Security of Computer Systems

20 January 2014

Exercise 1

Give the formal definition of the Vigenère cipher and show that with a key as long as the plaintext, picked at random it is a perfect cipher.

Exercise 2

A flawed RSA setup initializes the cipher with $n = 2p$, where p is a large prime (> 1024 bits). Describe an attack that computes the private exponent a from n and the public exponent b. Illustrate using small numbers.

Exercise 3

It is proposed a payment system for a drink machine in which the machine and the payment device (for example a RFID key) share a cryptographic key k and the recharge is done as follows:

1. The user inserts the payment device and the coins in the machine;
2. The machine counts the amount of money M inserted and sends message $E_k(M)$ to the payment device. M is padded with zeros as needed to reach the block size;
3. The device decrypts the message and increases the credit of the amount M.

Show an attack and discuss possible fixes to the system.

Exercise 4

In order to protect 8-bytes long system passwords, they are hashed using the following function:

$$h(\texttt{pwd}, \texttt{salt}) = \texttt{pwd} \oplus \texttt{salt}$$

The 8-bytes long `salt` is randomly picked for each user and, as usual, is stored in the password file together with the hash of the password. To verify a password the system follows the standard procedure: looks into the file, reads the user `salt` and recompute the hash of the password and the salt. The result is compared with the one stored in the file.
Describe an attack that permits to compute a valid password from the password file. Explain what is the vulnerability and what would be a possible fix.

Exercise 5 (optional, gives extra score)

Explain in detail the Meet-in-the-middle attacks for iterated ciphers.