cns20160914.odt

Name:	Last name:	Id:

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

Exam of 14th September 2016, a.y. 2015-16. Time: 2 hours
Outcomes will be published in web page within 30th September 2016

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

Q1: **Secure client authentication**

We consider a client-server application whose clients run on mobile devices and assume for simplicity there is a single server accessible via Internet.
Clients are downloaded and installed on devices through a standard interaction with the app store officially designated by the operating system.
The developers do not want that users can run on their devices other (compatible) client applications, possibly developed by third parties that know what protocols/interfaces are employed in the client-server interaction: only the official client should be used.

[6/30] Design an authentication system for the client side (this is not including the authentication of the user!) and draw the sequence of messages exchanged by the two parties.

Q2: **MAC and authentication tags**

Alice and Bob have agreed a shared and secure 256-bit secret key K_{AB} designated for supporting their procedure P (based on AES-256) for sending and verifying messages, to the purpose of data integrity and authentication (no confidentiality).
For sending a message M to Bob, Alice sends the pair (M, $K_{AB}\{M_1\}$), where M_1 is the first 128-bit block of M. K{B} denotes the encryption by AES-256 of the 128-bit block B, using the 256-bit key K.

Q2.1 [2/30] Describe the procedure at Bob's side for verifying message M.
Q2.2 [3/30] Show a possible attack where the adversary can replace M by a suitable message M' and send to Bob the pair (M', $K_{AB}\{M_1\}$), pretending to be Alice, and where the verification process described at Q2.1 succeeds.
Q2.3 [3/30] Propose a revision of procedure P that fixes the above attack and discuss its limits.

Q3: **PRNGs**

[6/30]
Discuss the security of the following PRNGs, by considering both cases of n_0 (initial seed) public and secret.
In what follows, H is a cryptographically secure hash function having a 256-bit digest, $H^{(i)}$ means H(H(H(...))) i times, and X is a 256-bit secret key.

$n_{i+1} = H(n_i)$, $i \geq 0$	$n_{i+1} = H^{(2)}(n_i)$, $i \geq 0$	$n_{i+1} = X\{n_i\}$, $i \geq 0$	$n_{i+1} = H^{(i+1)}(n_0)\{X\}$, $i \geq 0$
(a)	(b)	(c)	(d)

Q4: **Attacks**

Q4.1 [2/30] Describe what a **Meet-in-the-Middle** (not to be confused with Man-in-the-Middle) attack is and make an example.
Q4.2 [2/30] Describe what a **reflection attack** is and make an example.
Q4.3 [2/30] Describe what a replay attack is and make an example.

Q5: **Short questions**

Provide short answers (at most 4 lines and/or a figure) to the following questions. (Answers must be short!! Using more than 4 lines reduces the quality of the answer)

Q5.4 [2/30] State the Euler's theorem and (just) name one topic in cryptography where it is being used.

Q5.5 [2/30] Firewalls. Is session filtering *stateless* or *stateful*? Explain.

Q5.6 [2/30] HRU model. State an *undecidable* problem on a protection system.

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

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

Signature

____
(please sign in any case)