cns20160727.odt

Name:	Last name:	Id:

Computer and network security
Sicurezza nelle reti e nei sistemi informatici
Crittografia e sicurezza delle reti

Exam of 27th July 2016, a.y. 2015-16. Time: 2 hours
Outcomes will be published in web page within 12th August 2016

FOR NON-ENGLISH: 2 penalty points (only applicable to Computer and network security)
FOR UNREADABLE HAND-WRITING: discretionary decision

Q1: Secure client-server authentication

We consider a client-server application whose clients run on modern smartphones and assume for simplicity there is a single server accessible via Internet.
Client-server conversations are TLS-based, thus meeting most of the requirements of the information security. However the designers want to develop a mutual authentication that works independently of the TLS authentication (not based on third parties!), using symmetric and/or public-key cryptography, hashing, etc.

[8/30] Design the mutual authentication system, so that it is robust against *eavesdropping*, *spoofing*, *MITM*, *replaying*. (At client side, both client software and user should be authenticated). Draw the sequence of messages exchanged by the two parties.

Q2: IPSec and TLS

Q2.1 [3/30] Give a high-level and black-box description of the IPsec protocol.
Q2.2 [3/30] Give a high-level and black-box description of the TLS protocol.
Q2.3 [2/30] Try proposing some guidelines to support application designers/developers in making a good choice between IPsec and TLS..

Q3: OFB

Q3.1 [3/30] Draw schemes for the operating mode OFB, both in encryption and decryption mode.
Q3.2 [3/30]

(a) Discuss how errors propagate in OFB encryption/decryption.
(b) Can OFB encryption/decryption be parallelised? Elaborate.
(c) Can pre-processing speed up the OFB encryption/decryption? Elaborate.

Q4: Birthday attack

Q4.1 [3/30] Describe what a *birthday attack* is.
Q4.2 [3/30] Eve wants to replace the original text of a digitally signed contract by a malicious alternative text. Describe a methodology allowing Eve to succeed, based on the *birthday attack*.

Q5: Short questions

Provide short answers (2 lines or a figure) to the following questions.

Q5.3 [1/30] Define the Euler totient function.
Q5.4 [2/30] What is the difference between *salted hashing* and *keyed hashing*?
Q5.5 [2/30] Access control: MAC vs DAC(draw a comparison table).

HAVE YOU SENT 2015-16 HOMEWORKS TO THE PROF.? YES / NO (<u>circle your answer</u>)

If YES:
I hereby confirm that I sent no. ________________ contributions (how many Qs)

Signature

____
(please sign in both cases)