Master in Computer Engineering, Master in Embedded Computing Systems

SECURITY IN NETWORKED COMPUTING SYSTEMS

20 JUNE 2016

◆: LMCE+LMECS **■:LMCE**

EXERCISE NO. 1 (◆) #MARKS: 10

With reference to the RSA crypto-system,

1. Illustrate the key generation, encryption, decryption algorithms;
2. Argue why it is considered secure;
3. Argue whether it can be considered perfect according to Shannon's theory.

EXERCISE NO. 2 (◆) #MARKS: 10

In an electronic auction, bidder B cast his bid β encrypting it by mean of the auctioneer *Alice*' s public key Π_A. Let us assume that a bid is an integer number on b-bits, $b = 32$. Argue whether the following protocols are secure w.r.t. to a passive adversary.

1. $B \rightarrow A: \{B, \beta\}_{\Pi_A}$
2. $B \rightarrow A: \{B, \beta, H(\beta)\}_{\Pi_A}$
3. $B \rightarrow A: \{B, H(\beta)\}_{\Pi_A}$
4. $B \rightarrow A: \{B, \rho, \beta\}_{\Pi_A}$
5. $B \rightarrow A: \{B, K\}_{\Pi_A}, \{B, \beta\}_K$

where H is a secure hash function whose output is t-bit, ρ is a random number of r-bits and, K is a random cryptographic key on k bits. Bob generates ρ and K upon casting his bid. Assuming that the encryption and the hash function are secure, determine the size in bit of ρ and K so that an attack requires 2^{128} steps.

EXERCISE NO. 3 (■) #MARKS: 10

With reference to the Kerberos system, argue the need for the Ticket Granting Service (TGS)?

June 20th, 2016

martedì 23 maggio 2017 16:22

Exercise 1

With reference to RSA,

1. .
2. .
3. .

Exercise 2

In an electronic auction, bidder B cast his bid BETA encrypting it by means of the auctioneer Alice's public kye pi_A.
Let us assume that a bid is an integer number on b-bits, b = 32.
Argue whether the following protocols are secure w.r.t. a passive adversary.

1. B → A: {B, Beta}_pi_a
2. B → A: {B, Beta, H(Beta)}_pi_A
3. B → A: {B, H(Beta)}_pi_a
4. B → A: {B, p, Beta}_pi_a
5. B → A: {B, K}_pi_a, {B, Beta}_K

Where H is a secure hash function whose output is t-bit, p is a random number of r-bits and, K is a random cryptographic key on k bits. Bob generates p and K upon casting his bid.
Assuming that the encryption and the has function are secure, determine the size in bit of p and K so that an attack requires 2^128 steps.

Solution

June 20th, 2016

1. Se l'avversario ha un'idea di Beta, non ha nemmeno bisogno di provare 2^32 valori per Beta.
2. Uguale al primo ma con un hash in più.
3. …
4. Dipende dalla lunghezza del numero random p.
   Beta is on 32 bits, therefore p has to be at least 128-32 = 96 bits long.
5. L'avversario deve:
   a. Provare le possibili chiavi

Exercise 3