5.5

LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Cryptography and Security

http://lasecwww.epfl.ch/cs2007/

Cryptography and Security

2006 – 2007

Survey n° 3

Name:

1. Which of the following ciphers is based on a Feistel scheme?

☒ DES ☐ SAFER ☐ IDEA ☐ RC4

2. In the AES MixColumns procedure, a byte represents ...

☐ a polynomial of degree less than 16 with coefficients in $\mathbf{Z}_2$
☐ a polynomial of degree less than 4 with coefficients in $\mathbf{Z}_4$
☒ a polynomial of degree less than 8 with coefficients in $\mathbf{Z}_2$
☐ an integer between 0 and 255.

3. LFSRs are used within ...

☐ IDEA ☒ A5/1 ☐ AES ☐ SAFER

4. What is the length in bits of the input and output of a DES S-Box respectively?

☐ 6 and 6 ☐ 4 and 6 ☒ 6 and 4 ☐ 4 and 4

5. Tick the *false* assertion.

☐ A Feistel scheme is invertible even if the round functions are not injective.
☒ A Feistel scheme is not invertible if the round functions are not surjective.
☐ A Feistel scheme is an involution if the round functions are all identical.
☐ The name of Feistel schemes goes back to the LUCIFER cipher.

6. Which of the following terms represents a mode of operation which transforms a block cipher into a stream cipher?

☐ 3DES ☐ CBC ☐ ECB ☒ CTR

7. What is the worst-case complexity of an exhaustive key search attack against a block cipher having a 64-bit key and 128-bit blocks?

☐ 2^{128} ☒ 2^{64} ☐ 2^{96} ☐ 2^{127}

8. Which of the following algorithms is a stream cipher?

☐ FOX ☐ IDEA ☒ RC4 ☐ AES

9. Tick the true assertion.

☐ A dictionary attack requires less memory than a time-memory tradeoff.
☒ Double-DES succumbs under a Meet-in-the-Middle attack.
☐ AES is the ancestor of DES.
☐ IDEA has the same round functions as DES.

10. Tick the *false* assertion.

☐ E0 is a Bluetooth standard. ☐ E0 is a stream cipher.
☐ E0 makes use of LFSR. ☒ E0 is based on RC4.