



SECURITY AND CRYPTOGRAPHY LABORATORY

EPFL / I & C

CH-1015 Lausanne

Phone: ++41 (0) 21 693 76 03

Fax: ++41 (0) 21 693 68 79

URL: <http://lasecwww.epfl.ch>

Example Survey - Solution

Name: _____

1. The *Kerckhoffs Principle* is one of the most famous laws of modern cryptography. This principle says that ...
 - ☐ in a network of n users, there is a number of potential pairs of users within the order of magnitude of n^2 .
 - ☒ security should not rely on the secrecy of the cryptosystem itself.
 - ☐ the speed of CPUs doubles every 18 months.
 - ☐ cryptosystem specifications should be made public.
2. Visual Cryptography is a visual illustration of ...
 - ☒ the Vernam Cipher.
 - ☐ Enigma.
 - ☐ the Vigenère Cipher.
 - ☐ the Caesar Cipher.
3. Which one of these cipher is perfectly secure (when used in the appropriate way)?
 - ☐ Enigma
 - ☒ Vernam
 - ☐ ROT13
 - ☐ Turing
4. The index of coincidence allows to ...
 - ☐ find the initial position of the rotors of an Enigma machine.
 - ☐ break the Vernam cipher.
 - ☒ check a guess for the length of the key of a Vigenère cipher.
 - ☐ improve the letter frequency analysis in a simple substitution cipher.
5. Insuring the *integrity* of the information...
 - ☐ means that the information should not leak to any unexpected party.
 - ☐ means that the information should make clear who the author is.
 - ☒ means that the information must be protected against any malicious modification.
 - ☐ is usually performed using Steganography.

6. Which of the following ciphers does not fulfill the Kerckhoffs Principle?
- ☐ Vernam
 - ☐ DES
 - ☐ Vigenère
 - ☒ Caesar
7. The fact that the index of coincidence of a (non void) text equals 1 implies that ...
- ☐ the text is truly random according to a uniform distribution.
 - ☐ the length of the text is 1.
 - ☒ all the characters of the text are equal.
 - ☐ the alphabet is binary.
8. A cryptosystem consists of carrying out the following operations:
- ☐ encryption and decryption only.
 - ☐ encryption, decryption, and key exchange.
 - ☒ encryption, decryption, and key generation.
 - ☐ encryption, decryption, key exchange, and key generation.
9. Which of the following assertions is not a property of a simple substitution cipher?
- ☐ Two letters of the ciphertext are equal if they are equal in the plaintext as well.
 - ☒ If a given character appears in the plaintext, then it appears in the ciphertext as well.
 - ☐ A simple substitution can be viewed as a permutation of the underlying alphabet.
 - ☐ The length of a ciphertext equals the length of the corresponding plaintext.
10. Crypto is ...
- ☐ complicated.
 - ☐ adversity theory.
 - ☐ fun.
 - ☐ a multidisciplinary area.

Note: You should definitely answer to question 10.