Exercise n.2 (10 points)

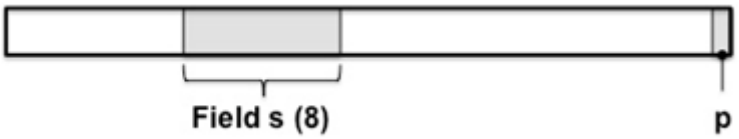

Figure 1. Plaintex format

Let us assume that a plaintext *P* has the format specified in the figure where *s* is an 8-bit field that specifies an amount of money and *p* is a *parity bit* s.t. *p* is 0 if the number of 1s in the plaintext (bit *p* excluded) is even; it is 1 otherwise. The whole plaintext is encrypted by means of one-time-pad.

Question 1.

Does this encryption scheme suffer from malleability? Motivate the answer.

Question 2.

Assume that the adversary knows that field *s* specifies the value 130. Argue whether and how, it is possible to modify the cipher-text so that the decrypted plaintext specifies 146 in the field *s* and such a modification goes undetected.

Question 3.

Propose a possible countermeasure to prevent malleability attacks against OTP.

SOLUTION

Question 1.

The encryption scheme is malleable. A simple way to prove it is the following. Let P[i], C[i], and K[i] be the i-th bit of the plaintext, ciphertext and key, respectively, s.t. C[i] = P[i] xor K[i]. Notice that P[0] = p. Finally let C' be the modified ciphertext and P' the resulting plaintext after decryption. Notice that an adversary can easily complement a bit of the plaintext by operating on the ciphertext. Assume that the adversary wishes to complement bit *i*. Then, (s)he computes C'[i] = C[i] xor 1 = (P[i] xor K[i]) xor 1 = (P[i] xor 1) xor K[i] = P'[i] xor K[i]. It follows that P'[i] = P[i] xor 1, that is, P'[i] is the complement of P[i] (P'[i] = ~P[i]).

For the attack to go undetected, and the scheme to be malleable, the parity bit must be consistently modified as well. Notice that, since P[i] is complemented, the number of 1 either increment or decrement by one. In both cases the parity bit must be complemented as well. This implies that C'[0] = C[0] xor 1.

Q2. The attack consists in complementing C[0] and the 5-th bit in *s*.

Q3. The problem can be solved by replacing the parity bit by a tag resulting from a secure hash function.