Survey n° 1

Cryptography and Security 2025

Full Name: _____

SCIPER: _____

C

1. The n^2 problem principle states that:

   - ☐ the number of communicating devices in a network squares every 16 month.
   - ■ the number of symmetric keys needed for n users to communicate grows quadratically in n.
   - ☐ it takes n^2 operations to perform a brute force search on a key of size n.
   - ☐ confidentiality requires a ciphertext of size n^2 for a plaintext of size n.

2. Given X a plaintext and Y a ciphertext, which of the following does **not** define perfect secrecy?

   - ☐ $\forall x, y,\ \mathbb{P}[X = x|Y = y] = \mathbb{P}[X = x]$
   - ☐ X and Y are independent
   - ■ $|\text{supp}(X)| \leq |\text{supp}(Y)|$
   - ☐ $\forall x, y,\ \mathbb{P}[Y = y|X = x] = \mathbb{P}[Y = y]$

3. Kerkhoffs principle states that:

   - ☐ any security vulnerability will be exposed eventually.
   - ☐ cryptographic constructions should not be patented.
   - ■ the security of a cryptosystem should only rely on the secrecy of the key.
   - ☐ computational power doubles roughly every 16 months.

4. Which of the following is **incorect**.

   - ☐ Confidentiality ensures that no information is leaked to undesired parties.
   - ☐ Authentication ensures that a malicious party cannot send a message and claim it was sent by another party.
   - ☐ Authentication ensures that a message makes sure who its author is.
   - ■ Confidentiality ensures that a message is protected from malicious tampering.

5. In Vernam cipher, which of the following is **not** necessary for security?

   - ■ The message must be uniformly distributed.
   - ☐ The message must be independent of the key.
   - ☐ The key must be used only once.
   - ☐ The key length must be at least as large as the plaintext.