Univ. Grenoble Alpes/Grenoble INP **2016–2017**

M2 Cybersecurity

MCQ Training

MCQ (Level 1) : *Good answer gives 1 points. Bad answer gives -0.5 points*

After appropriate training, you should be able to answer such questions in less than 1 minute on average.

1 In a hybrid cryptosystem we use ECC based cryptographic primivites for the asymmetric part and a symmetric cipher with keys of 256 bits. What should be the (minimal) length of the keys for the ECC part in order to be coherent with the key size of our symmetric cipher ?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits

2 For a classical computer, the runtime complexity of the best generic attack for the ECDLP for a curve of order p (prime) is
A) $O(p)$ B) $O(p^{\frac{1}{2}})$ C) $O(p\log(p))$

3 In our current knowledge, which of the following mathematical problem is not solved in quantum polynomial running time ?
A) Factorization of large integers B) ECDLP C) CVP

4 In our current knowledge, if we want to use RSA with a security level of 256 bits (i.e., the best generic attack requires at least 2^{256} operations), what should be the corresponding length (in bits) of the RSA modulus ?
A) 2048 bits B) 4096 bits C) 15360 bits D) 30720 bits

5 Which of the following is not a valid key size for AES ?
A) 128 B) 192 C) 224 D) 256

6 Which of the following finite fields cannot be used in order to construct $\mathbb{F}_{256}$ as a finite extension on it ?
A) $\mathbb{F}_4$ B) $\mathbb{F}_8$ C) $\mathbb{F}_{16}$

7 Which of the following algorithms has the best asymptotic complexity (on a classical Turing machine) for the factorisation of large RSA modulus ?
A) Pollard/Brent (ρ-algorithm) B) ECM C) NFS

8 In our current knowledge, which of the following cryptosystems is not broken in quantum polynomial running time ?
A) RSA B) ECC C) NTRU

9 In Rinjdael, what is the largest number of rounds that we can choose ?
A) 14 B) 16 C) 18

10 In AES, which operation is not performed in the last round ?
A) SubBytes B) ShiftRows C) MixColumns D) AddRoundKey

...Turn the page please.

MCQ (Level 2) : *Good answer gives 2 points. Bad answer gives -1 points*

1 We consider the alphabet $\mathscr{A} = \{1,2,3,4,5,6,7,8,9\}$ and the mathematical substitution

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 2 & 5 & 8 & 9 & 1 & 3 & 7 \end{pmatrix}.$$

Which of the following number is, in the cryptographic meaning, either a substitution or a permutation of 314159265 by σ ? (*there is only one correct answer*)
A) 911656342 B) 265687498 C) 911535642 D) 265678497

2 Let $\mathbb{F}_4$ built as the quotient of $\mathbb{F}_2[T]$ by $T^2 + T + 1$. Denote by ω the class of T in the quotient (i.e., $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}$ and $\omega^2 = 1+\omega$). Which of the following polynomials of $\mathbb{F}_4[X]$ is irreducible and could be used for the construction of $\mathbb{F}_{256}$ as an extension of $\mathbb{F}_4$?
A) $X^2 + \omega X + 1$ B) $X^4 + X + 1$ C) $X^4 + \omega X + 1$ D) $X^4 + \omega X^2 + 1$

3 Which of the following algebraic curves given in affine form (with integer coefficients) is elliptic over $\mathbb{F}_7$?
A) $y^2 = x^5 + x + 1$ B) $y^2 = x^3 + 7x$ C) $y^2 = x^3 + x + 5$ D) $y^2 = x^3 + 4x$