Survey n° 5-a

Cryptography and Security 2025

Full Name: _____

SCIPER: _____

1. Which of the following is a standard property for cryptographic hash functions

   ☐ Unforgeability; ■ One-wayness; ☐ Integrity; ☐ Robustness.

2. To achieve 128-bit security, we would need a hash function with digest size at least:

   ☐ 128-bits for preimage attacks, and 64 bits for collision attacks.
   ☐ 256-bits for preimage attacks, and 256 bits for collision attacks.
   ■ 128-bits for preimage attacks, and 256 bits for collision attacks.
   ☐ 128-bits for preimage attacks, and 128 bits for collision attacks.

3. Which of the following best describes Figure 1?

   ☐ Decryption of Encrypt-then-Mac. ■ Decryption of Encrypt-and-Mac.
   ☐ Decryption of Mac-then-Encrypt. ☐ Decryption of Encrypt-or-Mac.

4. Which of the following describes the (computationally) binding property for a commitment scheme com?

   ☐ For a known m, and unknown r, $\mathsf{com}(m;r)$ is indistinguishable from random;
   ☐ For any m and c $\Pr_r[\mathsf{com}(m;r) = c]$ is negligible;
   ☐ Given $\mathsf{com}(m;r)$ it is computationally infeasible to recover m;
   ■ It is computationally infeasible to find m_1, m_2, r_1, r_2, with $m_1 \neq m_2$ such that $\mathsf{com}(m_1;r_1) = \mathsf{com}(m_2;r_2)$.

5. Which one of those hash functions is not considered secure in 2025 ?

   ■ SHA1 ☐ SHA256 ☐ SHA3 ☐ Poly1305

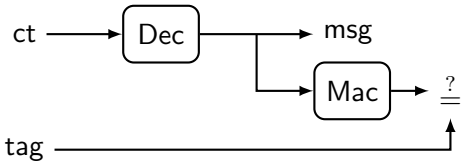

Figure 1