Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

Classic cryptography
Self-assessment test

Select the correct answer.

1. What are the pair of basic techniques applied in classic ciphers?

   o Inversion and substitution.
   o Substitution and permutation.
   o Dispersion and compression.
   o Compression and expansion.

2. Complete the sentence with the right words:

   "_____ is a _____ cipher because the result of encrypting _____ characters is always the same"

   o Playfair, monoalphabetic, two.
   o Playfair, polygraphic, two.
   o Vigenère, monoalphabetic, two or more.
   o Vigenère, polygraphic, two.

3. A monoalphabetic cipher...

   o It is the one that just alters the order of characters in the cleartext.
   o It always replaces each character (for instance, "a") by other (for instance, "d")
   o It can operate with one or several characters in each operation.
   o It is implemented in the Enigma machine.

4. The scytale...

   o It is a cipher that works with substitutions.
   o The key is the length of the leather strip.
   o The key corresponds to the diameter of the cylinder.
   o The message is written along the leather strip and it is read by rows.

5. What is the right statement according to Hill cipher?

   o The decryption process requires the calculus of the modular inverse of the determinant of a matrix.
   o It is based on character transposition.
   o The message is encrypted character by character.
   o It is known as the perfect cipher, that is, mathematically unbreakable, though it is impractical in a real setting.