4.0

LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Cryptography and Security
http://lasecwww.epfl.ch/cs2007/

Cryptography and Security

2006 – 2007

Survey n° 1

Policy: Each question has exactly one possible right proposition. An answer is considered as right if you tick only the right proposition. A right answer provides 0.5 point. If nothing is ticked (unanswered), you obtain no point. If a bad proposition is ticked or several propositions are ticked you obtain a negative point of -0.5.
The mark of the test is

$$\text{mark} = \max(1, p + 1),$$

where p is the sum of all points (positive or negative).

+ 1. Which one of the following notions is not in the fundamental trilogy of cryptography?

☐ authentication ☐ integrity ☒ privacy ☐ confidentiality

+ 2. Which one of the following notions means that “the information should make clear who the author of it is”?

☒ authentication ☐ steganography ☐ privacy ☐ confidentiality

+ 3. Visual cryptography is a nice visual application of …

☐ … the Vigenère cipher.
☒ … the Vernam cipher.
☐ … the Caesar cipher.
☐ … ROT13.

− 4. Tick the *false* assertion.

☐ The index of coincidence is a useful tool to break the Vigenère cipher. ✓
☒ The index of coincidence is invariant under substitution.
☒ The Kasiski test makes use of the index of coincidence. ✓
☐ The Kasiski test is a useful tool to break the Vigenère cipher.

+ 5. Which one of the following encryption method is a simple substitution cipher?

☐ Vigenère cipher
☐ Vernam cipher
☒ Caesar cipher
☐ Spartan scytales

+ 6. The Enigma cipher …

☐ … never existed.
☐ … was invented by Kasiski.
☐ … does not respect the Kerckhoffs principle.
☒ … is less secure than the Vernam cipher.

+ 7. How many different simple substitution ciphers do exist with respect to an alphabet of 26 characters?

☒ 26! ☐ 2^{26} ☐ 26^2 ☐ 26

+ 8. What is the main reason why we usually do not use the Vernam cipher?

☐ The encryption step is too costly.
☐ This cipher does not guarantee the integrity.
☒ Generation of randomness and the exchange of keys are too costly.
☐ This cipher violates the Kerckhoffs principle.

− 9. The composition of a simple substitution cipher with itself corresponds to …

☐ … a Vigenère cipher with a key of length 2.
☒ … the identity.
☒ … another simple substitution cipher.
☐ … the Caesar cipher.

+ 10. "`0x7a11372a 0x480a5f46 0xe19a5a14 0x5ee04969 0x08b048bb`" To whom is this famous quotation attributed?

☐ Alexander the Great
☐ Blaise de Vigenère
☒ Serge Vaudenay
☐ Anonymous

Note: You should definitely answer question 10.