Master in Computer Engineering *Master in Embedded Computing Systems*

SECURITY IN NETWORKED COMPUTING SYSTEMS

September 20, 2016

Name_____ **Serial nr.** _____

EXERCISE NO. 1 (ALL) #MARKS: 12

With reference to the perfect ciphers,

1. Give the Shannon's definition;
2. Give an intuitive practical interpretation of the definition;
3. Prove the Shannon's theorem;
4. Argue under which assumptions one-time pad is perfect.

EXERCISE NO. 2 (ALL) #MARKS: 8

When using the one-time pad (OTP) encryption scheme, it can occur that $k = \{0\}^*$, that is the key is a sequence of 0's. In this case ciphertext is equal to the plaintext.

Alice suggests to improve the one-time pad by only choosing non-zero keys. What do you think of this improvement? In particular, is the improved OTP still perfectly secret?

Let us suppose that you receive the message "Attack". In the improved OTP is it more likely that the plaintext is "Attack", "Defend" or "Rabbit"? What about in the original-OTP?

EXERCISE NO. 3 (LMCE) #MARKS: 10

Kerberos supports delegation.

1. Explain the delegation problem.
2. Illustrate the proxy ticket solution
3. Argue pros and cons of proxy tickets w.r.t. forwardable tickets

September 20th, 2016

martedì 23 maggio 2017 15:46

Not found on the professor's filesystem.
Here's a copy of it:

Exercise 1

With reference to the perfect ciphers,

1. Give the Shannon's definition
2. Give an intuitive pratctical interpretation of the definition
3. Prove the Shannon's theorem
4. Argue under which assumptions OTP is perfect

Exercise 2

When using the one-time pad (OTP) encryption scheme, it can occur that k = [0]*, that is the key is a sequence of 0's. In this case ciphertext is equal to the plaintext.
Alice suggests to improve the OTP by only choosing non-zero keys.
What do you think of this improvement? In particular, is the improved OTP still perfectly secret?
Let's suppose that you receive the message "Attack". In the improved OTP is it more likely that the plaintext is "Attack", "Defend" or "Rabbit"? What about in the orriginal-OTP?

Solution

Non è perfetto perché la probabilità a priori e a posteriori sono diverse.
Se si è in grado di dimostrare che |K| < |P|, è fatta.

September 20th, 2016

Le 3 stringhe son 3 possibili plaintext.
Nell'OTP canonico e nell'OTP modificato, cambia la probabilità che il plaintext sia uno di quei 3 se il ciphertext è "Attack"?

- OTP-canonico: l'avversario non può sapere quale plaintext ha più probabilità
- OTP-modificato: avendo levato k = [0]*, di sicuro il plaintext non è "Attack", la sua probabilità a priori non è più la stessa.
  Per quanto riguarda gli altri due ciphertext, non si conosce niente, nemmeno la probabilità legata.

Exercise 3

September 20th, 2016

Kerberos supports delegation.

1. Explain the delegation problem
2. Illustrate the proxy ticket solution
3. Argue pros and cons of proxy tickets w.r.t. frowardable tickets