Survey n° 4

Cryptography and Security 2025

Full Name: _____

SCIPER: _____

1. Which of the following is **true** about a hash inversion attacks, with success probability 1, on a output space of size N?

   - ☐ Given N preprocessing operations, and N bits of stored memory, a dictionary attack requires run-time of at least $\sqrt{N}$.
   - ☐ An exhaustive search with run-time N, requires at least $\frac{N}{2}$ bits of memory.
   - ■ With sufficient preprocessing, dictionary attacks can run in time 1.
   - ☐ With sufficient preprocessing, dictionary attacks can run with memory 0.

2. Among the block cipher modes of operation CBC, OFB, and CTR, which require the use of a nonce?

   - ☐ OFB only.
   - ■ OFB and CTR.
   - ☐ CBC, OFB, and CTR.
   - ☐ CBC only.

3. Which of the following is **true**?

   - ☐ Double DES is designed to resist meet-in-the-middle attacks.
   - ☐ Double DES effectively has the same security as 2-Key Triple DES.
   - ☐ Both 2-Key Triple DES and 3-Key triple DES have 112 bit keys length
   - ■ There exists a key recovery attack with time complexity 2^{113}, and memory complexity 2^{56}, against 3-key Triple-DES.

4. Which of the following statements is **false**?

   - ☐ AES is not linear as it uses multiplication in $\mathsf{GF}(2^8)$.
   - ■ A Feistel scheme using a round function F requires computing F^{-1} to obtain its inverse.
   - ☐ In a Feistel scheme, the final halve swap of the Feistel scheme is omitted.
   - ☐ AES is a block cipher that always operate on blocks of 128 bits, independently of the security level.

5. Which of the following statement is **false**?

   - ■ In the security game against decryption under CPCA, for each n in the nonce space, the adversary can only query the decryption oracle with n once.
   - ☐ If a scheme is secure against decryption under CPCA, it is secure against key recovery under CPA
   - ☐ AES has not been proven secure against decryption under CPA.
   - ☐ An ideal cipher is secure against distinguishers under CPCA.