Name:	Last name:	Id:

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

Exam *of 14th January 2015, a.y. 2014-15. Time: 2 hours*

Q1: Modes of operations

Q1.1 [3/30] Describe what modes of operations are in the framework of block ciphers and the most relevant features to be considered for their analysis.

Q1.2 [3/30] Illustrate a mode of operations that makes the usage of a block cipher behaving similar to that of a stream cipher and discuss its security.

Q2: RSA

Q2.1 [3/30] Describe how RSA encryption/decryption work.

Q2.2 [2/30] Explain what is the mathematical relationship between *e* and *d* (the two exponents used in RSA).

Q2.3 [3/30] Why the textbook implementation of RSA is insecure? Provide at least an example.

Q3: Authentication and integrity

Sometimes Alice needs to send a file to Bob, guaranteeing her identity and the file integrity (no confidentiality required); the two parties are sharing a secret w and make use of a hash function H that outputs 40-bit numbers. Each time they use the following (pre-agreed) protocol.

$A \rightarrow B$: $w\{n_A\}$, where n_A is a nonce (Alice sends a challenge)

$B \rightarrow A$: $w\{n_A+1\}$ (Bob proves he knows the secret, providing response to challenge)

$A \rightarrow B$: $(F, H(F), w\{H(F)\})$ (Bob, given F, computes H(F) and $w\{H(F)\}$, and then compare his results to data actually received)

Q3.1 [3/30] Show how an attacker can act in place of Alice and send a file to Bob tricking him into believing that the file is coming from Alice.

Q3.2 [3/30] Fix the protocol without significantly perturbing it too.

Q4: Short questions on proxies

A company is protecting its intranet by a multi-homed bastion host B, acting as an application-level proxy. Provide short answers (2 lines max) to the following questions.

Q4.1 [2/30] Can B allow HTML incoming files and deny incoming JPG files in HTTP connections?

Q4.2 [2/30] Can B allow HTML incoming files and deny incoming JPG files in HTTPS connections?

Q4.3 [2/30] Can B allow HTML incoming files and deny incoming JPG files in HTTP VPN-connections?

Q5: Miscellaneous

Provide short answers (2 lines max) to the following questions.

Q5.1 [1/30] $\Phi(7) = ?$ (Φ is the Euler's totient function)

Q5.2 [1/30] $\Phi(12) = ?$

Q5.3 [2/30] Find the multiplicative inverse of 5 (mod 6)

Q5.4 [1/30] Define the birthday bound

Q5.5 [2/30] Is weak resistance to collisions implying strong resistance?

HAVE YOU SENT HOMEWORKS TO THE PROF.? IF YES, PLEASE CONFIRM HERE

I hereby confirm that the homework I sent to prof. d'Amore was (complete as appropriate)

- *produced entirely by myself*
- *prepared together with* _____

Signature

_____