SICUREZZA NELLE RETI **SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)**

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

22 July 2015

EXERCISE NO. 1 — #MARKS: 10

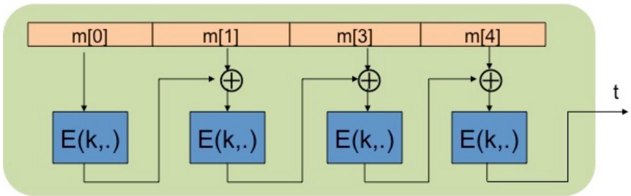
With reference to a perfect cipher,

1. State the Shannon's formal definition of perfect cipher and give an intuitive explanation of the definition;
2. Prove that in a perfect cipher the number of keys cannot be smaller than the number of messages;
3. Argue whether an asymmetric cipher can be perfect or not.

EXERCISE NO. 2 — #MARKS: 10

State the security definition of a Message Authentication Code (MAC).

List and briefly introduce the main methods of building a MAC out of other cryptographic primitives.

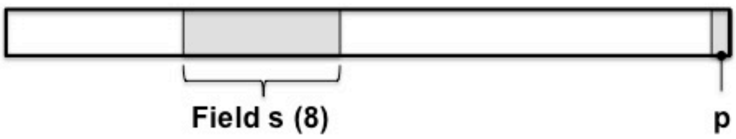


raw CBC

Show that the rawCBC-MAC (see figure) is insecure. Hint: compute the MAC t_1 of the single block message m_1 and the MAC t_2 of the two-block message $m_2 = (m_1, m_1 \oplus t_1)$. Generalize the attack for an arbitrary number of blocks message.

EXERCISE NO. 3 — #marks: 10

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.



Q1. Does this encryption scheme suffer from malleability? Motivate the answer.

Q2. Assume 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.

Q3. Propose a possible countermeasure.

SICUREZZA NELLE RETI SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

22 July 2015

SOLUTION

Exercise n.1

Q1, Q2, Q3. See theory.

Exercise n.2

Q1. See theory

Q2. See theory.

Q3. Compute t_1 and t_2 as hinted, and verify that $t_1 = t_2$. This means that a collision has arisen. One possible way to generalize is to consider a message having the following structure m = (m_1, $m_1 \oplus t_1$,…, $m_1 \oplus t_1$), where m_1 is a single block message and t_1 is m1's tag.

Exercise n. 3

Q1. 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]. If follows that P'[i] = P[i] xor 1, that is, P'[i] is the complement of P[i] (P'[i] = ~P[i]).

In order 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 has to 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 most significant bit in *s*.

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