail@plt>
   0x08048576 <+89>: leave
   0x08048577 <+90>: ret
}
```

Explain what security mechanism is implemented by the above code and discuss an example of attack that is prevented thanks to that specific mechanism.

Exercise 2.2

Consider the following PHP fragment

```
<?php
    ...
    $query = "SELECT 1 FROM people WHERE lastname = '" . $_POST['lastname']. "'";
    ...
?>
```

If the query is successful the application goes on asking for more user input, otherwise message ``User does not exists'' is displayed. Describe an attack that recovers the value of field `password` in the rows of table `people`.

Exercise 2.3

What is a reflected XSS? Show an fragment of code which is vulnerable to reflected XSS and discuss possible fixes.