Cryptography – Questionnaire 6

Name: _____

Matr.: _____

Questions

	true	false
OWF exist if and only if CCA-secure ES exist.	☐	☐
RSA "works" for $N = 35$ and $e = 3$, i.e. $x \mapsto x^e \bmod N$ is a permutation (in particular: invertible).	☐	☐
The ElGamal-PKES is CCA-secure.	☐	☐
If DDH is hard w.r.t. $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ then ElGamal based on $\mathsf{Gen}\mathbb{G}_{\mathsf{cyc}}$ is CPA-secure.	☐	☐

"(One|two)-liners"

Exercise 6.1 **2P**

Briefly state why the DDH over $\mathbb{Z}_p^*$ (p prime) is *not* hard.
Answer:

Exercise 6.2 **2P**

Suppose Bob's public ElGamal key is $(\mathbb{G}, q, g, h_b) = (\mathbb{Z}_{17}^*, 16, 6, 5)$. Alice wants to send him the message $m = 7$ encrypted using the ElGamal PKES. Compute the ciphertext $c = (c_1, c_2)$ that is sent to Bob assuming Alice has generated $a = 3$ as her secret.
Answer:

Exercise 6.3 **2P**

Briefly state

- why RSA-based PKES use a probabilistic padding scheme and
- name one of these schemes used in practice.

Answer: